國家通訊傳播委員會

資訊安全管理系統研究計畫
期末報告

執行單位：中華民國資訊軟體協會

中華民國100年11月

目　次

1. 計畫緣起與目的 1
1.1. 計畫緣起 1
1.2. 研究目的 2
1.2.1. 引進國外最新資訊安全管理標準 2
1.2.2. 督促通訊傳播事業導入資通安全管理機制 2
1.2.3. 確保通訊傳播事業之消費者個人資料安全 2
1.2.4. 完備通訊傳播事業資通安全管理規範對象 2
1.3. 報告研究範圍 3
2. 研究方法概述 4
2.1.1. 文獻研究法 5
2.1.2. 質性(個案)研究法 6
2.1.3. 問卷調查法 8
3. 專案進行步驟與結果 13
3.1. 通訊傳播事業特性之分析 13
3.1.1. 用詞定義 13
3.1.2. 業務區分 13
3.2. ISMS 國際標準之發展 18
3.2.1. ISO/IEC 27001:2005 19
3.2.2. ISO/IEC 27002:2007 22
3.2.3. ISO/IEC 27003:2010 23
3.2.4. ISO/IEC 27005:2008 29
3.2.5. ISO/IEC 27004:2009 39
3.2.6. ISO/IEC 27011:2008 43
3.3. 個案訪談 43

3.3.1. 研究命題 43
3.3.2. 文獻探討 44
3.3.3. 風險意識文化建構過程 46
3.3.4. 企業營運 50
3.3.5. 主管機關的影響 51
3.3.6. 研究發現 52
3.4. 問卷調查 54
3.4.1. 國內通訊傳播產業現況 54
3.4.2. 電信事業通過 ISMS 驗證之統計 57
3.4.3. 調查作業進行 63
3.4.4. 問卷設計說明 64
3.4.5. 調查結果統計 64
3.4.6. 結構化方程模式分析 79
3.4.7. 研究發現 91
3.4.8. 重要度績效分析法 92
3.4.9. 研究發現 102
3.5. 個人資料保護法 103
3.5.1. 法案修正重點 103
3.5.2. 相關重要條文摘錄 106
3.5.3. 施行細則內容摘錄 111
3.5.4. 台灣個人資料保護與管理制度簡介 114
3.5.5. 特定隱私保護措施(Privacy-Specific Safeguards) 115
3.5.6. 個人資料保護策略擬定 118
3.5.7. 個資保護安全控制措施 120
4. 研究分析 122
4.1. 風險概念與模型 122
4.2. 風險分析策略選項 124

4.2.1. 基準作法(Baseline Approach) 124
4.2.2. 詳細風險評鑑(Detailed Risk Analysis) 125
4.2.3. 組合式作法(Combined Approach) 126
4.3. 美國聯邦風險管理架構 127
4.3.1. NIST SP 800-30 Risk Management Guide 127
4.3.2. FIPS 199 聯邦資訊系統分類分級標準 128
4.3.3. NIST 風險管理框架 129
4.4. 我國資訊安全管理制度發展歷程 133
4.4.1. 資安等級區分方式 133
4.4.2. 資安等級應執行之工作事項 134
4.4.3. 防禦機制強度 135
4.4.4. ISMS 推動作業之範圍 136
4.4.5. 資訊安全責任等級分級作業流程修訂 137
4.4.6. 資訊系統分類分級鑑別機制 139
4.5. 研究心得 144
5. 結論與建議 148
5.1. 結論 148
5.2. 建議事項 149
5.2.1. 資通安全管理機制影響構面、評估等級及實施範圍 149
5.2.2. 資通安全實施程序與風險評鑑模式之建議 152
5.2.3. 資通安全管理之有效性量測方法與量測措施 157
5.3. 通訊傳播事業資訊通訊安全管理作業要點修訂 161
5.4. 通訊傳播事業資通安全管理手冊修訂建議 164
5.5. 通訊傳播事業安全控制措施修訂建議 164
6. 辦理資通安全管理機制座談會 165
7. 參考文獻 206

8. 附件 213
8.1. 附件 1 資訊安全管理系統研究問卷 ..... 附件 1-1
8.2. 附件 2 資訊安全測量構面範例 ..... 附件 213
8.3. 附件 3 通訊傳播事業資通安全管理要點修正條文對照表(英文版)..... 附件 3-1
8.4. 附件 4 通訊傳播事業資通安全管理手冊修訂建議草案 ..... 附件 4-1
8.4.1. 附錄 1 通訊傳播事業資通安全等級自我評估彙整表 ..... 附錄 1-1
8.4.2. 附錄 2 通訊傳播事業資通安全等級自我評估說明表 ..... 附錄 2-1
8.4.3. 附錄 3 通訊傳播事業資通安全管理詳細風險評鑑表 ..... 附錄 3-1
8.4.4. 附錄 4 通訊傳播事業資通安全管理機制實施計畫參考範本 ..... 附錄 4-1
8.4.5. 附錄 5 資通安全管理實施計畫應執行工作事項表 ..... 附錄 5-1
8.4.6. 附錄 6 通訊傳播事業資通安全管理內部稽核表(修訂對照)..... 附錄 6-1
8.4.7. 附錄 7 通訊事業增項稽核表 ..... 附錄 7-1
8.4.8. 附錄 8 傳播事業增項稽核表 ..... 附錄 8-1
8.4.9. 附錄 9 個人資料保護安全控制措施 ..... 附錄 9-1
8.4.10. 附錄 10 國家通訊傳播委員會資通安全事故通報單 ..... 附錄 10-1
8.4.11. 附錄 11 資通安全管理矯正／預防措施一覽表 ..... 附錄 11-1
8.4.12. 附錄 12 資通安全管理矯正／預防措施單 ..... 附錄 12-1
8.4.13. 附錄 13 內部稽核表檢查項目勾選不適用之說明 ..... 附錄 13-1
8.4.14. 附錄 14 增項稽核表檢查項目勾選不適用之說明 ..... 附錄 14-1
8.5. 附件 5 通訊傳播事業資通安全管理手冊修訂建議草案(英文版) ..... 附件 5-1
8.6. 附件 6 通訊傳播事業資通安全管理內部稽核修訂對照表 ..... 附件 6-1
8.7. 附件 7 通訊事業增項稽核修訂對照表 ..... 附件 7-1
8.8. 附件 8 傳播事業增項稽核修訂對照表 ..... 附件 8-1

8.9. 附件 9 通訊傳播事業個資保護控制措施內部稽核修訂對照表 ..... 附件 9-1
8.10. 附件 10 第 1 場次資通安全管理機制座談會會議紀錄..... 附件 10-1
8.11. 附件 11 第 2 場次資通安全管理機制座談會會議紀錄..... 附件 11-1
8.12. 附件 12 第 3 場次資通安全管理機制座談會會議紀錄..... 附件 12-1
8.13. 附件 13 第 4 場次資通安全管理機制座談會會議紀錄..... 附件 13-1
8.14. 附件 14 第 5 場次資通安全管理機制座談會會議紀錄..... 附件 14-1
8.15. 附件 15 第 6 場次資通安全管理機制座談會會議紀錄..... 附件 15-1
8.16. 附件 16 資通安全管理機制成果發表會會議記錄..... 附件 16-1
8.17. 附件 17 ISO/IEC 27011 控制措施對照表..... 附件 17-1

圖　目　次

圖 1　文獻研究架構圖 6
圖 2　個案研究之程序 7
圖 3　紮根理論研究流程圖 8
圖 4　適用於 ISMS 過程之 PDCA 模型 20
圖 5　ISO/IEC 27002 架構圖 23
圖 6　ISMS 專案階段區分 24
圖 7　獲得管理階層的承諾，啟動 ISMS 專案階段 25
圖 8　定義 ISMS 的範圍與政策階段 26
圖 9　資訊安全需求分析階段 27
圖 10　進行風險評鑑與風險處理規劃階段 28
圖 11　設計 ISMS 階段 29
圖 12　資訊安全風險管理過程圖 31
圖 13　詳細風險評鑑作法活動程序圖 37
圖 14　ISMS PDCA 循環之安全測量 41
圖 15　資訊安全測量模型 42
圖 16　風險意識文化建構過程 46
圖 17　風險意識文化建置整體過程 53
圖 18　問卷調查－產業類別統計 65
圖 19　問卷調查－員工人數統計 65
圖 20　問卷調查－資本額統計 66
圖 21　問卷調查－個人資料數量統計 66
圖 22　問卷調查－通過 ISMS 驗證之範圍統計 67
圖 23　問卷調查－安全損害組織信譽之重視程度統計 69
圖 24　問卷調查－安全造成人員傷亡之重視程度統計 70
圖 25　問卷調查－個人資料保護之程度統計 70

圖 26　問卷調查－安全影響業務運作之重視程度統計 71
圖 27　問卷調查－資料保護受到損害之重視程度統計 71
圖 28　問卷調查－安全相關法律規程之遵循程度統計 72
圖 29　問卷調查－營運業務所需資訊化程度統計 72
圖 30　問卷調查－對上述營運資訊系統之依賴程度統計 73
圖 31　問卷調查－主管機關政策對於資源投入資安之影響程度統計 73
圖 32　問卷調查－法律對於落實資訊安全意願之影響程度統計 74
圖 33　問卷調查－委外作業安全重視程度統計 74
圖 34　問卷調查－營運持續重視之程度統計 75
圖 35　問卷調查－員工安全認知訓練之程度統計 75
圖 36　問卷調查－明確安全權責區分之程度統計 76
圖 37　問卷調查－系統化方式實施資訊安全管理統計 76
圖 38　問卷調查－安全概念融入組織文化之程度統計 77
圖 39　問卷調查－風險評鑑作業之程度統計 77
圖 40　問卷調查－資訊設備與員工比例統計 78
圖 41　問卷調查－資訊安全資源投入比例統計 78
圖 42　風險意識文化建置整體過程 79
圖 43　本計畫修正前 SEM 模型 83
圖 44　本計畫修正後 SEM 模型 85
圖 45　本計畫實證模型 87
圖 46　重要度--滿意度矩陣 94
圖 47　IPA 分析 98
圖 48　第一類電信 IPA 分析 100
圖 49　第二類電信 IPA 分析 101
圖 50　傳播事業 IPA 分析 102
圖 51　個人資料管理之 PDCA 循環 115
圖 52　損害賠償訴訟成立要件 119

圖 53　安全元件關係圖 123
圖 54　風險管理關係圖 124
圖 55　Risk Assessment Methodology Flowchart 128
圖 56　Risk Management Reamework of NIST 130
圖 57　美國政府機關資訊系統風險管理整體角度思考圖 132
圖 58　Multi-Tiered Organization-Wide Risk Management 133
圖 59　資訊系統分類分級與鑑別機制處理程序 140
圖 60　風險管理生命週期 157

表　目　次

表 1　研究方法與專案進行步驟 4
表 2　可信度高低與 Cronbach α係數之對照表 11
表 3　樣本與因素負荷量選取標準值 11
表 4　KMO 與 Bartlett's 球形檢定 12
表 5　通訊傳播事業業務區分表 14
表 6　ISO/IEC 27000 系列標準說明表 19
表 7　PCDA 模型中之各過程工作內容 21
表 8　ISMS 與資訊安全風險管理過程之對照 33
表 9　第一類電信事業執照數統計表 55
表 10　第二類電信事業執照數統計表 55
表 11　廣播電視事業執照數統計表 56
表 12　全球通過 ISO/IEC 27001 數量統計表 57
表 13　取得 ISO/IEC 27001 驗證之電信事業 59
表 14　取得電信事業資通安全管理手冊之 ISO/IEC 27011 增項稽核表驗證合格證明之電信事業 61
表 15　我國通過 ISMS 驗證之產業分析表 63
表 16　通訊傳播事業對於企業資訊環境之認知程度統計表 68
表 17　結構化方程模式之研究假說 80
表 18　規劃階段－結構方程模式之變項命名 80
表 19　建置階段－結構方程模式之變項命名 81
表 20　維持階段－結構方程模式之變項命名 82
表 21　結構方程模式變項之判斷 84
表 22　問卷信度分析 86
表 23　整體模式適配度說明表 88
表 24　非標準化之各項估計值 89

表 25　標準化之各項估計值 90
表 26　自變項間之共變異數 90
表 27　自變項間之相關係數 91
表 28　結構化方程模式之統計推論 91
表 29　因素分析法之信效度 96
表 30　IPA 分析結果 99
表 31　個資法施行細則內容摘錄 111
表 32　個資保護安全控制措施 120
表 33　FIPS 199 安全等級區分表 129
表 34　NIST 安全防護基準表(範例) 131
表 35　政府機關資安等級區分方式 134
表 36　各類資安系統等級應執行之工作事項表 135
表 37　資訊安全機制強度等級 136
表 38　ISMS 推動作業之範圍 136
表 39　各機關(構)資安等級應執行工作事項表 138
表 40　鑑別機制處理程序步驟說明表 140
表 41　安全等級設定原則表 143
表 42　影響構面／安全等級評估 151
表 43　ISMS 專案施行程序檢查表 152
表 44　資訊安全測量構面樣板 158
表 45　通訊傳播事業資訊通訊安全管理作業要點修正條文對照表 161
表 46　資通安全管理機制座談會場次表 165
表 47　資通安全管理機制座談會參與專家名單 166
表 48　資通安全管理機制座談會意見彙整表 170

摘要

通訊傳播事業擁有網路與系統等資源，因經營業務之需，留存大量用戶個人資料，常為不法人士覬覦目標，為防堵該等事件發生，國家通訊傳播委員會(以下簡稱 NCC)，規劃通訊傳播事業之「資訊安全管理系統研究計畫」(以下簡稱本專案)。

研究目的：

- 引進國外最新資訊安全管理標準
- 督促通訊傳播事業導入資通安全管理機制
- 確保通訊傳播事業消費者個人資料安全
- 完備通訊傳播事業資通安全管理規範對象

本研究首先針對通訊傳播事業特性進行分析，依據通訊傳播基本法用詞定義：通訊傳播指以有線、無線、衛星或其他電子傳輸設施傳送聲音、影像、文字或數據者。通訊傳播事業則指經營通訊傳播業務者。

通訊(電信)事業因涉及通信秘密保護，訂有相關刑責，對於機密性之要求相當高，且有大量電信機線設備，為維持通訊服務水準，故對於可用性之要求亦相當高；少部分第二類電信不具備機線設備，單純提供轉售服務者，對於資訊安全之要求相對降低。

傳播事業所擁有之廣播機線設備特性與第一類電信雷同，對於可用性之要求不分軒輊，但因係對公眾進行傳播，故對機密性之要求極低。廣播電視節目供應事業較為特殊，重點在於節目內容分級與限制觀看年齡與時段，或是有關新聞報導之中立客觀，幾乎不涉及機密性與可用性之要求，就資訊安全管理觀點，其風險等級較低，對於營運安全之改善效益有限。

本研究從資訊安全觀點，以不同安全領域、安全目標及控制措施，考量

上述目的事業，對於資訊安全管理之機密、完整性及可用性之要求差異，參考 CNS/ISO/IEC 27002 及 27011 之內容，建議適用之安全控制措施。

其次，本研究以「風險意識文化建置」為觀點，由宏觀的角度，探討組織在建置資訊安全管理系統(以下簡稱 ISMS)之過程中，內部建構風險意識與資安文化塑造的現象，經訪談發現，企業導入資訊安全管理制度，主要來自外部力量要求，也就是主管機關的態度將是推動的關鍵。但資訊安全管理制度要能夠被落實，則需要企業形成內部力量，藉由意識重建、情境認知、資安治理及資安文化之形成，逐步建立企業風險文化。

本研究第三步驟針對國內通訊傳播事業進行問卷調查，將個案研究發現之風險意識文化建置整體過程，依個案導入 ISMS 過程，劃分為規劃階段、建置階段及維持階段，並以此三階段為結構化方程模式之自變項(外因潛在變項)，探討組織成員對組織資訊環境之認知。

調查發現：規劃階段重要因素包含「資料保護受損」、「影響業務運作」及「法規遵循」，企業在建置 ISMS 之規劃認知，即是避免企業的「資料保護受到損害」與避免事故的發生「影響組織正常營運」，且需遵循安全相關法律規程進行規劃。後續將以上述三項因素作為通訊傳播事業資通安全等級評估之三個重要影響構面。

另運用重要度績效分析法(Importance Performance Analysis, IPA)，調查企業對於資安控制措施的認知程度與內部實際的實施程度。經由 IPA 分析後發現，落入「優先改善」區域之 22 個問項，大多源於「資訊安全組織」、「資產管理」、「人力資源安全」、「通訊與作業管理」、「存取控制」、「資訊系統獲取、開發及維護」與「資訊安全事故管理」等安全領域。後續以此作為資通安全等級劃分之最小限安全等級需求。

本研究第四步驟針對 ISMS 國際標準與我國個資法內容，進行文獻探討，標準文獻部分：

ISO/IEC 27001:2005 資安管理系統要求事項(Information technology − Security techniques − Information security management systems − Requirements)，其目的是制定一個用以建立、實作、運作、監控、審查、維持及改進「資訊安全管理系統」之模型，也是驗證之要求事項。

ISO/IEC 27002:2007 資訊安全管理作業規範資訊安全管理作業規範(Information technology − Security techniques − Code of practice forinformation security management)，其目的是建立一套用以起始、實作、維持及改進組織內之資訊安全管理指導綱要與一般原則。其控制目標與控制措施將被實作以滿足風險評鑑所識別的要求而設，可作為發展組織安全標準與有效安全管理實務的作業指導綱要，協助建立組織間活動之信賴。

ISO/IEC 27003:2010 資訊安全管理系統實施指引(Information technology — Security techniques — Information security management system implementation guidance)，主要在補充說明 ISO/IEC 27001 規劃階段之 4.2.1 建立 ISMS，包含定義資訊安全管理系統之範圍與邊界、發展組織資安政策、選定風險評鑑方法，並進行風險評鑑工作，再依據風險評鑑之結果選擇控制措施。

ISO/IEC 27005:2008 資訊安全風險管理(Information technology − Security techniques − Information security riskmanagement)，提供組織內資訊安全風險管理指導綱要，並支援 CNS 27001 資訊安全管理系統的特定要求，然而，本標準並不提供任何資訊安全風險管理之特定方法論，組織可自行依據例如資訊安全管理系統之範圍、風險管理之全景或產業別等，定義其風險管理作法。

ISO/IEC 27004:2009 資訊安全管理－測量方法(Information technology — Security techniques — Information security management — Measurement)，此標準提供發展與使用安全控制措施與測量方法之指引，用以評估 ISMS 實施 ISO/IEC 27001 所描述控制措施之有效性，包含政策、資訊風險管理、控制目標、流程及程序等評估，協助鑑別哪些控制措施需要改變或強化，但同時也特別強調沒有一種安全控制措施之測量方法，可以完全保證安全。

ISO/IEC 27011:2008 植基於 ISO/IEC 27002 之電信業資訊安全管理指引

Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 其控制措施之架構與 ISO/IEC 27002 之架構一致，大部分控制措施均引用自 ISO/IEC 27002，修訂內容著重點於機密性協議，包含人員與外部團體，主要來自對通信秘密之保護要求，並加強實體環境與電信設施與機線設備之保護，計新增一個安全目標，強化設置於第三方通信設施之管理，共計新增 13 個控制措施，另外補充修訂 26 個控制措施。

有關我國之個資保護法案已於 99 年 5 月 26 日經總統公布，並將名稱修正為「個人資料保護法」，施行日期由行政院定之，為配合本法修正內容，避免人格權受侵害，促進個人資料合理利用，以及順利推動本法施行，將施行細則內容修正如下：

規定受委託蒐集、處理或利用個人資料之法人、團體或自然人，於本法適用範圍內視同委託機關，增訂委託人之適當監督義務規定。並增訂本法所稱適當安全維護措施、安全維護事項或適當之安全措施之事項內容規定。

最後依據以上研究心得，本研究之結論與建議摘述如后：

(1) 通訊傳播事業對於資訊安全之重視，進行因素分析之結果，發現目的事業組織信譽遭受影響，其原因係來自於「資料保護受損」、「影響業務運作」及「影響法律規章遵循」違反後之結果，且就主管機關之立場，應著重於民眾權益維護，與通訊傳播事業個別公司之信譽或形象無關，故建議針對通訊傳播事業所擁有之資產群組，分類為「關鍵業務」、「支援業務」及「行政業務」，依據「資料保護受到損害」、「影響業務運作」及「影響法律規章遵循」三個構面，將資產群組之安全等級區分為「高」、「中」、「普」三級進行資產安全等級評估，才是目的事業真正關心的重點所在，亦可相對簡化目的事業之作業負擔。

(2) 考量通訊傳播事業特性分析，第一類電信與第二類電信，對於通信秘密之保護有嚴格法令限制，對於機密性要求極高。有線廣播電視業者等，

擁有大量電信、傳播機線設備，對於可用性要求極高。廣播節目供應事業，著重於節目與廣告管理，對於資訊安全管理之要求極低。故建議宜依據上述之企業安全等級評定方法，區分為 A 、B 、C 三級，以針對不同安全等級，建議適用之安全防護基準，較為妥適。

(3) 通訊傳播事業對資訊安全之重視程度，不因員工人數或資本額度而有差異，均相當重視侵犯個人隱私、資料保護受到損害而影響業務運作等，避免降低顧客對於企業之信任。

(4) 通訊傳播事業宜實施高階風險評鑑作法(High-Level Risk Assessment)，依據執照核發之營業項目範圍，調查通訊傳播事業營運所需之資產群組，若組織規模龐大者，得區分為不同事業體或部門，區分為「關鍵業務」、「支援業務」及「行政業務」三大類，分別進行資產安全等級評估，最後將所有經評定資產群組之資產安全等級彙整，取其最高者，作為評定企業安全等級之依據，區分為 A、B、C 三級，如最高之資產群組安全等級為「高級」者，其企業安全等級為「A」級；如最高之資產群組安全等級為「中級」者，其企業安全等級為「B」級；如最高之資產群組安全等級為「普級」者，其企業安全等級為「C」級，分別適用不同防護基準。

有關「通訊傳播事業資通安全管理要點」修訂、「通訊傳播事業資通安全管理作業手冊」修訂及通訊傳播事業導入資通安全管理機制之實施計畫參考範本等工作事項，請參閱本研究報告附件。

Abstract

The communication industry, with such resources as networks and systems, usually retain the personal information of a large number of users, so they often become the targets of unscrupulous people. To prevent the occurrences of such attempts, the National Communications Commission (hereinafter referred to as the NCC) has been drafting the “Information Security Management System Plan” (hereinafter referred to as the Project) for the communication and broadcasting industry.

Objectives of the Project:

- Introduce the updated information security management standards from foreign countries.
- Urge the communication industry to adopt the information security management system.
- Ensure the security of the personal information of the consumers of the communications and broadcasting industry.
- Complete the targeted subjects to be restricted for the information security management for the communication and broadcasting industry.

In this study, the characteristics of the communication and broadcasting industry were analyzed. According to the terminology defined in the Fundamental Communication and Broadcasting Act, communication and broadcasting refer to wired, wireless, satellite, or other electronic transmission facilities which transmit voice, images, text, or data. The communication and broadcasting industry refers to those who operate communications and broadcasting businesses.

The communications (telecommunications) industry is involved in the protection of communication secrets, so relevant criminal liabilities are stipulated,

and the requirements of confidentiality are very high. In addition, because a large number of telecommunications facilities are used, the requirements of availability are also very high in order to maintain the standard of communications services. For some of the Type II telecommunications enterprises which do not have telecommunications facilities but simply provide resale services, the requirements for information security is relatively lower.

The broadcasting facilities owned by the broadcasting industry have the same characteristics as those owned by Type I telecommunications enterprises, so their requirements of availability are nearly identical. However, the contents are for public broadcasting, so the confidentiality requirements are extremely low. The radio and television program providers are unique businesses which are focused on the classification of program contents and the restrictions on ages and time slots of viewers. For news which is neutral, objective, or not very involving of confidentiality and availability requirements, the risk level is relatively low in terms of the information security management. Therefore, the improvement of operation security is limited.

The plan focused on proposing suitable security control measures from the viewpoints of information security; different security domains, security objectives and control measures; the differences of the requirements for the confidentiality, integrity, and availability of information security management for the aforementioned businesses; and the provisions in CNS/ISO/IEC 27002 and 27011.

Secondly, this study is based on the viewpoint of “establishing a risk awareness culture” with a broad perspective to discuss the internal establishment of risk awareness and the shaping of information security culture during the establishment of an information security management system (hereinafter referred to as ISMS) in an organization. According to the interviews, the adoption of the

information security management system by the enterprises is mainly promoted via external forces and requirements. That is, the attitude of the authorities is the key to the promotion. However, the implementation of the information security management system requires the enterprises to form the internal forces by means of awareness reconstruction, scenario awareness, information security management, and information security culture, so as to establish the enterprises' risk culture.

In this study, the third step is to conduct a questionnaire survey for the domestic communication and broadcasting enterprises. The entire process of establishing the risk awareness culture discovered in case studies is analyzed based on the progress of adopting the ISMS in the respective cases and categorized into the planning phase, the establishing phase, and the maintenance phase. These three phases are then used as the independent variables (external potential variables) to discuss the organization members' awareness of the organization's information environment.

According to the survey: The important factors in the planning phase include "infringement of data protection", "influence on business operations", and "compliance to regulations". The goal of awareness of the enterprises' ISMS is to prevent the enterprises' data protection from being infringed, to prevent the normal business operations of the organizations from being affected by incidents, and to comply with security-related regulations for planning. The above mentioned three factors are then used as the three important aspects for evaluating the information security ratings of the communication and broadcasting enterprises.

In addition, the Importance Performance Analysis (IPA) is used to investigate the enterprises' level of awareness and the level of internal implementation of the information security control measures. According to the IPA analysis, it is found that the 22 issues in the "priority improvement" area mostly originate from such

security areas as “information secure organizations”, “asset management”, “human resource security”, “communications and operation management”, “access control”, “acquisition, development and maintenance of information systems”, and “management of information security incidents”. These are then used as the minimum security requirements for the classification of the information and communication security levels.

The fourth step in this study is the literature survey of the international standards of ISMS and the domestic Personal Information Protection Act. The normative literatures include:

ISO/IEC 27001:2005 Information technology − Security techniques − Information security management systems − Requirements. Its objective is to establish a model to establish, implement, operate, control, review, maintain, and improve the “Information security Management System”, which is also the item for assessment.

ISO/IEC 27002:2007 Information technology − Security techniques − Code of practice for information security management). Its objective is to establish the instructive guidelines and general rules for initiating, implementing, maintaining, and improving the information security in an organization. Its control objectives and control measures will be implemented so as to meet the requirements identified for risk assessment and become the instructive guidelines for developing the organization’s security standards and the practice of effective security management, assisting the establishment of mutual credibility for inter-organization activities.

ISO/IEC 27003:2010Information technology — Security techniques — Information security management system implementation guidance. It is mainly used to supplement section 4.2.1 of ISO/IEC 27001 for the establishment of ISMS during the planning phase, including the definition of scope and boundary of the

information security management system, the development of organization's information security policy, and the selection of a risk assessment method. In addition, the risk assessment is performed and the risk assessment results are then used for selecting the control measures.

ISO/IEC 27005:2008 Information technology − Security techniques − Information security risk management. It provides the instructive guidelines for the risk management of internal information security and supports the specific requirements for the CNS 27001 Information Security Management System. However, this standard does not provide any specific methodology for the risk management of information security. The organization can define its own risk management approach according to the scope of the information security management system, the scenario of risk management, or the category of the industry section.

ISO/IEC 27004:2009 Information technology — Security techniques — Information security management — Measurement. This standard provides guidance for the development and use of security control measures and their measurement methods, so as to evaluate the effectiveness of the control measures described in ISO/IEC 27001 after the implementation of ISMS, including the assessment of policy, information risk management, control objectives, processes, procedures, etc. It can assist the organization in identifying which measures require modification or strengthening. Meanwhile, it also emphasizes that there are no security control measures or measurement methods which can completely guarantee security.

ISO/IEC 27011:2008 Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002. Its architecture for the control measures are the same as

those specified in ISO/IEC 27002. Most of the control measures are referred from ISO/IEC 27002. The revised contents are focused on confidential agreements, including those between personnel and external parties, which mainly come from the requirements of protection of communication secrets. It also strengthens the protection of the physical environment and the telecommunications facilities and equipment. It is planned to add a strengthened security objective and to strengthen the management of the communications facility located at the third party. There are 13 newly added control measures in total and 26 amended control measures.

The domestic personal information protection law has been announced by the President on May 26th, 2010, and its title has been revised to the "Personal Information Protection Act", which will take effect on a date announced by the Executive Yuan. To be in line with the amended content in this Act, avoiding the infringement of personality rights, promoting the reasonable use of personal information, and implementing the Act smoothly, the detailed contents will be amended as follows:

The legal persons, groups, or individuals which are entrusted to collect, process, or use the personal information are regarded as the entrusted organizations within the scope of this Act, and the proper supervision obligation of the entrusted person is amended. In addition, the stipulations for the security maintenance measures, security maintenance items, and proper security measures are also amended.

Finally, according to the above research results, the conclusions and suggestions of this study are summarized as below:

According to the results of the factor analysis of the attitudes of the communication and broadcasting enterprises towards information security, it is found that the credibility of the business organization may be affected by the

“infringement of data protection”, “influence on business operations”, and “influence of compliance of the regulations”. The authority’s position is to focus on the maintenance of the rights of people, which is not relevant to individual communication and broadcasting enterprises’ reputations or images. Therefore, it is recommended for the asset groups owned by the Communication and broadcasting enterprises. It is classified as " core business", the " supporting business", and the "administrative business". According to the three aspects of "infringement of data protection", " influence on business operations" and " influence of compliance of the regulations", the security level of asset groups is divided into "high", "medium" and "fair". These shall be the key points upon which an enterprise must focus. Such an approach can relatively simplify the enterprise’s operation burdens.

Considering the analysis results of the characteristics of communication and broadcasting enterprises, the Type I and Type II telecommunication entries are subject to strict legal restrictions for the protection of communication secrets, so they have very high requirements of confidentiality. The wired broadcasting TV enterprises focus on the management of programs and advertisement, so they have extremely low requirements of information security management. According to the above method of enterprise security rating, it is suggested to categorize these requirements into the three levels of A, B, and C, and proper security protection criteria for the respective level shall be used.

The attitudes of communication and broadcasting enterprises towards information security shall not be any different, even if the number of employees or the amount of capital are different. They shall be valued equally. The infringement of personal privacy and data protection may affect the business operation and avoid to reduce the customer’s trust in the enterprise.

Communication and broadcasting enterprises should perform high-level risk

assessment based on the scope of the licensed business operations to investigate the asset groups required for the operations of the communication and broadcasting businesses. For large-scale organizations, it is allowed to divide the enterprise by business units or departments into three categories, the “core business”, the “supporting business”, and the “administrative business”, and then carry out the assessment of the asset security level. Finally all the assets security level of the asset groups are assessed. Whichever is highest as a basis for enterprise security rating, and then carry out the assessment of the assets security levels as “A”, “B”, or “C”. For example, the highest security level of asset groups to "high", its enterprise security level to "A" grade; such as the highest security level of asset groups of "medium", their enterprise security level to "B" grade; such as the highest security level of asset groups of "fair", their enterprise security level to "C" grade. It applies to different respective protection criteria.

For the revisions of the “Guidelines for the Information and Communications Security Management for Communication and Broadcasting Enterprises” and the “Operation Manuals for Information and Communications Security Management for Communication and Broadcasting Enterprises”, as well as an example draft of the implementation plan for the enterprises to adopt the information security management systems and operation items, please refer to the attachment of this research report.

1. 計畫緣起與目的

1.1.計畫緣起

通訊傳播事業擁有網路與系統等資源，因經營業務之需，留存大量用戶個人資料，常為不法人士覬覦之目標，囿於國內通訊傳播事業尚未全面導入資通安全管理機制，致使公司業務機密與用戶資料外洩事件頻傳，造成社會信用危機。

為防堵該等事件之發生，國家通訊傳播委員會(以下簡稱 NCC)已於 98 年 7 月 15 日首次公告「電信事業資訊安全管理作業要點」，提出「電信事業資訊安全管理手冊」供業者做為內部稽核之參考；另為因應政府於 99 年公告開放電信事業赴大陸地區投資電信業務之資通安全需求，NCC 參考國際標準化組織（International Organization for Standardization, ISO）於 97 年針對電信事業公布之資通安全管理實作指引(ISO/IEC 27011)，於 99 年 6 月 2 日修正公告「電信事業資訊通訊安全管理作業要點」，並修正「電信事業資通安全管理手冊」，以為業者提升資通安全之參考。

由於前開要點與手冊之內容，並未參酌 99 年 4 月 27 日立法院三讀通過之「個人資料保護法」，且主要規範對象為電信事業，傳播事業部分並未納入，顯見資通安全防護未臻於完備；此外，該要點與手冊對於風險管理程序與風險評估亦著墨甚少，實應考量納入 ISO/IEC 27005 標準，以確保通訊傳播事業之資通訊資產遭受攻擊時，具備足夠能力即時維護系統之正常運作與資料之合法存取與回復，因此「電信事業資訊安全管理作業要點」與「電信事業資通安全管理手冊」仍須持續參考 ISO/IEC 27000 系列相關標準與個人資料保護法，進行修正。

NCC 爰依據行政院 98 年 12 月 30 日院臺經字第 0980099463 號函核定之「行政院『塑造資安文化、推升資安產值』產業科技策略會議關鍵推動方案(99 年至 102 年)」，附錄「行動計畫工作要項與績效指標說明表」之「1-1 推動資訊安全管理系統計畫」，規劃「資訊安全管理系統研究計畫」（以下

簡稱本專案）。

1.2.研究目的

1.2.1. 引進國外最新資訊安全管理標準

我國採用 ISO/IEC 27001 與 27002 做為資訊安全管理之標準，並推廣於政府機關(構)。NCC 亦於 99 年參考 ISO/IEC 27011 部分控制措施，修正「電信事業資通安全管理手冊」，為使通訊傳播事業資通安全管理之規範更臻完備，仍須參考 ISO/IEC 27003、27004、27005 及 27011 等標準最新版本，檢討「電信事業資通安全管理手冊」，以強化通訊傳播事業導入資通安全管理機制之查核內容。

1.2.2. 督促通訊傳播事業導入資通安全管理機制

通訊傳播事業存有大量消費者個人資料，已經成為不法集團窺伺與竊取之目標，使民眾之財產與生活安全受到嚴重威脅，社會之人際信任感亦面臨瓦解，為有效提升通訊傳播事業之資料、系統、設備及網路的安全，亟須督促該等事業全面導入資通安全管理機制。

1.2.3. 確保通訊傳播事業之消費者個人資料安全

配合「個人資料保護法」通過，保障消費者個人資料無洩漏或被竊取之虞，以及避免通訊傳播事業因巨額的賠償金額而倒閉，導致通訊傳播網路無法持續運作。因此，參考「個人資料保護法」，全面要求通訊傳播事業導入資通安全管理機制，以有效強化該等事業資訊與通訊內容之安全維護品質，已是勢在必行之作為。

1.2.4. 完備通訊傳播事業資通安全管理規範對象

NCC 現行之資通安全管理相關規範，為「電信事業資訊通訊安全管理作業要點」與「電信事業資通安全管理手冊」，目前適用之對象僅限於電信事業，為避免個人資料之安全維護出現漏洞，亦須針對廣電事業之資通安

全管理相關規範加以補強，以完備國內通訊傳播事業之資通安全管理規範。

1.3.報告研究範圍

- 參考 ISO/IEC 27003 及 27005，研提適合通訊傳播事業導入資通安全管理機制之實施程序與風險評估模式。
- 參考 ISO/IEC 27004，研提適合通訊傳播事業評估導入資通安全管理之有效性量測方法與量測措施。
- 針對通訊傳播事業之經營規模（如資本額、員工數等）與業務特性（如核心業務）等因素，提出分析報告並研提適合之資通安全管理機制影響構面、評估等級與實施範圍。
- 研析個人資料保護法與本專案之關聯性，並據以強化資通安全管理手冊之控制項目。
- 研提通訊傳播事業導入資通安全管理機制之實施計畫參考範本。
- 參考 ISO/IEC 27001、27002、27011、「電信事業資訊通訊安全管理作業要點」及「電信事業資通安全管理手冊」，研提適用於通訊與傳播事業之「通訊傳播事業資通安全管理作業要點」建議草案及「通訊傳播事業資通安全管理手冊」建議版本。
- 舉辦 6 場資通安全管理機制座談會(電信事業 4 場、廣電事業 2 場)與 1 場成果發表會，邀請具資通安全領域專業之專家學者參與，會後須提出會議紀錄，總計 7 份。

2. 研究方法概述

依據前述研究範圍，本研究擬定之研究構想如下：

- 藉由個案研究，遴選優質之通訊傳播業者進行訪談，以瞭解業者導入資訊安全管理系統(Information Security Management System, ISMS)之成功經驗與窒礙因素，以進行理論發展與模式設立。
- 再根據發展之模式實施問卷調查，進行驗證性因素分析，以瞭解影響企業建置 ISMS 之關鍵因素，作為修訂資通安全管理要點與管理手冊之參考。
- 另針對通訊傳播事業進行普查，利用重要度績效分析法，以瞭解業者目前之資通安全相關控制措施執行情形，找出優先改善項目。
- 分析 ISO/IEC 27000 系列標準，研擬適當之建議，以協助業者強化資通安全防護工作。
- 分析個人資料保護法及施行細則內容，研擬適當之建議，以協助業者強化個人資料保護工作。

研究構想結合工作項目，區分為文獻研究、個案研究及問卷調查三階段，依據工作進行之時間順序，分別採用不同之研究方法，詳見表 1 所示：

表1　研究方法與專案進行步驟

研究方法	RFP 工作項目	工作內容
文獻研究法	1-1 1-2 1-4	● 參考 ISO/IEC 27003 與 27005，研提適合通訊傳播事業導入資通安全管理機制之實施程序與風險評估模式 ● 參考 ISO/IEC 27004，研提適合通訊傳播事業評估導入資通安全管理之有效性量測方法與量測措施

研究方法	RFP 工作項目	工作內容
		● 參考個人資料保護法及施行細則內容，研擬適當之建議，以協助業者強化個人資料保護工作。
個案研究法	1-3	針對通訊傳播事業之經營規模(如資本額、員工數等)與業務特性(如核心業務)等因素，探討目的事業對於資訊安全管理之重視程度與窒礙因素
問卷調查法	1-3	針對通訊傳播事業之經營提出分析報告並研提適合之資通安全管理機制影響構面、評估等級及實施範圍

資料來源：本計畫自行整理

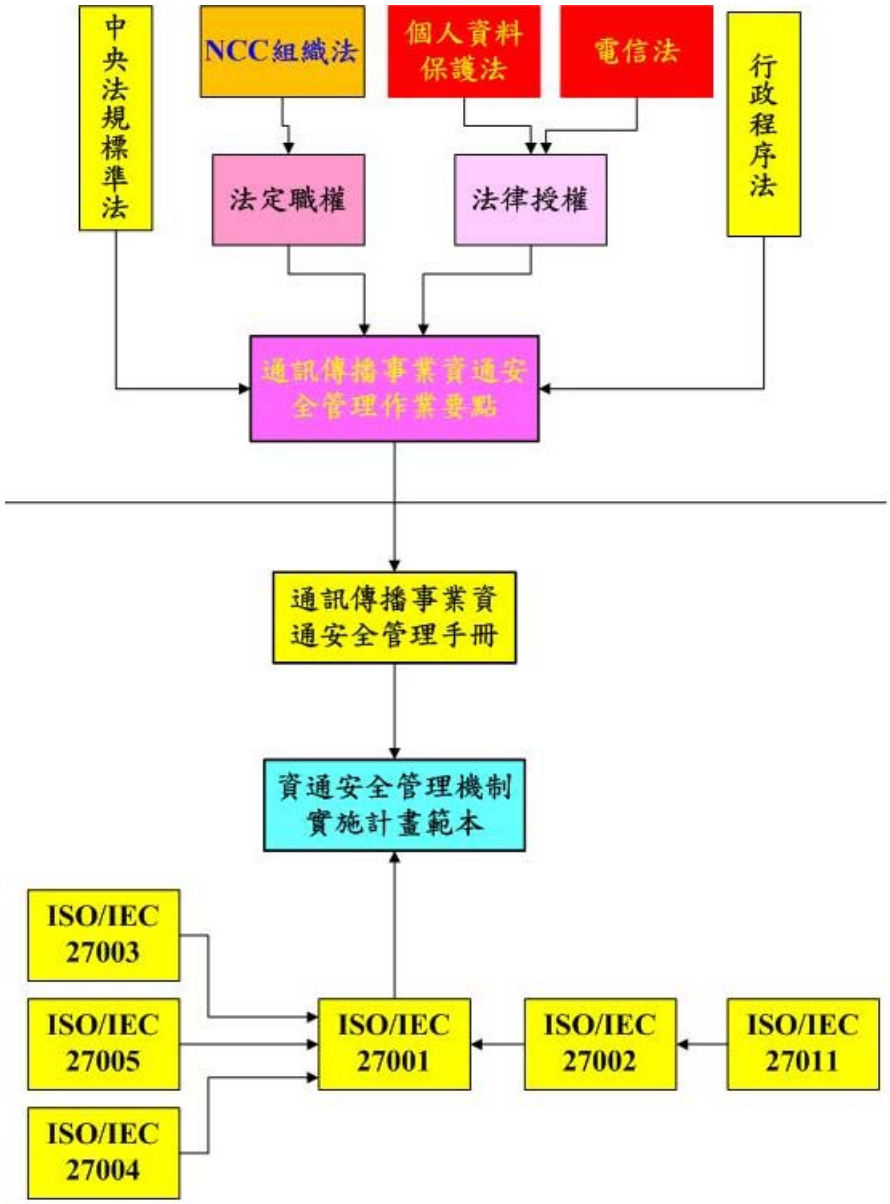
以下將各階段之研究方法摘述如後：

2.1.1. 文獻研究法

本階段研究依據工作項目主要應分析 ISO/IEC 27003、27004、27005、27011、「電信事業資訊通訊安全管理作業要點」、「電信事業資通安全管理手冊」及個人資料保護法、施行細則等，據以研提適合我國通訊傳播事業所需之相關資安文件內容。

本計畫最終之產出為研提適用於「通訊傳播事業資通安全管理作業要點」與「通訊傳播事業資通安全管理手冊」，原要點係依據 NCC 組織法之法定職務進行公告，於電信法修訂草案未通過前，暫以行政規則位階，採用要點方式指導通訊傳播事業強化資通安全與個資保護作為。

有關「通訊傳播事業資通安全管理手冊」之內容，主要係依據 ISO/IEC 27001 之要求事項，於導入程序部分，宜藉 ISO/IEC 27003 實作指引、ISO/IEC 27005 風險評鑑及 ISO/IEC 27004 測量方法等予以強化其有效性，並研提通訊傳播事業導入資通安全管理機制之實施計畫參考範本。



資料來源：本計畫自行整理

圖1　文獻研究架構圖

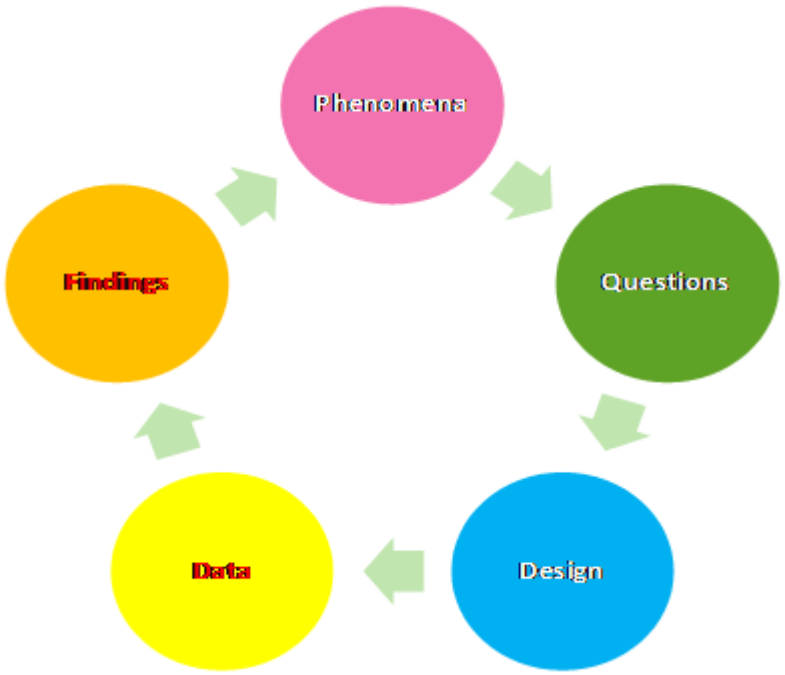
2.1.2. 質性(個案)研究法

本計畫試圖將組織導入 ISMS 的過程，詮釋為建構風險意識的過程，探討組織在建置 ISMS 之過程，組織內部如何建構成員整體之風險意識與

資安文化，並影響最後建置結果，擬採用質性(個案)研究法，區分為五個步驟：

- 發掘現象
- 擬定命題
- 研究設計
- 資料蒐集
- 研究發現

著重於現象之解釋與發現之實證。

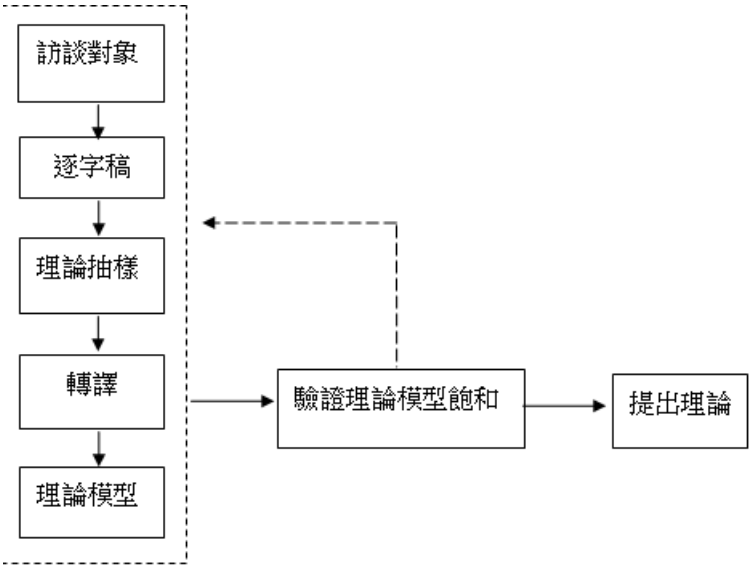


資料來源：[23]

圖2　個案研究之程序

另有關蒐集資料之分析，將採用紮根理論，探討個案如何(How)與為

什麼(Why)的研究議題，以符合本計畫探索個案的策略。紮根理論能經由訪談取得受訪者深層的感受與處境，進行理論的建構[23]，從訪談過程中與受訪者進行心智模式上的互動，貼近個案本身之議題，勾勒出組織整體導入資訊安全標準的經過，並發掘新的現象，使之抽象化以利於探討抽象名詞的關係，最後並進行多個跨個案的比較。



資料來源：[23]

圖3　紮根理論研究流程圖

2.1.3. 問卷調查法

本計畫採驗證式問卷，藉以瞭解通訊傳播事業之經營規模(如資本額、員工數等)與業務特性(如核心業務)等因素，探討目的事業對於資訊安全管理之重視程度與窒礙因素。

2.1.3.1. 問卷設計

問卷調查是目前量化研究中最廣泛採取之調查方式(董和昇，2006)，故本計畫設計符合研究目的之調查問卷，並採取普查方式研究樣本，透過樣本中問卷施測者之填答，以完成問卷所設計之調查項目；最後，由統計分析得出問卷調查結果。問卷調查乃嚴格遵循機率與統計原理，故研究調

查之方式較具科學性與客觀性，並便於本計畫操作。

然而，問卷調查之結果將受到其樣本選擇、問卷設計及統計方法之影響故本計畫問卷採用李克特量表(Likert)，要求填答者表明對某一表述贊成或否定，並將贊成度分為若干類，範圍從非常贊成到非常不贊成，中間為中性類，由於類型增多，填答者在態度上的差別就能充分表現出來，以利於填答者感受度之量測(邱皓政，2009)。

2.1.3.2. 檢驗方法

問卷調查乃受訪者依自身所處情境與實際感受所形成的答案依序回答問題，在每位受訪者皆被要求回答相同問題的情況下，問卷能有效地提供量化分析所需之樣本。

林生傳(2003)依研究對象之抽樣與否，可將問卷調查的類型分成普查(Censuses)與抽樣調查(Sample Survey)，針對所研究之母體做全面之調查就是普查，如果客觀條件允許的話，普查是最周延且最正確的方法。

若不針對母體做全面性之調查，而只從母體中抽取具代表性者進行調查，稱為樣本調查，如果抽樣程序合適，蒐集資料方法正確，獲得的資料與研究該領域的重要問題相關，樣本調查亦不失其價值。

一般而言，有效樣本愈大，統計準確度愈高；有效樣本愈小，則準確度愈低。理想的狀況下，應至少達到 n 大於 30 以上，符合統計學之最小限度要求，調查實務中通常要求回覆之樣本數應達 100~200 份，有利於信度與效度之檢驗，以求呈現母體真實原貌。

Bell [4]為確認問卷蒐集之資料能精確回答研究問題，並達到研究目標，需將問卷回覆率、信度及效度等三者加以最大化(Oppenheim, 2000)。以下將本計畫擬採取之作法摘述如后：

2.1.3.2.1. 問卷回覆率

依據採購評選會議中委員之要求，本案之問卷調查回覆之樣本數應至少達 200 份以上，並同意以 NCC 之名義製作問卷，要求電信、傳播業者填答。

本問卷調查的研究母體包含現有已核准之第一類、第二類電信及傳播事業，根據 NCC 網站公告，目前共有 916 家業者(937 張執照)，若暫估回覆率以 20%計，則至少應發出 1000 份問卷，實已超過母體總數，因此，為達成決議事項之要求，採用普查方式，針對 916 家業者全數寄發自填式問卷，而不採用抽樣調查，應是最周延且最正確的調查方法。

由 NCC 寄發公文，提供問卷下載聯結網址，業者填寫完畢後，以紙本郵寄、傳真或電子郵件等方式回覆，除此之外，亦配合本計畫所辦理之資通安全管理機制座談會，於現場發放紙本問卷，受訪業者填寫完畢後以郵寄方式回收，以提升問卷回覆率。

調查期間自 100 年 5 月 16 日~100 年 6 月 10 日止，合計回收有效問卷計有 149 家廠商(211 張執照)。

2.1.3.2.2. 信度檢驗

信度(Reliability)：就是可靠的意思，亦即一個測量工具(例如問卷或量表)每次施測都會產生相似的結果，若信度高，施測後的結果比較能被研究者所信服。而 α 係數(Cronbach α)為目前社會科學研究最常使用的信度，量測一組同義或平行測驗總和的信度，一旦尺度中的所有項目都在反映相同的特質，則各項目之間應具有真實的相關存在(薄喬萍，2010)。

本計畫著重於一致性，故採用「內在一致信度」，以符合本計畫之性質，針對通訊傳播事業之經營規模(如資本額、員工數等)與業務特性(如核心業務)等因素，提出分析報告並研提適合之資通安全管理機制影響構面、評估等級與實施範圍，內在一致性估計值(α 係數)，預期應達 0.70 以上，以符合信度之要求，因當信度係數值愈接近 1，表示量表或測驗的信度愈高

(Babbie, 2004)，詳見表 2 所示。

表2　可信度高低與 Cronbach α係數之對照表

可信度	Cronbach α係數
不可信	Cronbach α係數＜0.3
勉強可信	0.3≦Cronbach α係數＜0.4
可信	0.4≦Cronbach α係數＜0.5
很可信（最常見）	0.5≦Cronbach α係數＜0.7
很可信（次常見）	0.7≦Cronbach α係數＜0.9
十分可信	0.9≦Cronbach α係數

資料來源：(薄喬萍，2010)

2.1.3.2.3. 效度檢驗

效度(Validity）即有效性，它是指測量工具或手段能夠準確測出所需測量事物的程度。本計畫採用構念效度，用以檢驗問卷調查之結果。

建構效度或構念效度(Construct Validity)指問卷能測量到理論上的構念或特質之程度，分為收斂效度與區別效度。而檢測問卷是否具備建構效度，最常使用之方法為因素分析法。同一因素構面中，若各題目之因素負荷量(Factor Loading)愈大，則愈具備「收斂效度」。若問卷題目在非所屬因素構面中，其因素負荷量愈小，則愈具備「區別效度」(邱皓政，2009)，詳見表 3 所示。

表3　樣本與因素負荷量選取標準值

樣本大小	因素負荷量選取標準值
50	0.750
60	0.700
70	0.650

樣本大小	因素負荷量選取標準值
85	0.600
100	0.550
120	0.500
150	0.450
200	0.400
250	0.350
350	0.300

資料來源：(吳明隆，2010)

另由 KMO(取樣適切性量數)統計量數之判斷準則，當 KMO 值於 0.7 至 0.8 時，其因素分析的適切性為適中，詳見表 4 所示。

表4　KMO 與 Bartlett's 球形檢定

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.726
Bartlett's Test of Sphericity	Approx. Chi-Square	19377.570
	df	3240
	Sig.	0.000

資料來源：本計畫自行整理

3. 專案進行步驟與結果

文獻探討之目的，主要係參考 ISO/IEC 27003 與 27005，研提適合通訊傳播事業導入資通安全管理機制之實施程序與風險評估模式。另參考 ISO/IEC 27004，研提適合通訊傳播事業評估導入資通安全管理之有效性量測方法與量測措施。規劃符合國內通訊傳播事業需求及民眾期待之資訊安全管理要點與手冊。摘述如后：

3.1.通訊傳播事業特性之分析

3.1.1. 用詞定義

依據通訊傳播基本法第 2 條 用詞定義如下：

- 通訊傳播：指以有線、無線、衛星或其他電子傳輸設施傳送聲音、影像、文字或數據者。
- 通訊傳播事業：指經營通訊傳播業務者。

為有效辦理通訊傳播之管理事項，政府應設通訊傳播委員會，依法獨立行使職權。另國家通訊傳播整體資源之規劃及產業之輔導、獎勵，由行政院所屬機關依法辦理之。故就政府機關職權之劃分，通傳會負責通訊傳播事業之管理，行政院新聞局負責無線廣播電視事業、廣播電視節目供應事業(含錄影節目帶事業)、衛星廣播電視事業以及有線廣播電視事業之政策、輔導及獎勵等事項。

3.1.2. 業務區分

通訊傳播事業依其業務屬性，區分為電信及傳播業務，詳見表 5 所示。

表5　通訊傳播事業業務區分表

區分	業務項目	擁有機線設備	管理重點	處罰規定
第一類電信	固定通信網路業務 行動通信網路業務 衛星通信網路業務	擁有極大量機線設備	電信建設與管理 電信設備之維護與管理 電信監理 專業人員管理 客戶管理	盜用他人電信設備通信者之刑責 侵犯通信秘密之刑責 行政罰則
第二類電信	數據交換通信服務 網際網路接取服務 非E·164 網路電話服務 E·164 網路電話服務 公司內部網路通信服務 語音會議服務 存取網路服務 視訊會議服務	擁有機線設備	電信設備之維護與管理 專業人員管理 客戶管理	盜用他人電信設備通信者之刑責 侵犯通信秘密之刑責 行政罰則
第二類電信	語音單純轉售服務 批發轉售服務 頻寬轉售服務 存轉網路服務 付費語音資訊服務	無	客戶管理	侵犯通信秘密之刑責 行政罰則

區分	業務項目	擁有機線設備	管理重點	處罰規定
	行動轉售服務 行動轉售及加值服務			
傳播事業	有線廣播電視 廣播電視 衛星廣播電視	擁有極大量機線設備	營運管理 節目管理 廣告管理 專業人員管理	行政罰則
	廣播電視節目供應事業	無	節目管理 廣告管理	行政罰則

資料來源：本計畫自行整理

電信事業依據電信法區分為第一類電信與第二類電信業務，

第一類電信業務有 3 項：分別為固定通信網路業務、行動通信網路業務及衛星通信網路業務，擁有極大量之電信機線設備，為維持通訊服務品質，對於設備之可用性要求極高，依據電信法之規定，著重點於電信建設與管理、電信設備之維護與管理、電信監理及專業人員管理，並對於盜用他人電信設備通信者及侵犯通信秘密者訂有極重之刑責，及相關之行政罰則，如依據電信法第 6 條，電信事業及專用電信處理之通信，他人不得盜接、盜錄或以其他非法之方法侵犯其秘密。電信事業應採適當並必要之措施，以保障其處理通信之秘密。另依據第 7 條，電信事業或其服務人員對於電信之有無及其內容，應嚴守秘密，退職人員，亦同。顯見對於機密性之維護要相當重視。

人員管理部分第一類電信事業應遴用符合規定資格之高級電信工程人員，負責及監督電信設備之施工、維護及運用。

第二類電信業務項目雖然眾多，但可依其是否具備電信機線設備，區分為具備機線設備者，如數據交換通信服務及網際網路接取服務等八項，對於設備之可用性要求與第一類電信雷同，管理上著重於電信設備之維護與管理，第二類電信事業亦應按其電信設備設置情形，依規定遴用該人員為之。對於機密性之要求與第一類電信亦雷同。

第二類電信另有毋需具備機線設備，如：語音單純轉售服務及批發轉售服務等 7 項，管理重點在於客戶管理，僅有支援業務所需之資訊處理設施，對於可用性之要求極低，對於機密性之要求則視客戶數量之多寡而定。

傳播事業區分為：有線廣播電視、廣播電視及衛星廣播電視 3 項，其所擁有之廣播機線設備特性與第一類電信雷同，具體之差別在於廣播系統係單向傳輸，而通訊系統係雙向傳輸，但對於可用性之要求應是一致的。著重於營運管理、節目管理、廣告管理及專業人員管理，但是廣播係對公眾傳送，故不涉及通信秘密之保護，沒有刑責之規範，僅有行政罰則，違反法令規定之處分較輕，故對於機密性之要求較低。

依廣播電視法第 50 條第 1 項規定，另訂定廣播電視節目供應事業管理規則，將廣播電視節目供應事業分為下列 3 類：

- 廣播電視節目業

  – 廣播節目製作業

    為無線廣播電臺或其客戶策劃、製作節目或提供製作廣播節目之設備及場地之獨資、合夥、公司或其他法人組織。

  – 電視節目製作業

    為無線電視電臺、有線廣播電視系統經營者、有線電視節目播送系統、衛星廣播電視事業或其客戶策劃、製作節目或提供製作電視節目之設備及場地之獨資、合夥、公司或其他法人組織。

– 廣播電視節目發行業

為無線廣播、電視電臺、有線廣播電視系統經營者、有線電視節目播送系統或衛星廣播電視事業提供節目之獨資、合夥、公司或其他法人組織。

- 廣播電視廣告業

為無線廣播、電視電臺、有線廣播電視系統經營者、有線電視節目播送系統、衛星廣播電視事業或其客戶策劃、製作或託播廣告之獨資、合夥、公司或其他法人組織。

- 錄影節目帶業

自行製作或取得權利人授權轉錄，並供應給錄影節目帶出租、買賣或播映業獨資、合夥、公司或其他法人組織。

上述之節目或廣告業，其管理重點在於完整性之維持，如：電視節目製作業、廣播電視節目發行業及廣播電視廣告業，供應有線廣播電視系統經營者及有線電視節目播送系統之節目、廣告及其節目表，應自播送日起保存 15 日備查。違反規定者僅有行政罰則，而未有相關之刑責處分。

廣播、電視節目分為以下 4 類：

- 新聞及政令宣導節目
- 教育文化節目
- 公共服務節目
- 大眾娛樂節目
- 主管機關應依電視節目內容予以分級，限制觀看之年齡、條件，電臺應將其節目時間表，事前檢送主管機關核備；變更節目時亦同。就資訊安全之觀點，幾乎不涉及機密及可用性之要求，雖然看似對於完整性有相

關之規定，但就資訊安全管理之立場，恐無可著墨之處，應尊重主管機關業管單位之想法。

- 綜上所述，通訊(電信)事業因涉及通信秘密之保護，訂有相關刑責，對於機密性之要求相當高，且有大量之電信機線設備，為維持通訊服務水準，故對於可用性之要求亦相當高，少部分第二類電信不具備機線設備，單純轉售服務者，對於資訊安全之要求亦相對降低。
- 傳播事業其所擁有之廣播機線設備特性與第一類電信雷同，對於可用性之要求不分軒輊，但因係對於公眾進行傳播，故對於機密性之要求極低。
- 廣播電視節目供應事業較為特殊，重點在於節目內容之分級與限制觀看之年齡與時段，或是有關新聞報導之中立客觀，幾乎不涉及機密性及可用性之要求，就資訊安全管理之觀點，其風險等級較低，對於營運安全之改善效益有限。
- 後續規劃將以資訊安全觀點，以不同之安全領域、安全目標及控制措施，考量上述之目的事業，對於資訊安全管理之機密、完整性及可用性之要求差異，參考 CNS/ISO/IEC 27002 及 27011 之內容，建議適用之安全控制措施。

3.2. ISMS 國際標準之發展

國際標準組織已將「資訊安全管理系統」標準統整為 ISO/IEC 27000 系列，並於 2007 年 7 月，將 ISO/IEC 17799:2005，正式更名為 ISO/IEC 27002，以符合 ISO 國際標準之命名原則。

目前已編訂的 ISO/IEC 27000 系列標準之編號、用途說明及發展時程詳見表 6 所示。

表6　ISO/IEC 27000 系列標準說明表

項次	ISO/IEC 27000 系列號碼	定位用途說明	公布日期
1	ISO/IEC 27001	ISMS 資安管理系統要求事項	2005 年
2	ISO/IEC 27002	ISMS 作業規範，原名 ISO 17799	2007 年
3	ISO/IEC 27003	ISMS 導入指引	2010 年
4	ISO/IEC 27004	資安管理量測標準	2009 年
5	ISO/IEC 27005	風險管理指引	2008 年
6	ISO/IEC 27006	國際認證機構對「驗證機構」之規範	2007 年
7	ISO/IEC 27007	針對 ISMS 稽核的參考指引	Working Draft development stage
8	ISO/IEC 27011	針對通訊產業資安認證導入指引	2008 年

資料來源：本計畫自行整理

整個 ISO/IEC 27000 系列標準，原適用範圍涵蓋所有型式的組織(例如：商業企業、政府機構及非營利組織)等，當然也包含本次研究之目的事業：通訊傳播事業，但也陸續針對特定的「行業別」提出相對建議，例如：ISO/IEC 27799 就是針對「醫療業」的資訊安全管理指引，ISO/IEC 27011 則是針對「電信業」的資訊安全管理指引。以下僅針對已頒布且與本計畫相關之標準內容加以摘述如後：

3.2.1. ISO/IEC 27001:2005

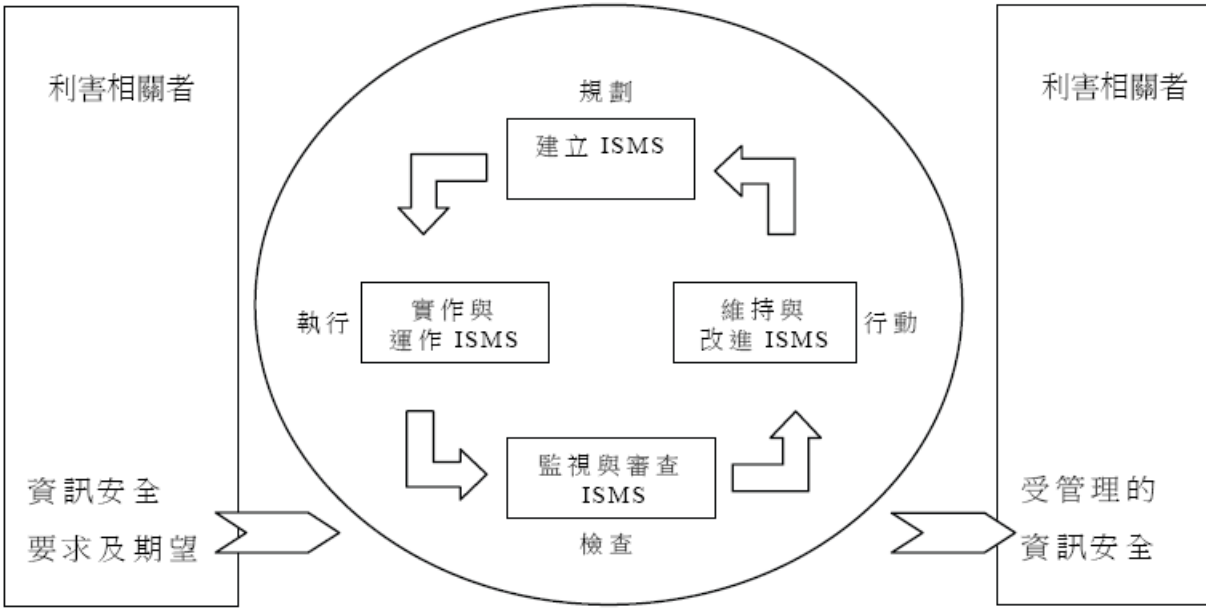
ISO/IEC 27001:2005 資訊安全管理要求事項(Information technology − Security techniques − Information security management systems − Requirements)的目的是要制定一個用以建立、實作、運作、監控、審查、維持及改進「資訊安全管理系統」之模型。機關(構)的 ISMS 之設計與實作受其需求與目標、安全要求、所採用的過程及組織之規模與架構所影響。

ISO/IEC 27001 標準內所展現之資訊安全管理的過程導向(作法)，鼓勵

其使用者強調下列事項之重要性：

- 瞭解組織資訊安全要求，以及瞭解建立資訊安全之政策與目標的需求。
- 在組織整體營運風險之全景(Context)中，實作與運作各項控制措施以管理組織的資訊安全風險。
- 監控與審查 ISMS 之績效與有效性。
- 基於客觀的測量以持續改進。

ISO/IEC 27001 採用「規劃—執行—檢查—行動(Plan-Do-Check-Act, PDCA) 」過程模型，適用於建置所有 ISMS 過程，詳見圖 4 所示。PDCA 模型的採用亦將反映經濟合作暨發展組織(Organization for Economic Co-operation and Development, OECD)指導綱要內所宣告之治理資訊系統與網路安全的原則。[29]



資料來源：CNS 27001

圖4　適用於 ISMS 過程之 PDCA 模型

PCDA 模型中之各過程工作內容，詳見表 7 所示。

表7　PCDA 模型中之各過程工作內容

項目	內容
規劃 （建立ISMS）	建立與管理風險，以及改進資訊安全相關之ISMS 政策、目標、過程及程序，以產生與組織整體政策、目標一致之結果 ● 界定ISMS 之範圍與邊界 ● 界定組織的風險評鑑作法 ● 選擇各項風險處理的控制目標與控制措施 參閱ISO/IEC 27003、27005內容
執行 （實作與運作ISMS）	實作與運作ISMS的政策、控制措施、過程及程序 ● 界定如何量測所選擇的控制措施或控制措施群的有效性，並規定如何使用這些量測去評鑑控制措施的有效性，以產生可比較與可再產生的結果 參閱ISO/IEC 27004內容
檢查 （監視與審查ISMS）	依據ISMS 政策、目標及實際經驗，評鑑及在適用時測量過程績效，並將結果回報給管理階層審查 ● 定期審查ISMS 的有效性(包括是否符合ISMS 政策與目標，以及安全控制措施的審查)，並將安全稽核、事故、有效性測量，以及來自所有利害相關者之建議與回饋之結果納入考量
行動 （維持與改進ISMS）	基於ISMS 內部稽核與管理階層審查結果或其他相關資訊採取矯正與預防措施，以達成ISMS 的持續改進

資料來源：本計畫自行整理

本標準涵蓋所有形式的組織(例如：商業企業、政府機構及非營利組織），但將受驗證組織視為獨立且唯一的，並未有經濟規模之考量，對於政府機關之應用需考量成本因素。

本標準規定在組織整體營運風險全景內建立、實作、運作、監視、審查、維持及改進已文件化之 ISMS 的要求。其規定依據個別組織或部分單位之需求量身打造安全控制措施的實作要求。

ISMS 係被設計以確保選擇適切與相稱的安全控制措施，以保護資訊

資產並賦予利害相關者信賴。本標準敘述之要求為一般性的，且適用所有組織，與其形式、規模大小及性質無關。在組織宣稱符合本標準時，排除本標準第 4 節至第 8 節所規定之任何要求，均不被接受。其內容涵蓋 ISO/IEC 27002 之安全控制措施。

若發現某些控制措施為滿足風險接受準則而有必要排除者，需加以衡量並提供相關風險已被可歸責人員接受之證據。當排除任何控制措施時，除非不影響該組織提供以符合由風險評鑑及適用之法規要求所決定之安全要求的資訊安全之能力及/或責任，否則宣告符合本標準時，均不被接受。

本標準之使用者需負責正確使用，符合標準並無法豁免法律義務。

3.2.2. ISO/IEC 27002:2007

ISO/IEC 27002:2007 資訊安全管理作業規範(Information technology − Security techniques − Code of practice forinformation security management)，其目的是要建立一套用以起始、實作、維持及改進組織內之資訊安全管理指導綱要與一般原則。其控制目標與控制措施將被實作以滿足風險評鑑所識別的要求而設，可作為發展組織安全標準與有效安全管理實務的作業指導綱要，協助建立組織間活動之信賴。

ISO/IEC 27002 的資訊安全控制領域內容包含如下所示：

- 「安全政策」(Security Policy)
- 「資訊安全組織」(Organizing Information Security)
- 「資產管理」(Asset Management)
- 「人員安全」(Human Resources Security)
- 「實體與環境安全」(Physical and Environmental Security)
- 「通信與作業管理」(Communications and Operations Management)

- 「存取控制」(Access Control)
- 「系統獲得、開發與維護」(Information Systems Acquisition, Development and Maintenance)
- 「資訊安全事故管理」(Information Security Incident Management)
- 「營運持續管理」(Business Continuity Management)
- 「符合性」(Compliance)

上述共有 11 個安全控制領域、39 個控制目標及 133 個控制措施。此標準建議採用過程導向(process approach)的方法論，以 PDCA 模式，即規劃(Plan)、執行(Do)、檢查(Check)及行動(Act)，應用於組織的資訊安全工作，以建立、實施、操作、監督、維護並持續改進組織的資訊作業安全，以管理角度出發，建立與維護組織的資訊安全管理系統。有關 ISO/IEC 27002 架構，詳見圖 5 所示。



資料來源：BSI 訓練教材

圖5　ISO/IEC 27002 架構圖

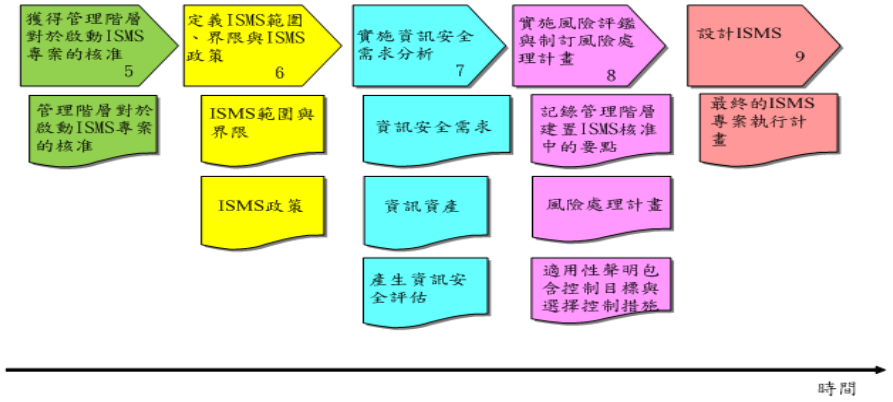
3.2.3. ISO/IEC 27003:2010

ISO/IEC 27003:2010 資訊科技－安全技術－資訊安全管理系統實施指

引(Information technology — Security techniques — Information security management system implementation guidance)主要在於補充說明 ISO/IEC 27001 規劃階段之 4.2.1 建立 ISMS，包含定義資訊安全管理系統之範圍與邊界、發展組織資安政策、選定風險評鑑的方法，並進行風險評鑑工作，再依據風險評鑑之結果選擇控制措施。

根據以上 ISO/IEC 27001 之要求事項，本項國際標準將 ISMS 專案區分為五個階段，詳見圖 6 所示，依序為：

- 獲得管理階層的承諾，啟動 ISMS 專案
- 定義 ISMS 的範圍與政策
- 進行資訊安全需求分析
- 進行風險評鑑與風險處理規劃
- 設計 ISMS

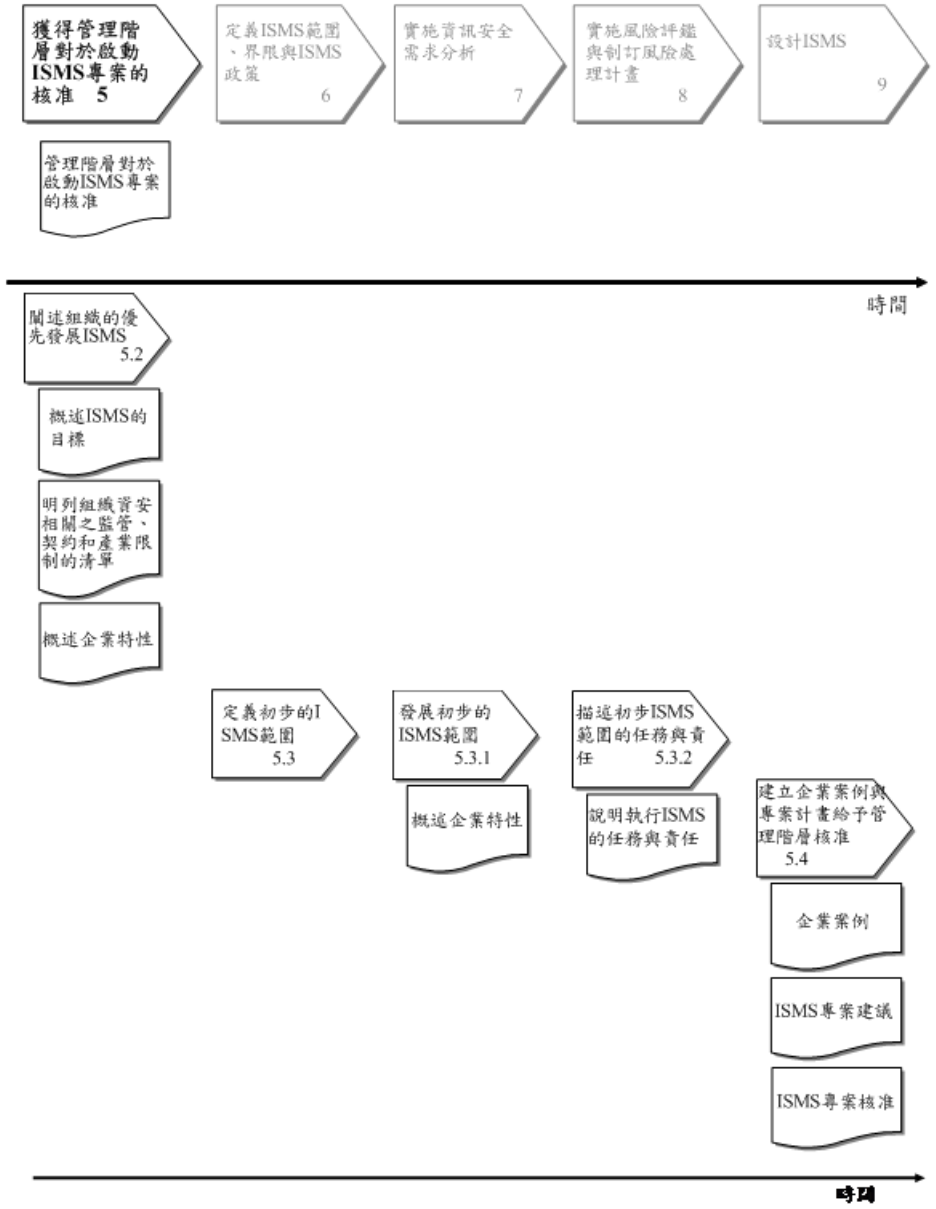


資料來源：ISO/IEC 27003：2010

圖6　ISMS 專案階段區分

- 上圖主要依據專案進行之時間順序，分階段說明應有之活動與產生之文件，摘述如后：

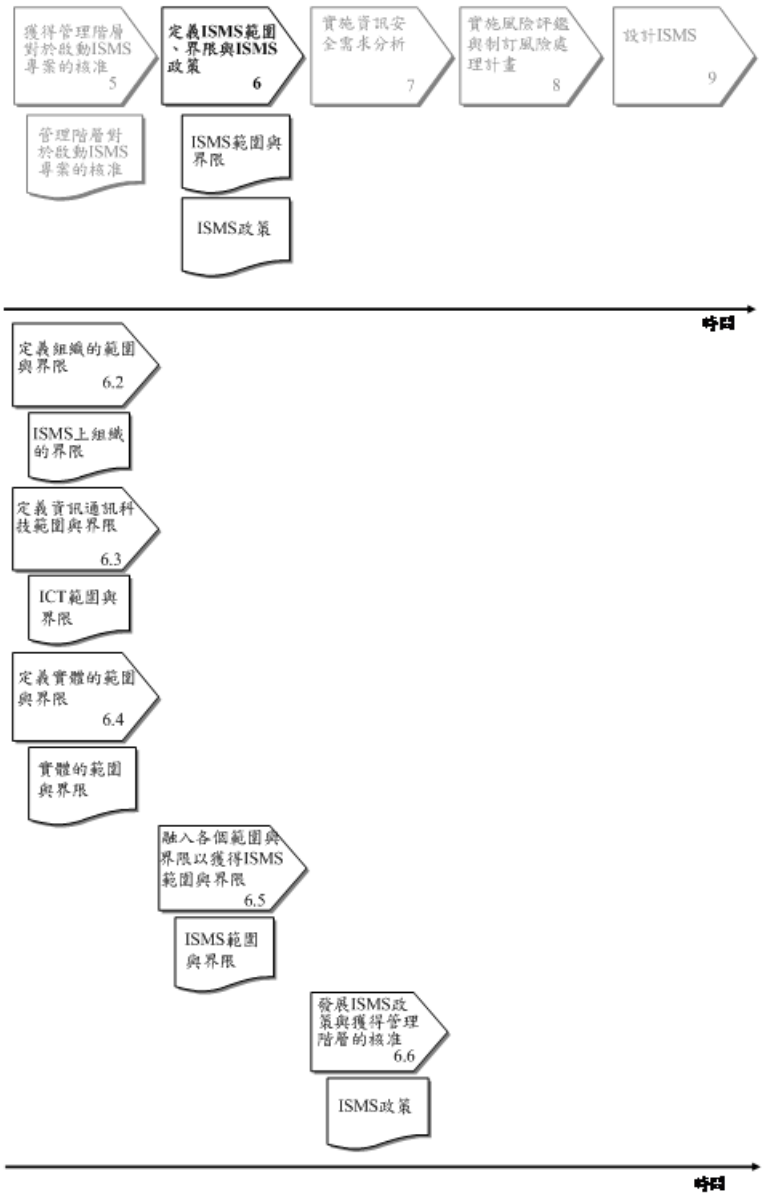
3.2.3.1. 獲得管理階層的承諾，啟動 ISMS 專案



資料來源：ISO/IEC 27003：2010

圖7　獲得管理階層的承諾，啟動 ISMS 專案階段

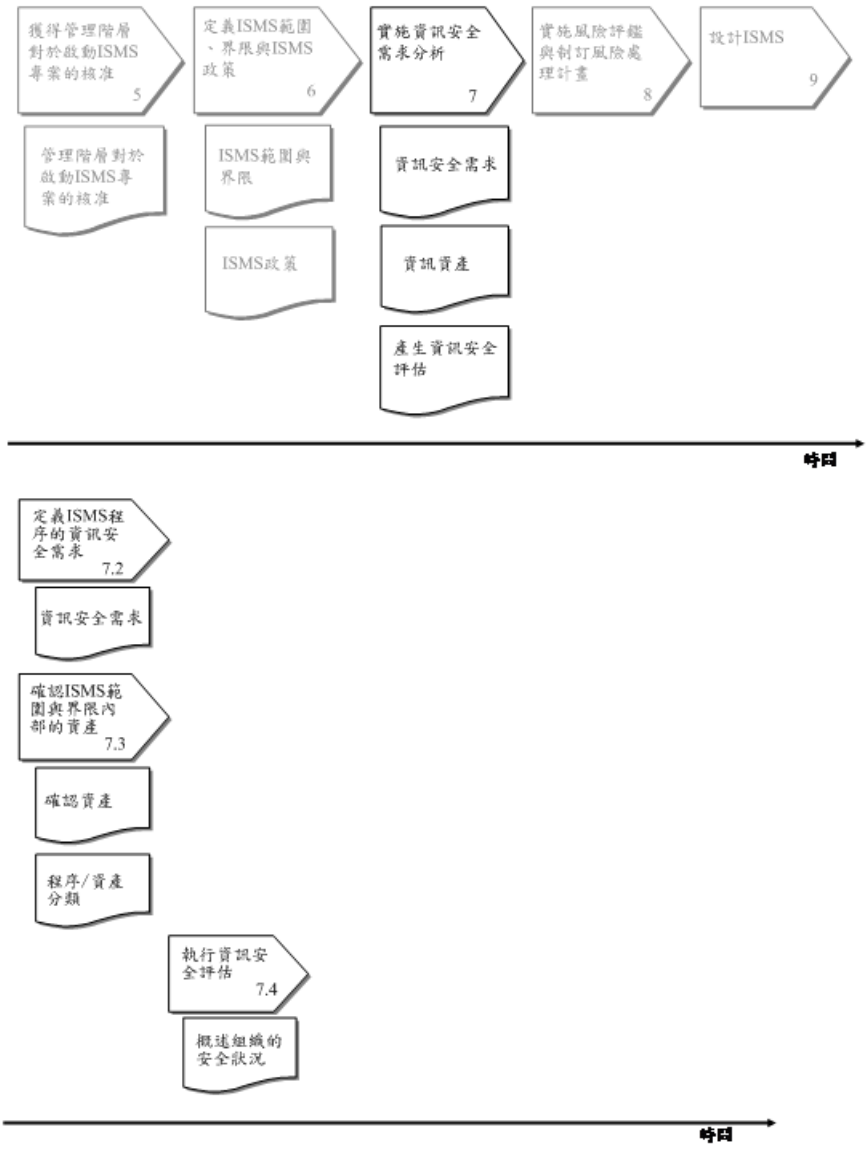
3.2.3.2. 定義 ISMS 的範圍與政策



資料來源：ISO/IEC 27003：2010

圖8　定義 ISMS 的範圍與政策階段

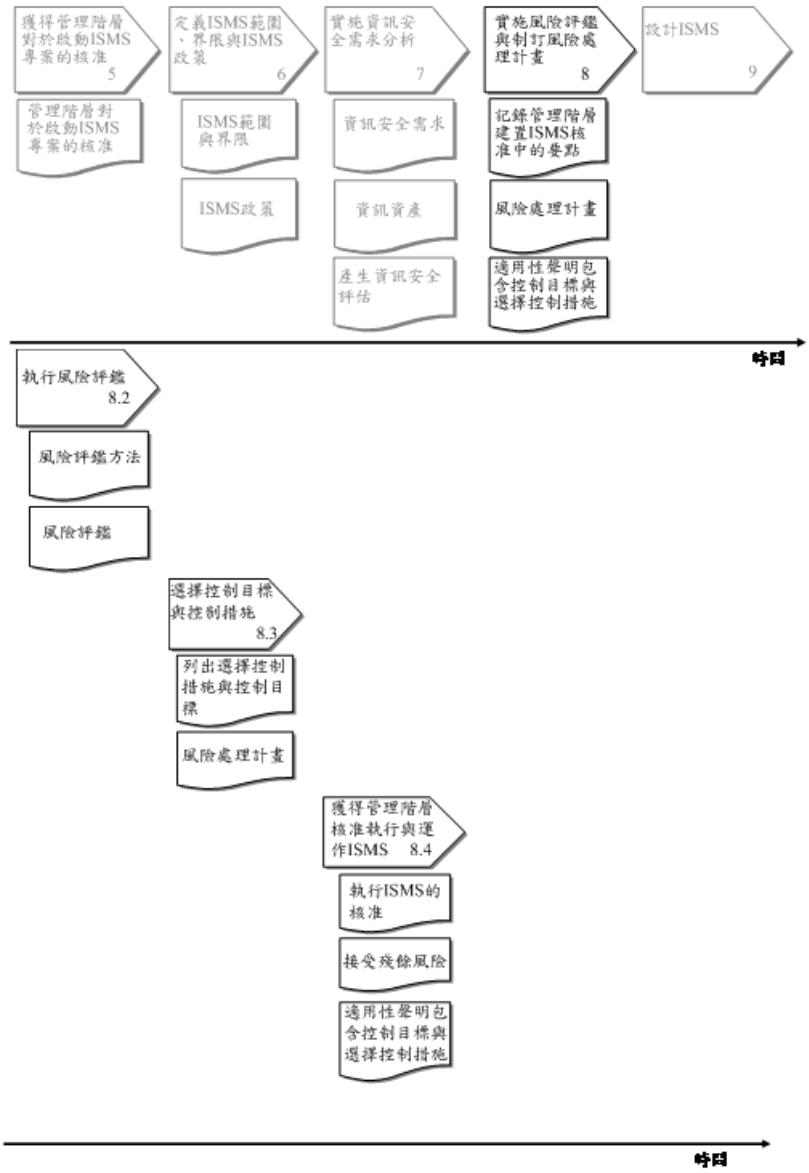
3.2.3.3. 進行資訊安全需求分析



資料來源：ISO/IEC 27003：2010

圖9　資訊安全需求分析階段

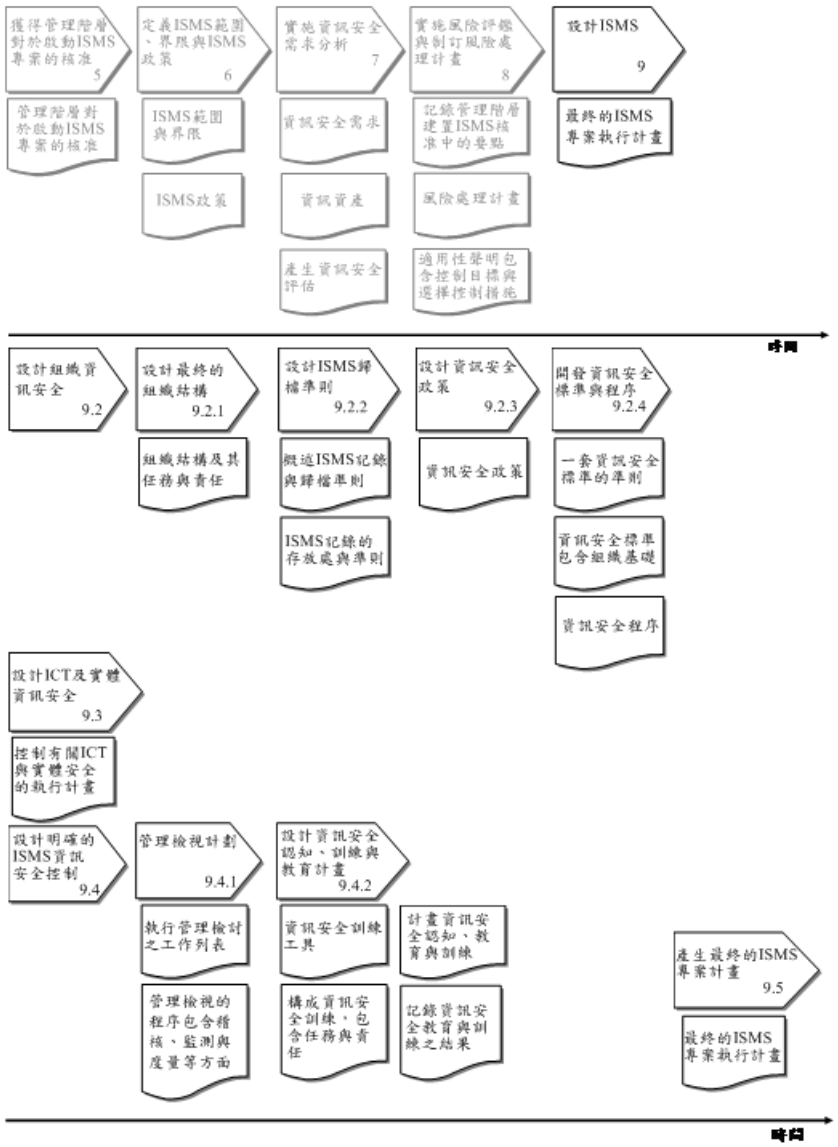
3.2.3.4. 進行風險評鑑與風險處理規劃



資料來源：ISO/IEC 27003：2010

圖10 進行風險評鑑與風險處理規劃階段

3.2.3.5. 設計 ISMS



資料來源：ISO/IEC 27003：2010

圖11 設計 ISMS 階段

3.2.4. ISO/IEC 27005:2008

ISO/IE 國際標準組織，於 2008 年頒布 ISO/IEC 27005 Information technology − Security techniques − Information security riskmanagement，接著於 2009 年 11 月頒布 ISO 31000 Risk management — Principles and guidelines，及至 2011 年 ISO/IEC 國際標準組織為因應 ISO 31000 之頒定，

針對 ISO/IEC 27005：2008 進行技術修訂，將相關之名詞定義與 ISO 31000 統一，於 2011 年 5 月頒定 ISO/IEC 27005：2011，惟內容架構均與 2008 年版本相同。

我國標準檢驗局亦於 2010 年 2 月引用 ISO/IEC 27005：2008 並翻譯為 CNS 27005 資訊技術－安全技術－資訊安全風險管理國家標準，以下內容主要以 CNS 27005 之版本為參考依據。

本標準提供組織內之資訊安全風險管理的指導綱要，並支援 CNS 27001 資訊安全管理系統的特定要求。然而，本標準並不提供任何資訊安全風險管理之特定方法論。組織可自行依據例如資訊安全管理系統之範圍、風險管理之全景或產業別等，定義其風險管理作法。既有在本標準描述之框架下可使用某些既有之方法論， 以實作資訊安全管理系統之要求。

資訊安全風險管理宜為一持續之過程，該過程宜使用風險處理計畫實作建議與決策，以建立全景、評估風險及處理風險。風險管理決定宜在何時做何事之前，要先分析會發生何事與可能之後果，以降低風險至可接受等級。

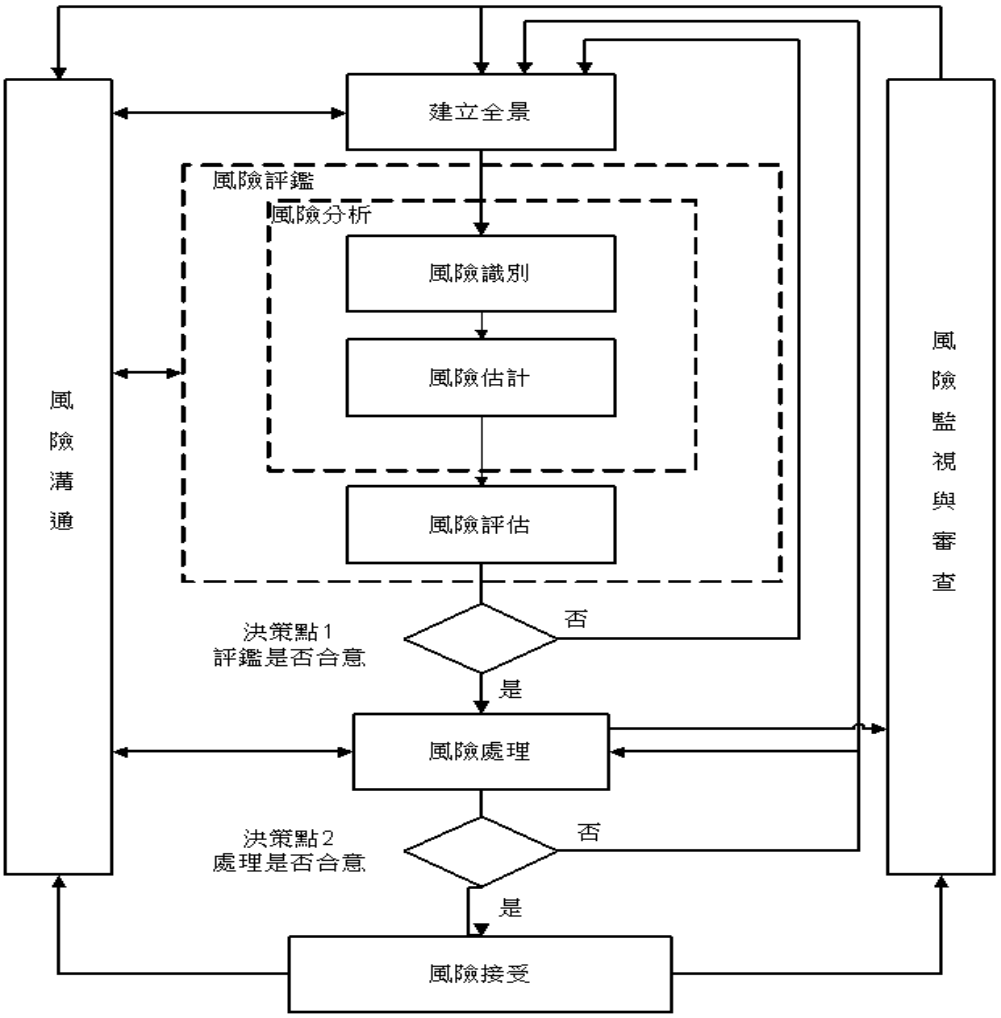
資訊安全風險管理宜對下列各項有所助益：

- 識別風險
- 依其對營運造成之後果與其發生之可能性描述受評風險
- 溝通並瞭解此等風險之可能性與後果
- 建立風險處理的優先次序
- 降低風險發生措施之優先順序
- 在進行風險管理決策時使相關者參與，並告知風險管理狀態
- 風險處理監視之有效性

- 定期監視與審查之風險與風險管理過程
- 為改善風險管理作法所擷取之資訊
- 接受關於風險與風險減緩措施之教育訓練的管理者與員工

3.2.4.1. 資訊安全風險管理過程概觀

資訊安全風險管理過程包含全景之建立、風險評鑑、風險處理、風險接受、風險溝通、風險監視與審查，詳見圖 12 所示。



資料來源：CNS 27005

圖12資訊安全風險管理過程圖

如上圖所顯示，資訊安全風險管理過程之風險評鑑及/或風險處理活動

為循環式，以循環作法進行風險評鑑能在每一循環中增加評鑑之深度與詳細度，循環作法提供在識別控制措施之時間與精力間取得最小化花費之良好平衡時，仍能確保高風險被適當評鑑。

首先建立全景，然後進行風險評鑑，若此資訊充分提供以有效地決定修正風險至可接受等級所需之措施，則評鑑工作完成，隨後並展開風險處理。若資訊不充分，則進行另一個修訂全景(例如：風險評估準則、風險接受準則或衝擊準則)之風險評鑑循環，此循環可能僅及於整體範圍之有限部分。

風險處理之有效性依風險評鑑之結果而定，風險處理可能並不能立即導致殘餘風險降至可接受等級，於此種情況下，可能需要變更全景參數(例如：風險評鑑、風險接受或衝擊準則)後進行另一次風險評鑑循環，並伴隨更進一步之風險處理。

風險接受活動必須確保剩餘風險被組織管理者明確地接受，此於控制措施之實作(例如：成本)被省略或延後之情形下，特別重要。

於整個資訊安全風險管理期間，風險及其處理對管理者與營運作業人員應有適當之溝通。即使是在風險處理之前，已識別之風險資訊對管理事故仍非常具有價值，且可能有助於降低潛在損害。管理者與員工對於風險之認知、對於用以緩和風險所實施之控制措施的本質之認知，以及對組織關切領域的認知，有助於以最有效方式處理事故與未預期事件。資訊安全風險管理過程之每一活動與來自二個風險決策點之每一活動的詳細結果宜予以文件化。

CNS 27001 規定 ISMS 範圍、邊界及全景內所實作之控制措施宜植基於風險，資訊安全風險管理過程之應用能滿足此要求，許多作法均可在組織內成功地實作，組織對過程中每一特定應用宜使用最適合其環境的作法。

於 ISMS 中，建立全景、風險評鑑、發展風險處理計畫及風險接受等，

全係「規劃」階段之部分，於 ISMS 之「執行」階段，降低風險至可接受等級所需之行動與控制措施依據風險處理計畫實作；於 ISMS 之「檢查」階段，管理者將按照事故與環境之變化，決定風險評鑑與風險處理之修改需要；於「行動」階段，包括額外資訊安全風險管理過程之應用在內，任何需要之行動均會被履行。

3.2.4.2. ISMS 與資訊安全風險管理過程之對照(alignment)

彙總與 ISMS 過程 4 個階段有關之資訊安全風險管理過程活動，詳見表 8 所示：

表8 ISMS 與資訊安全風險管理過程之對照

ISMS 過程	資訊安全風險管理過程
規劃	建立全景 風險評鑑 發展風險處理計畫 風險接受
執行	風險處理計畫之實作
檢查	持續監視與審查風險
行動	維持與改善資訊安全風險管理過程

資料來源：本計畫自行整理

3.2.4.3. 資訊安全風險評鑑作法

風險評鑑決定資訊資產之價值、識別適用之存在(或可能存在)的威脅與脆弱性、識別既有之控制措施，以及其對已識別風險之效應、決定潛在後果，最後依全景建制中所設定之風險評估準則，訂定衍生風險之優先順

序並排序之。

風險評鑑通常於兩個(或更多)循環中進行，首先實施「高階風險評鑑」，以識別出需進一步評鑑之潛在高風險。下一循環則對起始循環所揭露之潛在高風險作更深度考量，若此循環未能提供充分資訊以評鑑該風險，則要進行更詳細分析，可能是對整個範圍之某些部分，也可能使用不同之方法，完全由組織依據目標與風險評鑑之標的選擇其自身適用之風險評鑑作法。

CNS/ISO/IEC 27005 附錄 E 列舉了二種資訊安全風險評鑑作法，摘述如后：

3.2.4.3.1. 高階風險評鑑作法

高階風險評鑑允許訂定行動之優先等級與時間表。因為各種理由(如預算）可能無法同時實作所有控制措施，且在風險處理過程中只能處理最關鍵風險。同樣的，若僅在實作一或二年後即開始詳細風險管理，可能是不成熟的。要達到目標，高階風險評鑑可由評鑑衝擊後果開始，而非以威脅、脆弱性、資產及衝擊後果之系統化分析開始。

另一高階風險評鑑開始之理由為其他與變更管理(或營運持續)有關的計畫同步。例如，若一系統或應用系統被規劃要在最近委外，則要完全保護其安全是不合理的，雖然可能仍值得執行風險評鑑以定義委外契約之內容。

所謂「高階風險評鑑作法(High-Level Risk Assessment)」，乃是組織基於各種人力、預算、時間或資源等理由或限制，首先針對其內部所有資訊系統與資訊資產，進行初步的「高階風險評鑑」，找出每個資訊系統在該組織的營運業務價值以及「高階衝擊影響」開始，而不用從資產價值、威脅、脆弱性與後果等系統化的詳細風險評鑑開始。針對被識別為「重要」及/或【高風險/高衝擊影響】的資訊系統，組織如對其風險評鑑結果不合意，

可再運用「詳細風險評鑑作法」對其進行另一個風險評鑑循環；至於在「高階風險評鑑」後，屬於「較不重要」或者【較低風險/較低衝擊影響】的資訊系統，組織則可自行根據其安全要求與風險評鑑目標，自行選擇適用的風險評鑑方法或者風險處理方式。

- 作法特色

「高階風險評鑑作法」特色，說明如下：

– 針對組織所有資訊系統的風險評鑑工作，在準備投入大量專業、人力、時間及預算資源之前，組織先進行快速而簡單的「高階風險評鑑作法」，區隔出屬於【高風險/衝擊】資訊系統，則進一步運用「詳細風險評鑑作法」，如果屬於【中、低風險】則可直接套用該組織認同之基準風險處理作法，將能協助組織迅速建立一個適用於該組織資安政策的風險管理計畫，並有助於該組織的整體資安規劃與持續維護。

– 藉由「高階風險評鑑作法」，組織之資源與預算可被最有效的運用，同時對於該組織最關鍵且需受到保護的資訊系統將會被優先提出與實作，對於後續各項風險處理與應變作為行動，也將更為成功。

- 注意事項

鑑於所有組織因其業務職掌與組織規模不同，同時其業務與資訊系統複雜度、安全等級及系統間關聯程度皆有差異，因此在運用本「高階風險評鑑作法」時，組織必須考量下列注意事項：

– 初期先透過「高階風險評鑑」進行資訊系統重要性與衝擊影響之分類分級，如果在此階段將較為關鍵重要的資訊系統分類錯誤而被識別成【中、低風險】，不需要執行「詳細風險評鑑」，將導致該資訊系統沒有受到足夠安全等級的防護，此點需要特別謹慎注意。

– 無論如何，這些高階風險分類分級錯誤的資訊系統至少還有該組織

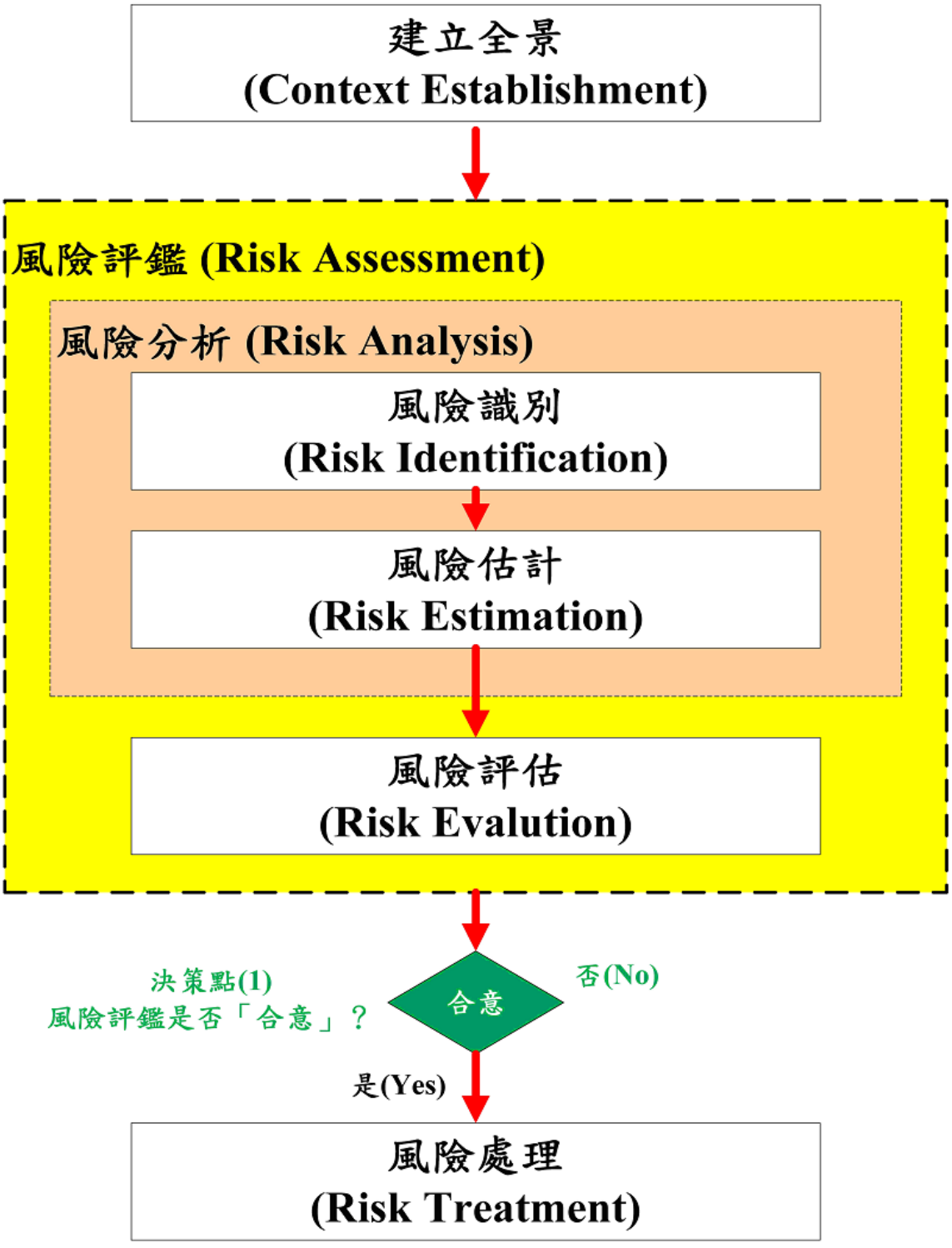
認同之基準風險處理作法的防護措施，因此，組織可以透過「定期」進行高階風險評鑑，重新檢視是否每個資訊系統需要執行比基準風險處理作法更高階的安全防護措施。

– 雖然透過「高階風險評鑑」將重要性與高風險/高衝擊影響的資訊系統區隔出來後，但是後續依然需要投入專業、人力、時間及預算資源進行「詳細風險評鑑」，對於資訊編制較大或資源較為充裕的機關而言，資源投入可能問題不大，但如果要廣泛應用到各級政府機關，則需衡量不同規模機關，其資源之可用性與可行性能否勝任「詳細風險評鑑」的工作負擔與落實成效。

3.2.4.3.2. 詳細風險評鑑作法

所謂「詳細風險評鑑作法(Detailed Risk Assessment Approach)」，乃是組織針對其內部所有資訊系統與資訊資產，逐一詳查風險，包含深入的識別資產與價值、對資產威脅與脆弱性的評鑑，據以分析風險所造成的機密性、完整性、可用性衝擊及其可能性，然後針對這些分析結果，評估與識別符合該組織安全等級的防護控制措施。

「詳細風險評鑑作法」主要分成「風險評鑑(Risk Analysis)」與「風險評估(Risk Evaluation)」兩項主要活動，其中「風險評鑑」則可再細分為「風險識別(Risk Identification)」與「風險估計(Risk Estimation)」兩項步驟，詳見圖 13 所示，茲分別簡述如下：



資料來源：[67]

圖13 詳細風險評鑑作法活動程序圖

- 作法特色

「詳細風險評鑑作法」特色，說明如下：

– 所有資訊系統之資訊資產均能識別出對該資訊資產適當的防護控制措施

– 針對每個資訊系統之資訊資產所作詳細風險評鑑之結果，未來可在該組織或該資訊系統之安全變更的異動管理時參考運用

- 注意事項

鑑於所有組織因其業務職掌與組織規模不同，同時其業務與資訊系統複雜度、安全等級及系統間關聯程度皆有差異，因此在運用本「詳細風險評鑑作法」時，組織必須考量下列事項：

– 對於組織內部所有資訊系統之資訊資產，如果皆以詳細風險評鑑進行，將耗費大量專業人力、時間及預算資源，方能完成所有資訊系統風險評鑑工作，因此組織必須衡量資源的可行性與可用性；此外，因為需要評估分析所有資訊系統之資訊資產，可能會因而延宕該組織真正關鍵資訊系統的安全評估時機。

– 詳細風險評鑑作法將會產生大量的風險評鑑資料，如果所有資訊系統之資訊資產皆以詳細風險評鑑作法進行，可能造成該組織資料維護的負擔。

3.2.4.4. 資訊安全風險處理

風險處理有 4 個可用選項：

- 風險降低
- 風險保留
- 風險避免

- 風險轉移

風險處理選項之選擇宜基於風險評鑑結果、實作此等選項之預期成本及此等選項之預期利益。當風險的大幅降低可用相對低的花費取得時，此等選項應予實作。進一步的改善選項可能不經濟，需進行判斷以決定是否有理由支持。

一般而言，宜使風險的不利後果儘量合理可行的低且與任何絕對的準則無關。管理者宜考量稀有但嚴重的風險。在該種情況中，可能需實作在嚴格經濟考量下無理由支持的控制措施(例如：營運持續控制措施被視為可涵蓋特定之高風險）。

風險處理之 4 個選項並非互不包含，有時組織能經由諸如降低風險可能性、降低其後果與轉移或保留任何剩餘風險等選項之組合大大獲益。

3.2.5. ISO/IEC 27004:2009

ISO/IEC 27004:2009 資訊科技－安全技術－資訊安全管理－測量方法 (Information technology — Security techniques — Information security management — Measurement)

此一標準提供發展與使用安全控制措施與測量方法之指引，用以評估 ISMS 實施 ISO/IEC 27001 所描述控制措施之有效性，包含政策、資訊風險管理、控制目標、流程及程序等之評估，協助鑑別哪些控制措施需要改變或是強化，但同時也特別強調沒有一種安全控制措施之測量方法，可以完全保證安全。

ISO/IEC 27001 要求組織應經常性的審查 ISMS 測量方法的有效性，同時度量控制措施之有效性，以符合組織之安全需求。定義如何測量所選擇控制措施之有效性，並描述測量方法如何使用於評鑑安全控制措施，產生可比較與可重複之結果

本標準根據 ISO/IEC 27001 建議以下之活動，作為組織實施測量方法

之依據：

- 發展安全控制措施(measure)
- 實施與操作資訊安全測量計畫
- 收集與分析資料
- 發展測量方法(measurement)
- 通報測量結果予相關人員
- 利用測量成果作為 ISMS 相關決策之參考
- 使用測量成果識別需要改進的 ISMS 執行，包括範圍、政策、目標、控制措施、流程及程序等
- 持續改善資訊安全測量計畫

組織的規模與複雜程度是能否達成測量成果的重要影響因素之一，本標準適用於所有型態與規模之組織。

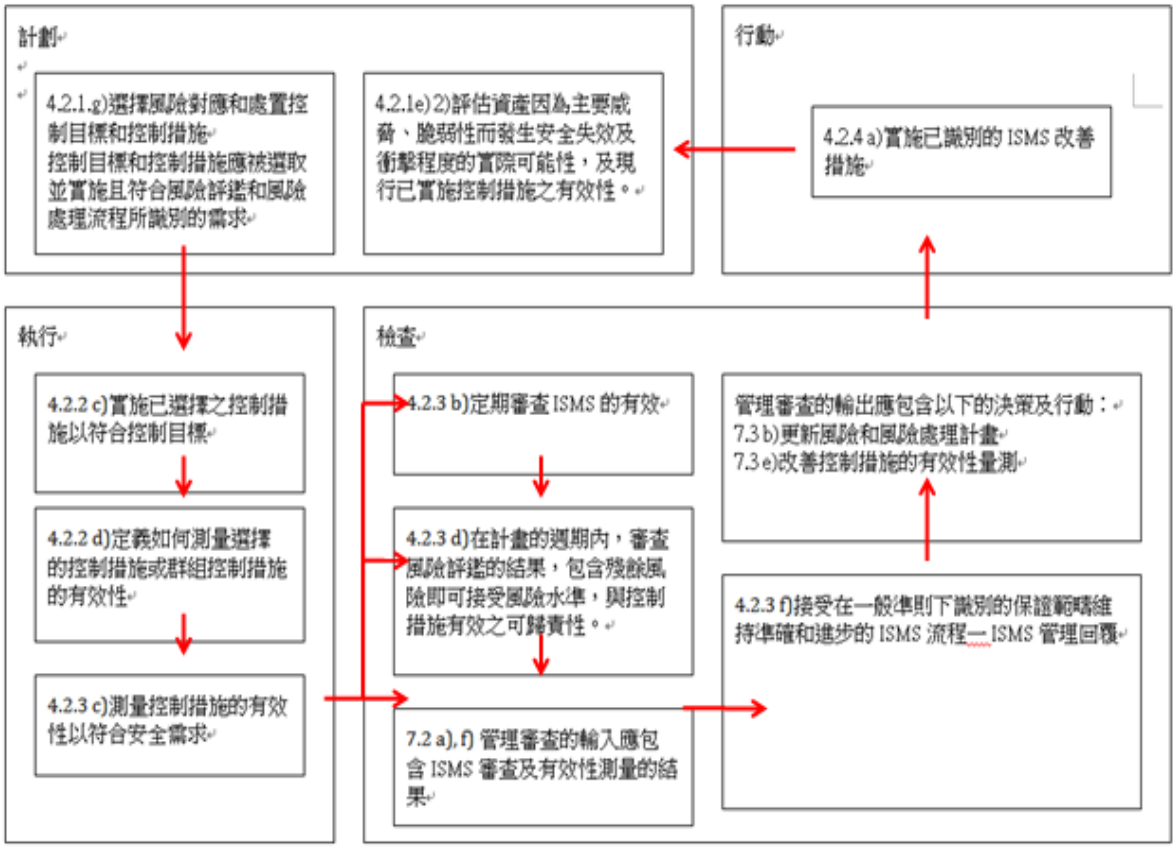
有關測量方法之目標如下：

- 評估安全控制措施之有效性
- 評估實施 ISMS 之有效性
- 證實資訊安全需求被滿足
- 促進組織營運績效之提升
- 提供管理階層審查 ISMS 相關決策之資訊，並評斷需要改進之處

其程序遵循 PDCA 之過程，依序為：

- 選擇控制措施
- 實施控制措施

- 定義如何測量
- 測量控制措施之有效性
- 週期性的進行審查
- 審查風險評鑑的結果
- 產出提供管理階層參考
- 進行管理階層審查
- 改善 ISMS
- 其作業流程與 PDCA 管理循環之關係，詳見圖 14 所示。



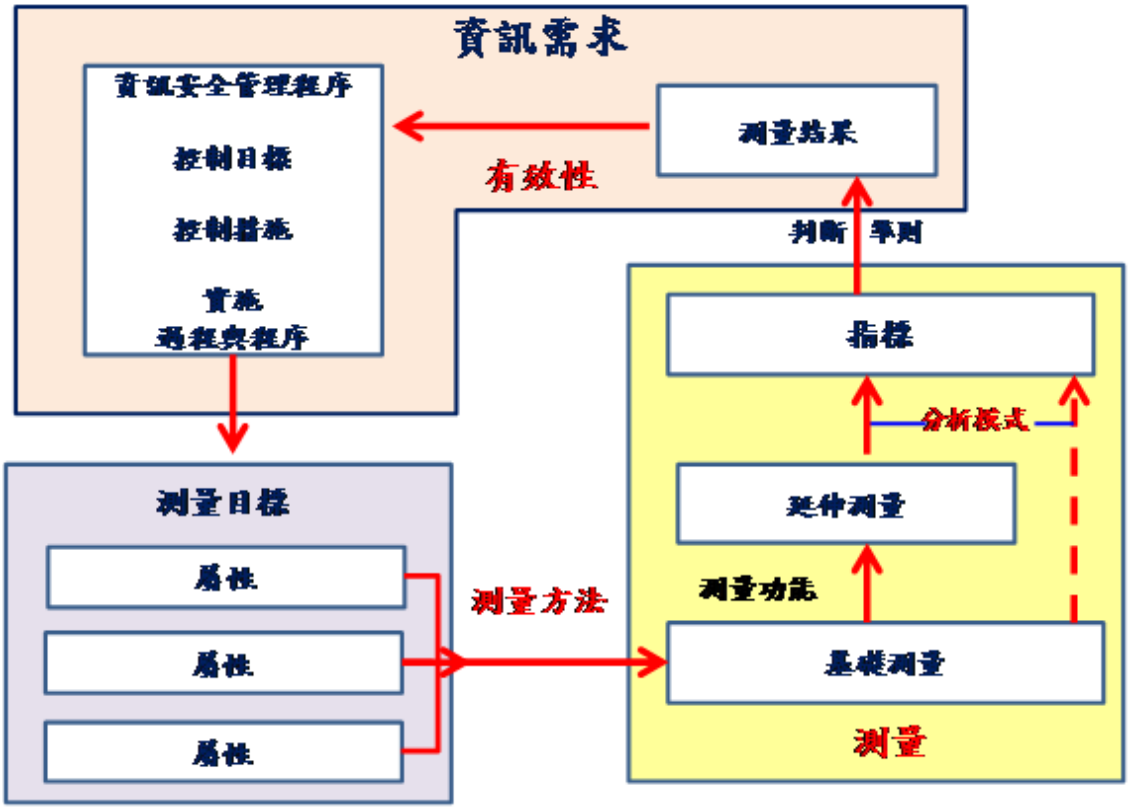
資料來源：ISO/IEC 27004：2009

圖14 ISMS PDCA 循環之安全測量

有關資訊安全測量模型與架構係源自於 ISO/IEC 15939，主要是協助如何將適當之屬性資料加以量化並轉換成指標，提供作為決策之準則。詳見圖 15 所示。組織應該根據資訊需求，決定資訊安全管理之程序，訂定控制目標，並選擇安全控制措施加以落實。

測量之目標是要找出安全控制措施之屬性，訂定測量方法之目標，再選擇適用的測量方法。有關測量方法依其功能多寡，區分為 3 種：

- 基本測量
- 延伸測量
- 指標測量



資料來源：ISO/IEC 27004：2009

圖15 資訊安全測量模型

組織應根據上述之資訊安全測量模型，發展組織的資訊安全測量計

畫，包含以下之過程：

- 安全控制措施與測量方法之發展
- 測量方法之實施
- 資料分析與測量結果之報告
- 資訊安全測量計畫之評估與改善

3.2.6. ISO/IEC 27011:2008

Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

資訊科技－安全技術－植基於 ISO/IEC 27002 之電信業資訊安全管理指引係由 ITU-T 和 ISO/IEC JTC1/SC27 共同制定，並聯合發布為 ITU-T X.1051 和 ISO/IEC 27011。

其控制措施之架構與 ISO/IEC 27002 之架構一致，大部分之控制措施均是引用自 ISO/IEC 27002，修訂內容著重點於機密性協議，包含人員與外部團體，主要來自於對於通信秘密之保護要求，並加強實體環境與電信設施與機線設備之保護，計新增一個安全目標，強化設置於第三方之通信設施之管理，共計新增 13 個控制措施，另外補充修訂了 26 個控制措施，總計共有 39 個控制措施。ISO/IEC 27011 控制措施對照表，詳見 8.17 所示。

3.3.個案訪談

3.3.1. 研究命題

當組織在建置 ISMS 的過程中，可能因組織所生存之外在整體環境(例如：政府規範或產業特色)、組織內部特有的組織營運模式及整體風險意識(Frames of Risk)，構成不同建置階段與導入結果，而組織在建置 ISMS 之過程中，得以改變組織既有的組織結構或作業流程，產生適應環境所需要

的能力，以提升組織整體資訊安全[10]。因此，外顯的組織規則、內隱的組織文化與意識為建置 ISMS 不可忽略的因素。故本計畫以「風險意識文化建置」為觀點，由比較宏觀的角度，探討組織在建置 ISMS 之過程中，內部建構風險意識與資安文化塑造的現象。

本計畫試圖將組織導入 ISMS 的過程，詮釋為建構風險意識的過程，探討組織建置 ISMS 之過程，組織內部如何建構成員整體之風險意識與資安文化，並進而影響最後的建置結果。

3.3.2. 文獻探討

3.3.2.1. 意識重構(Frames Reconfiguration)

意識(Frames)乃人們對於週遭人事物，藉由自我的認知進行詮釋並訂定意義 (Berger and Luckmann, 1967[5]; Smircih and Stubbart, 1985[53]; Weick, 1979a [57])。而 Gioia (1986) [22]認為意識會隨著時間與情境產生變動，亦即意識具有可變動的彈性。過去組織行為相關研究在探討意識的議題時，較關注於組織成員如何在任務與組織環境中建立認知與給予意涵，例如： Daft and Weick, 1984[15]; Dutton and Jackson, 1987[17]; Kiesler and Sproull, 1982[38])。

Moch and Bartunek[44]認為在組織中的成員乃藉由參考內隱的整體意識，作為調適與重組個人對於組織現象或事件的解釋與意涵[58]，特別是當組織成員面臨不確定性或決策不明時，組織整體的意識提供結構化的組織經驗，成為個人採取行動之基本準則[3][44]，亦即本計畫認為在 ISMS 建置的過程中，必須重新建構組織成員之資安意識，以利於組織成員面臨資安事故時，能採取符合資安要求的行動準則。

3.3.2.2. 情境感知(Context-awareness)

在情境資訊(Context Information)相關研究中所提及的情境感知為使用者操作科技設備時，當下的使用情形與環境[40]；亦即行動商務

(M-commerce)所提供情境感知的服務，無線裝置能提供使用者的個人檔案與操作成效，並提供使用者當下所在之環境與過去行為的歷史紀錄[26]，而 Koolwaaij et al.[39]提供使用者情境相依(Context-related)的資訊能令使用者更樂於操作設備，故所提供之服務需達到使用者在使用設備時心境與情境的結合。

因此，本計畫認為組織成員之日常作業應與資安意識或訓練產生連結，以達成心境與情境的結合，進而產生符合組織內部資安要求的行為與決策。

3.3.2.3. 資安治理(Information Security Governance)

Ohki et al.[47]認為資安治理由風險管理機制、資安管控機制及 ISMS 等構成，而資安治理不僅是資訊安全，而是涵蓋實體安全與文件安全。並參照 ISO/IEC 38500:2008 提出下述構面：

- 指導(Direct)，提供管理者從營運策略與風險管理的觀點
- 監測(Monitor)，確保治理相關措施符合度量指標
- 評價(Evaluate)，評價治理結果
- 監督(Oversee)，觀察與稽核治理過程
- 報告(Report)，公開報告予重要關係人

故本計畫認為組織在導入 ISMS 後，須建置與落實系統化的控制措施，以形成資安治理。

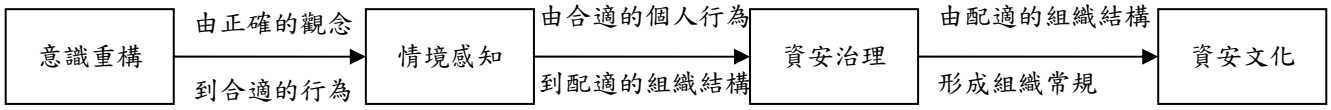
3.3.2.4. 資安文化(Information Security Culture)

Douglas[16]認為組織文化是內部成員不斷協商後的結果，包含共同的價值、思想及行為規範，由文化趨動著組織與其行動，以致組織得以存在於社會[11]。而 Hegberg and Heifetz(1997)認為文化如同組織的作業系統，領導成員的思考與行為。然而，當組織引進一項新的科技或系統，往往會

遇上挫折，起因於組織成員無法改變舊有的想法、邏輯及習慣，而缺乏改變的動機[13][14][1]；本計畫認為上述組織引進新系統失敗的過程如同組織建置 ISMS，若組織無法形成資安文化，使成員落實 ISMS 的制度與流程，將無法改變舊有缺乏資安思維的作業流程與行為準則。

3.3.3. 風險意識文化建構過程

本計畫將文獻探討歸納為「風險意識文化建置過程」之研究架構，詳見圖 16 所示。



資料來源：本計畫自行整理

圖16 風險意識文化建構過程

本計畫認為當組織建置 ISMS 的過程中，須重新建構組織成員對於資安的意識，亦即建立資安重要性的認知與符合組織內部資安需求之行為，此為意識重構階段；成員雖擁有正確的資安認知與行為，但在執行職務或日常作業時，須將正確的認知與行為帶入工作的情境中，以達到資安意識與工作情境之結合，此為情境感知階段；由個人層次提升至整體資安的意識，並維護組織整體的資訊安全，須借由系統化的控制措施與管理機制，此為資安治理機制；使成員落實 ISMS 的制度與流程，改變舊有缺乏資安思維的作業流程與行為準則，此為資安文化。

本計畫根據文獻探討所歸納「風險意識文化建置過程」架構進行訪談資料之分析。訪談對象為電信產業中建置 ISMS 的成功個案，故本計畫以個案研究的方式，從標竿企業中獲得建置 ISMS 的成功模式，以利其他企業仿效。

3.3.3.1. 意識重建

個案希冀主管機關應擬定資安推導的相關辦法與實施細則，提供企業導入資安時之參考，舉例而言，由 NCC 所頒布之「電信事業資訊安全管理手冊」，能給予企業建議與實施管理辦法之依據，讓組織意識並瞭解其有維護企業資訊安全之義務。然而，依組織產業特性與所擁有客戶資料數量與敏感性之不同，會影響其資安管控程度，且多數的企業傾向遵循內部既有文化與規範，故主管機關應對產業訂定適切的法令規範或罰則，給予企業明確的指導。

> *“我覺得真的，要不然就法律頒布嘛，要不然就是我們管理機關對我們要求嘛。...董事長就會...就知道他的想法了。而且據我所知，今天早上我們剛剛開會，針對個資法這個部分，非常重視...”*

企業為營利組織，所擬定之決策與內部資源配置皆以營利為導向，然而，組織若要維護完善的資安環境，需要投入大量的人力與財力，但組織投入資源後產生的資安績效難以衡量，且因產業特性，使得組織內部負責資安維護之資訊單位往往受限於過去的組織層級，難以獲得適當的資源投入，故企業導入資安標準與建置 ISMS 之動機程度高低，取決於主管機關規範的要求程度。

> *“...我們資訊預算其實並沒有那麼高...我們內部也會檢討說，我們花這筆錢，成效在哪裡...如果公部門有一個管理辦法，或者是強制要求，那也許我們就會比較有辦法去執行...”*

個案在導入 ISMS 的過程中沒有一套既定的方法與步驟，只能由不斷地嘗試，從中學習並累積經驗，以制定符合資安標準的管制措施，例如：建立資訊存取與使用的權限。

> *“...沒有一套標準來告訴你該怎麼做，但是我們自己...應*

該是說 lesson learn 啦…”

在個案尚未認證前，其實已存在資訊安全的管理規範，例如：門禁系統與相關監控程序，雖然成員各有職責，但相對於資安標準而言，較缺乏系統化作法。然而，由於高階主管對於資安非常重視，並不斷地向同仁宣導資訊安全的重要性，因而啟發組織需取得資安認證之動機。並藉由現有的資安管理規範，在內部迅速地建置整體資安管理體系。

“…高階主管對於這件事情非常重視，也是不斷地在告訴同仁資訊安全的重要…過去的資安比較…不是一個體系…就像我們知道 ISO 是一個體系…”

個案藉由定期對組織成員進行資安相關的教育訓練，並在組織內部張貼或流通資訊安全有關的訊息，藉由定期與不定期的內、外部稽核，皆能使成員對資訊安全產生意識並進而重視。

“…讓員工可以清楚的知道公司對資訊安全的重視…稽核是一個，training 是一個…佈告也是一個…”

3.3.3.2. 情境認知

個案之成員定期接受教育訓練並利用電子佈告欄或電子報，不斷地被灌輸組織目前既有的資安控制措施並更新資安相關訊息，如：門禁管制、資訊存取控制、桌面與螢幕淨空政策、最新的病毒等。此外，組織制定違反資安控制措施的相關罰則，藉此讓組織成員執行業務時，能時時警惕，並將所接受的資安訓練與認知帶入工作情境。

“每一年都會有那種 training…告訴我們資安應該是怎麼樣…如果說有違反到公司的安全規定，他一定會受到處罰…”

個案不定時地稽核經銷商與加盟店的內部員工，以強化資安相關的規範與確保資安的落實，並將組織內部已形成之資安典範移植至外部組織。

“...那他們會不定時去稽核他，就是告訴他...“

3.3.3.3. 資安治理

個案成立企業安全委員會，其代表為各部門的資訊安全官，並定時召開跨部門資安會議，針對公司相關的資訊議題進行討論，並擬定資安政策與資安相關控制措施。

“比如說像我們會討論說，今天 vendor 進來我們這邊，是不是要安裝所謂的我們的防毒軟體...”

個案內部具有完整的資安管理機制，例如：組織運用實體管控的機制，針對 USB 埠進行權限控管，避免敏感資訊透過類似的管道遭到洩露。

“...工程師去做安裝的時候，讓你 USB 開可以安裝，裝完以後其實我們就要馬上鎖住...”

個案藉由資安標準的導入，建立更為完整的權責架構，以利任務指派與權責區分；建立符合組織需求的資安制度，以明確的制度規範組織成員依所指派之工作內容負起維護資安之責任，並約束成員的行為須符合組織的資安要求，以更明確的組織規章與內部標準作業流程，要求成員對組織資安的投入。

“在那個地方我們是真的有一個第二機房，而且我們是常駐有人力在那邊輪...包括假日也會有人在那邊在做檢查...如果沒有資安的好的一個結構或制度...那個第二機房你很有可能就是做不出來...”

3.3.3.4. 資安文化

當組織落實 ISMS 後，資安規範與相關控制措施融入組織成員之日常生活並進而產生資安文化時，縱使組織面臨科技不斷演進導致外部威脅不斷增加的環境，組織內部的資安維護仍能持續獲得改善。

“...養成一般的人員他在作業的時候...任何跟個資有相關

的...只要離開位子，他就要鎖在抽屜裡面，回家也要鎖在櫃子裡面...”

3.3.4. 企業營運

3.3.4.1. 風險文化建置契合營運領域

電信是一個充滿競爭且競爭者都很積極的產業，尤其每一家電信業者皆擁有數百萬計的客戶個資，更是受到社會所關注，故每一家電信業者都非常重視資訊安全，相關業務與控制措施都很嚴格。除此之外，目前個案仍持續擴大認證範圍，規劃目標為未來 ISO 27011 的認證將涵蓋近四分之三的人力。

“...我們很清楚知道電信業如果有一次重大的什麼資安洩漏事件的話，對我們的影響是大到不得了...”

3.3.4.2. 主要營運流程導入標準

定義重要營運業務之關鍵流程，並納入關鍵流程下所有的營運系統，再決定資安導入範圍之規模，雖然標準的指引方針提及組織可考量部門比或程序比做為導入範圍的選擇，但個案強調應以組織的營運關鍵流程作為考量。

“...因為我們有很多的那個經銷商，直營店或是加盟店等等這些，那如果有客人來申辦的話，他會有一些申請書等等這些資料是透過 Internet 的方式進來的，那我們當時是選定這一個範圍...”

3.3.4.3. 形成資安策略價值

在 2005 年個案的管理高層認為資訊安全不只是為了保護個人資料而已，其他的資訊安全也應有所著墨，進而推動資安認證，使個案的資安管理擁有一個參照準則，而且每位員工都能做到。除此，ISO 27001 認證的

通過，可以讓整個組織體系更為健全，相關的資安政策、文件及流程具有整體性。

“...有了認證以後，其實那個公信力更好，客戶對我們的 trust 也更高...”

一旦發生資安事件(例如：系統不穩定、服務中斷等)後，組織成員才意識到資安的重要性，故企業投入資訊安全之成效往往難以一般績效評鑑投入與產出之量化觀點來衡量。而個案以持續提供穩定的資訊服務之「累積天數」，做為投入資安維運的績效指標，更精準地衡量目前組織整體資安管理的現況，達到將資安標準的思維與制度融入組織標準作業程序中。當資訊單位面對組織高層時，能提出確切的指標數據，證實投入資安推動之績效，並成為組織成員明確的資安改善指標。

“...我覺得我們訂定這個指標以後，會變成是從你的人員的素質，你的作業程序，你的管理方法落不落實...也不用再做什麼客戶滿意度啦，直接看這個最準。”

3.3.5. 主管機關的影響

3.3.5.1. 政策出現

個案認為「個人資料保護法」原本就已具有影響力，但經過修法以後，損害賠償的上限調整，以及其他行政與刑事的責任都加重。除此，尚有一些實質源自行政機關的管制措施，都將加重企業的負擔。

“個資法...影響層面非常大...負擔還真的還蠻重的...”

3.3.5.2. 正當性產生

個案本來就非常重視資安的管理活動，而資安認證運用了一套有系統的方法告訴組織應該怎麼做，雖然仍會增加日常作業與職務上的流程、表單等等負擔，但個案仍願進行資安導入，其主要原因是個案處於競爭激烈

的電信產業，導入標準將對提升組織競爭力有所幫助。

“我們覺得這時機，差不多也是該做的，所以我們就把整個範圍再擴大...”

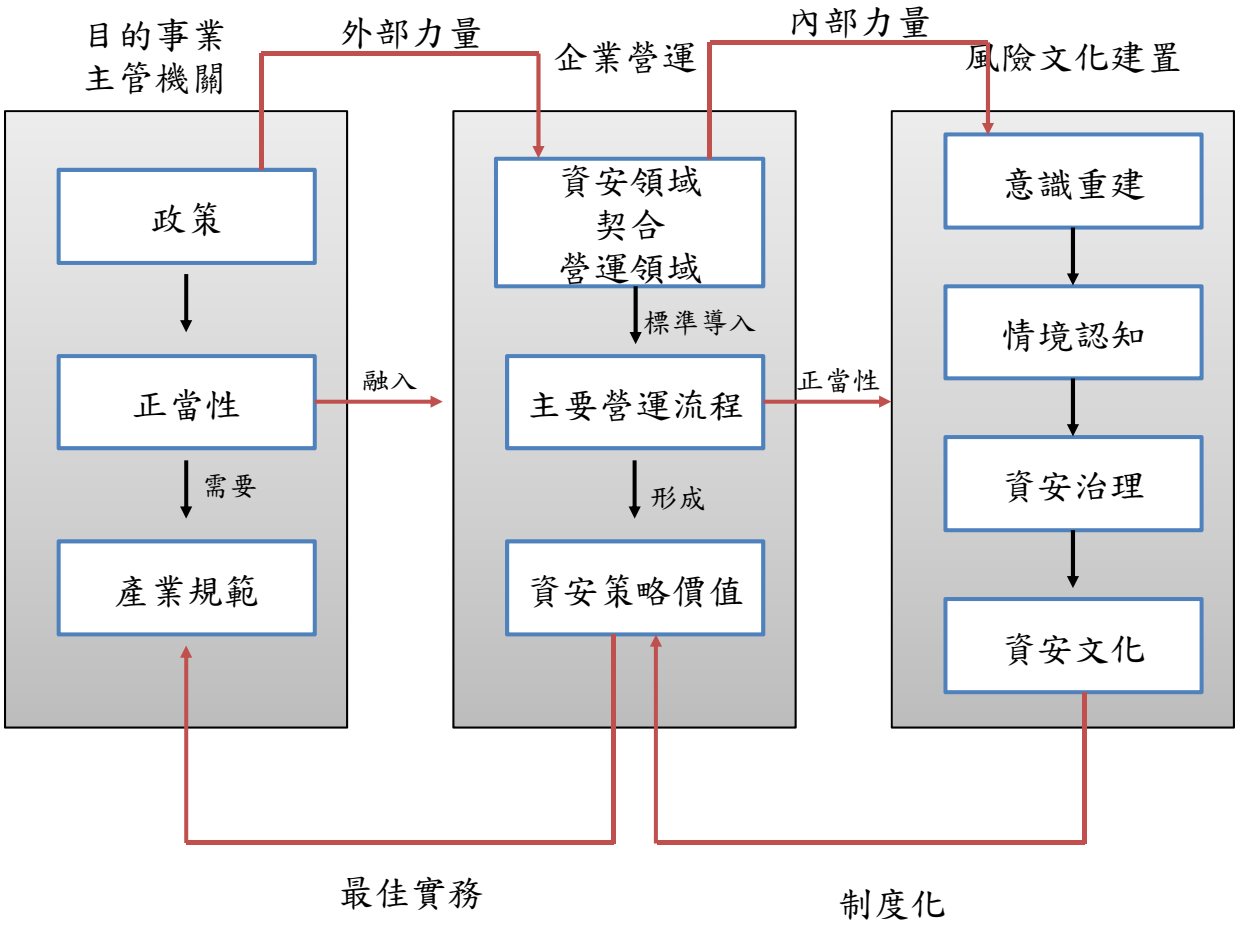
3.3.5.3. 產業規範

由於個案高層的支持與整體組織對資安的認知與需求，過去進行資安導入的過程中，曾投入大量的資源與時間，最後通過資安認證並持續改善，力求將資安相關正確之思維融入常規。此導入的過程與成功經驗，足以成為產業典範。

“...我們很期待說我們新的這個 project 完成後，在業界是指標，我們希望說我們是在，至少在臺灣，已經是算很前面的，在保護個人資料的一家公司...”

3.3.6. 研究發現

經由訪談個案之資料分析，詳見圖 17 所示。本研究計畫發現組織建置 ISMS 或導入資安標準之過程與緣由，可分為政府、企業營運及風險文化建置等面向。



資料來源：本計畫自行整理

圖17 風險意識文化建置整體過程

企業營運：當組織的營運領域(Business Domain)契合風險文化建置時，將促使組織導入資安標準或建置 ISMS；亦即，當組織營運的相關業務，可能因資安事件的發生造成營運的損失時，組織會自發性的導入相關資安標準，而其導入範圍將涵蓋組織目前關鍵的營運流程，並形成資安的策略價值(例如：將營運流程與資安的控制措施完整契合，使得組織對於資安管控更具整體性，以降低風險發生時的營運損失，增強營運持續運作的穩定性，而提升企業形象)，並提供產業或政府最佳實務之典範。

風險文化建置：當組織的營運領域契合資安領域時，將由組織內部產生趨動資安標準導入之動能，並經由「風險意識文化建置過程」，以重新建

構組織成員對於資安的意識，使組織成員擁有正確的資安認知與行為，並在執行營運業務時，將正確的認知與行為帶入工作情境當中，使之達到資安意識與工作情境之結合，並由組織內部系統化的控制措施與管理機制，使個人層次提升至整體資安的意識，以維護組織整體的資訊安全，進而使成員落實 ISMS 的制度與流程，改變舊有缺乏資安思維的作業流程與行為準則。最後，將資安標準所提及的準則與規範，在組織內部進行制度化，亦即將 ISMS 內化為組織制度，並產生資安策略的價值。

目的事業主管機關：當政府擬定或通過新的法規或政令時，將對企業營運產生外部趨動之動能(例如使組織產生建置 ISMS 之動機或壓力)，促使企業面臨改變(例如資安標準之導入)並迫使企業改變或遵循法規及政令的正當性之形成。然而，在此過程中，目的事業主管機關需要產業規範以協助企業遵循或改變組織內部政策，以在企業內部形成推動 ISMS 之正當性。

3.4.問卷調查

3.4.1. 國內通訊傳播產業現況

近年來，由於數位科技的快速發展，通訊與傳播二領域因數位化而日趨匯流，服務樣貌不斷推陳出新。為因應此一科技發展趨勢並有效兼顧國民權益、消費者利益及產業發展，政府於民國 93 年制定公布通訊傳播基本法，並於該法第 3 條明定為有效辦理通訊傳播之管理事項，政府應設「通訊傳播委員會」，依法獨立行使職權。在各界努力下，於民國 95 年 2 月 22 日成立，通訊傳播歷數十年之二元管理劃上句點，統一領航數位匯流時代下之臺灣通訊傳播發展。NCC 所業管之目的事業如下：

3.4.1.1. 第一類電信事業統計

第一類電信業務區分為：固定通信網路業務、行動通信網路業務及衛星通信網路業務，皆屬特許行業，迄 99 年 10 月止發放之執照數共計有 104 張，第一類電信事業家數統計表，詳見表 9 所示。

表9　第一類電信事業執照數統計表

業務項目		執照數
固定通信網路業務	綜合網路業務	4
	電路出租業務國際海纜電路	4
	電路出租業務市內國內長途陸纜電路	62
	市內網路業務	2
行動通信網路業務	無線寬頻接取業務	6
	第三代行動通信業務	5
	行動電話業務	8
	無線電叫人業務	6
	數位式低功率無線電話業務 1900 兆赫	1
衛星通信網路業務		6
	合計	104
資料來源：NCC（資料時間：99 年 10 月 19 日）		

3.4.1.2. 第二類電信事業統計

第二類電信事業，迄 100 年 4 月底止發放之執照數計有 474 張，詳見表 10 所示。

表10 第二類電信事業執照數統計表

服務項目	執照數
語音單純轉售服務	**63**
非 E．164 網路電話服務	**61**
E．164 網路電話服務	**2**

批發轉售服務	196
公司內部網路通信服務	32
頻寬轉售服務	34
語音會議服務	12
網際網路接取服務	186
存轉網路服務	45
存取網路服務	80
視訊會議服務	17
數據交換通信服務	19
付費語音資訊服務	49
行動轉售服務	3
行動轉售及加值服務	12
合計	474
資料來源：NCC（資料時間：100 年 4 月）	

3.4.1.3. 傳播事業統計

廣播電視事業，迄 100 年 4 月底止發放之執照數計有 359 張，詳見表 11 所示。

表11 廣播電視事業執照數統計表

類　別	執照數
無線廣播電臺	171
無線電視電臺	5
社區共同天線業者	8
衛星廣播電視事業(直播衛星廣播電視服務經營者)	9

衛星廣播電視事業	**104**
有線電視系統經營者	**59**
有線電視播送系統	**3**
合計	**359**
資料來源：NCC(資料時間：100 年 4 月)	

3.4.2. 電信事業通過 ISMS 驗證之統計

依據行政院國家資通安全會報(以下簡稱資安會報)之要求，國內資訊安全管理驗證業務開始蓬勃發展，迄 100 年 10 月止，我國通過 ISMS(ISO/IEC 27001)驗證之組織數量為 451 個，目前全球排名第五，詳見表 12 所示。

表12 全球通過 ISO/IEC 27001 數量統計表

國家	數量	國家	數量	國家	數量
Japan	3939	Bulgaria	18	Macau	3
UK	534	Croatia	17	Qatar	3
India	527	Slovenia	17	Albania	2
China	494	Philippines	15	Argentina	2
Taiwan	451	Iran	14	Belgium	2
Germany	181	Pakistan	14	Bosnia Herzegovina	2
Korea	106	Saudi Arabia	14	Cyprus	2
Czech Republic	111	Vietnam	14	Isle of Man	2
USA	104	Iceland	13	Kazakhstan	2
Spain	74	Indonesia	13	Luxembourg	2
Italy	72	Colombia	11	Macedonia	2

國家	數量	國家	數量	國家	數量
Hungary	69	Kuwait	11	Malta	2
Poland	58	Norway	10	Ukraine	2
Malaysia	55	Portugal	10	Mauritius	2
Ireland	44	Sweden	10	Armenia	1
Thailand	43	Canada	9	Bangladesh	1
Austria	39	Russian Federation	9	Belarus	1
Romania	35	Switzerland	9	Denmark	1
Hong Kong	32	Bahrain	8	Ecuador	1
Greece	30	Egypt	5	Jersey	1
Australia	29	Oman	5	Kyrgyzstan	1
Singapore	29	Peru	5	Lebanon	1
Mexico	27	South Africa	5	Moldova	1
France	25	Sri Lanka	5	New Zealand	1
Slovakia	25	Dominican Republic	4	Sudan	1
Turkey	25	Lithuania	4	Uruguay	1
Brazil	24	Morocco	4	Yemen	1
UAE	20	Chile	3		
Netherlands	22	Gibraltar	3	**Total**	**7536**

資料來源：[27]

因政府機關帶頭推動 ISMS 驗證工作，國內產業也逐漸重視資訊安全管理，依據 NCC 之統計，至 100 年 10 月取得 ISO/IEC 27001 驗證之電信事業已有 14 家廠商，詳見表 13 所示。取得電信事業資通安全管理手冊之 ISO/IEC 27011 增項稽核表驗證合格證明之電信事業，詳見表 14 所示。

表13 取得 ISO/IEC 27001 驗證之電信事業

業者	ISMS 認證範圍
中華電信股份有限公司	共 7 張，認證範圍包括數據通信分公司 IDC 業務、SOC 業務、憑證管理系統、代研考會為運之政府入口網、行動通訊分公司帳戶系統、北區電信分公司訂單系統、帳務系統、帳單印寄系統
台灣中油股份有限公司	the provision of development, operation and maintenance of the information management system and planning, implementation and maintenance of the telecommunication, optical giber and computer network system including telecommunications center provided by CPC Corporation, taiwan, department of information management.
台灣固網股份有限公司	the provision of operation, maintenance, and value-added services for Neihu internet Data Center. This in accordance with the Staternent of Applicability.
新世紀資通股份有限公司	the provision of internet data center operation management with value added services provided by ICT Operations Division.
遠傳電信股份有限公司	the provision of development and maintenance of the IA(Internet Activation)and (Store Portal)
台灣大哥大股份有限公司	The provision of: (1) the management of customer information security for the business processes of application, activation and deactivation, change, billing, fraud management, and customer service by TWM headquarter and all TWM direct stores, and related IT services including infrastructure, operating systems, application systems and related assets; (2) the development, operation, and maintenance of mobile communication related Operations Support Systems and management of NOC for mobile communication network activities. This is in accordance with the Statement of Applicability, v2.6 dated 08 Nov. 2010.
是方電訊股份有限公司	IDC 機房， VPN 機房， NOC 維運作業系統及相關部門與維運管理人員
正源科技股份有限公司	The provision of (1)co-location service including hosting service, data backup and network operation center service; and (2)operation and maintenance of server room and network infrastructure activities.
台灣碩網網路娛樂股份有限公司	The provision of customer data protection in system development, operation, and maintenance for Billing Management System,Game Point Express System,and Payment Service System；and operation service for internet Data Centers.

業者	ISMS 認證範圍
亞太電信股份有限公司	資通安全管理涵蓋本公司資訊中心硬體維運管理處資訊機房及加值服務機房與技術暨產品中心網路維運管理部北區維運處電信機房所提供之網路服務、機房維運與其相關支援作業管理流程。依據適用性聲明書版次 V4.0。
關貿網路股份有限公司	對外線上營運服務包括通關、金融、報稅、保險、電子商務、地政及全球運籌之系統營運、電子資料交換、網路服務、資訊安全服務及網路加值服務相關之資訊及系統之資訊安全管理；以及電腦網路應用系統之規劃設計與開發服務、電腦設備設施管理服務及電腦軟硬體相關設備之代理與銷售服務與公司內部營運所需之資訊及系統之資訊安全管理，並與最新版本之適用性聲明一致(version v1.5）
財金資訊股份有限公司	the provision of system design, delvelopment, maintenance and operation of interbank transaction system and related banking services. This is in accordance with the statement of applicability dated 28 july 2009
台灣集中保險結算所	the delvelopment and maintenance of the following systems: central depository and book-entry system, securities depository management system, futures clearing system, bill clearing andsettlement system, remote inquireing printing system, lost securities claim system, global internet system, firewall system, email system, short-term interest rate index system, office automation system, external audit system, official document internet system which are provided by system development department, computer operation department and fixed income information planning department of taiwan depository & clearing corporation.
台灣恩悌悌股份有限公司	The daily operation and management of the sales, marketing, administrative affair product, network activities and the supporting office automation infrastructure, including the lan, servers and server room in the taipei branch office in accordance with the statement of applicability version 1.1 dated 28/10/08
精誠資訊股份有限公司	the provision of operation and physical control of internet data center service in neihu provided by network operation center, server room operation of Financial information service in Neihu provided by network service department.
神通電腦股份有限公司	技術服務處客戶服務辦公室及【客戶服務系統】相關之機房設備。業務範圍涵蓋【客戶服務系統】之操作及維護。此系統依據 2007 年 1 月 19 日版本 1.1 之適用聲明書

業者	ISMS 認證範圍
汎宇電商股份有限公司	提供台灣網路通關服務包含進海空出口貨品前肢申請、回覆、線上授權及檢驗，以符合適用性聲明書 2.1
宏碁股份有限公司	Provision of Facility Services and Operational Management Services for Data Center Co-Location and Back-UP Site in Accordance with the Latest Version of the Statement of Applicability.
台灣國際商業機器股份有限公司	providing clients with it equipments, information, personnel, infrastructure and related facilities to recover it operations for business resilience & continuity services at e-center. IBM Taiwan corporation.
威寶電信股份有限公司	The provision of (1) the operation of Network Management Center and the management of north core network activities of 3.75G mobile communication network provided by Network Management Division (2) the development, operation, maintenance of internal information system, and management of related server room activities, networking infrastructure supporting activities within IT Group.This is in accordance with the Statement of Applicability, version 1.2, dated 29 Sep. 2011.
資料來源：[69]	

表14取得電信事業資通安全管理手冊之 ISO/IEC 27011 增項稽核表驗證合格證明之電信事業

業者	ISMS 認證範圍
是方電訊股份有限公司	IDC 機房， VPN 機房， NOC 維運作業系統及相關部門與維運管理人員
中華電信行動分公司	The provision of: (1) the management of mobile communication network activities provided by Network Operation & Maintenance Department；(2) the peration, maintenance and management of all mobile communication network switching facilities, mobile value-added service equipment sites; (3) the development,operation, maintenance and management of mobile Billing and Management System (BMS), and related IT services including infrastructure, operating systems and related assets. This is in accordance with the Statement of Applicability, v.05 dated 29 April 2008.

業者	ISMS 認證範圍
台灣大哥大股份有限公司	The provision of: (1) the management of customer information security for the business processes of application, activation and deactivation, change, billing, fraud management, and customer service by TWM headquarter and all TWM direct stores, and related IT services including infrastructure, operating systems, application systems and related assets; (2) the development, operation, and maintenance of mobile communication related Operations Support Systems and management of NOC for mobile communication network activities. This is in accordance with the Statement of Applicability, v2.6 dated 08 Nov. 2010.
亞太電信股份有限公司	資通安全管理涵蓋本公司資訊中心硬體維運管理處資訊機房及加值服務機房與技術暨產品中心網路維運管理部北區維運處電信機房所提供之網路服務、機房維運與其相關支援作業管理流程。依據適用性聲明書版次 V4.0。
中華電信國際分公司	The provision of operation and maintenance of Tanshui and Kinchung submarine cable services at Tanshui cable station, Kinchung cable station, Taipei ITMC, network arrangement center, and CHTNet, including circuit provision & restoration, equipment operation & maintenance, and supported information network management.This is in accordance with the Statement of Applicability, CHTI-ISMS-M-003, Ver. 01, dated Mar. 31, 2011.
威寶電信股份有限公司	The provision of (1) the operation of Network Management Center and the management of north core network activities of 3.75G mobile communication network provided by Network Management Division (2) the development, operation, maintenance of internal information system, and management of related server room activities, networking infrastructure supporting activities within IT Group.This is in accordance with the Statement of Applicability, version 1.2, dated 29 Sep. 2011.
資料來源：[69]	

3.4.2.1. 國通過 ISMS 驗證之產業別分析

我國通過 ISMS 驗證之組織，依其產業別分析，詳見表 15 所示。通訊傳播事業目前合計取得 31 張證照，其中又以中華電信與臺灣中油所擁有之證照數佔大多數。

表15 我國通過 ISMS 驗證之產業分析表

行業別	通過 ISO27001 驗證	百分比	備註
政府機關	136	32.9%	
醫院	94	22.8%	
學校	37	9.0%	
資訊業	32	7.7%	
通訊傳播事業	31	7.5%	
其他	30	7.3%	
財團法人	22	5.3%	
金融業	21	5.1%	
國營事業	10	2.4%	
合計	413	100%	

資料來源：本計畫自行整理

3.4.3. 調查作業進行

本階段問卷調查採驗證性問卷，藉以瞭解通訊傳播事業之經營規模(如資本額、員工數等)與業務特性(如核心業務)等因素，探討目的事業對於資訊安全管理之重視程度與窒礙因素，提出適合之資通安全管理機制影響構面、評估等級及實施範圍。

本問卷調查的研究母體包含現有已核准之第一、第二類電信及傳播事業，根據以上所述之各類執照發放數量，目前共有 916 家業者(937 張執照)，採用普查方式，針對全數業者，由 NCC 寄發正式公文，要求業者填答，並

提供問卷下載連結網址，業者填寫完畢後，以紙本郵寄、傳真或電子郵件等方式回覆，除此之外，亦配合本計畫所辦理之資通安全管理機制座談會，於現場發放紙本問卷，受訪業者填寫完畢後以郵寄方式回收，以提升問卷回覆率。調查期間自 100 年 5 月 16 日~100 年 6 月 10 日止，合計回收有效問卷計有 149 份（149 家廠商、211 張執照）。

3.4.4. 問卷設計說明

本計畫之問卷乃依據計畫目的與個案研究發現所得，問卷內容包含「企業基本資料」、「企業資訊環境」及「認知重要程度與實際實施程度」等三部分。

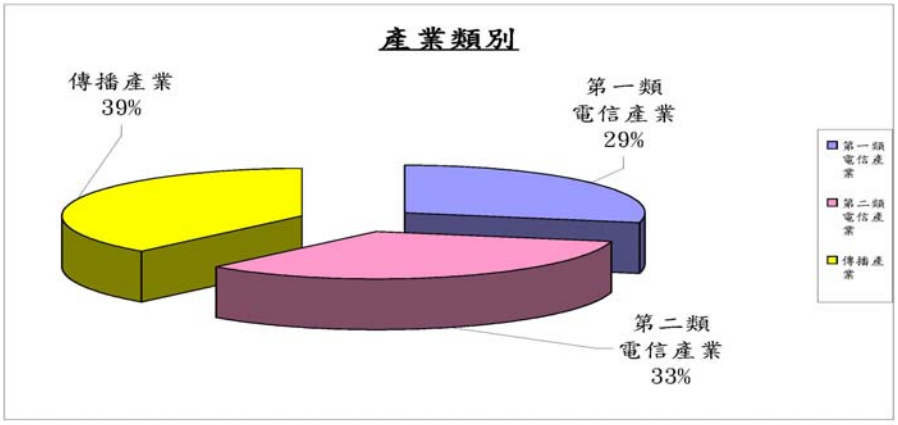
本計畫依個案研究發現之風險意識文化建置整體過程，劃分為規劃、建置及維持階段，以此為結構化方程模式之外因潛在變項，擬以問卷探討組織成員對組織資訊環境之認知，影響導入 ISMS 意願之因素，藉以瞭解通訊傳播事業之經營規模(如資本額、員工數等)與業務特性(如核心業務)等因素，探討目的事業對於資訊安全管理之窒礙因素與優先改善項目。

以上採用李克特量表，要求填答者表明對某一表述贊成或否定，以利於填答者感受度之量測(邱皓政，2009)，但為使「認知重要程度與實際實施程度」部分之問卷題目能瞭解組織內部成員對於資安之認知與組織內部資安相關控制措施之實際實施程度，故此部分題項區分為兩部分：第一部分，填答者依自我知覺認為問項提及之資安相關議題的重要程度選擇「非常重要」、「重要」、「普通」、「不重要」及「非常不重要」；第二部分，填答者依自我知覺認為問項提及之組織內部實施資安相關控制措施之實際程度選擇「完全落實實施」、「大部分已實施」、「已部分實施」、「僅少部分實施」及「完全沒有實施」。

3.4.5. 調查結果統計

3.4.5.1. 企業基本資料

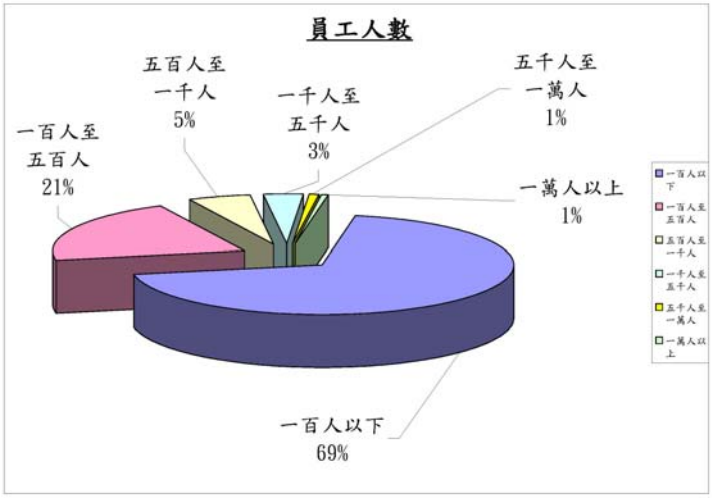
本次調查回收之有效問卷，依產業別區分，第一類電信產業佔 29%、第二類電信佔 33%、傳播事業佔 39%，詳見圖 18 所示。



資料來源：本計畫自行整理

圖18 問卷調查－產業類別統計

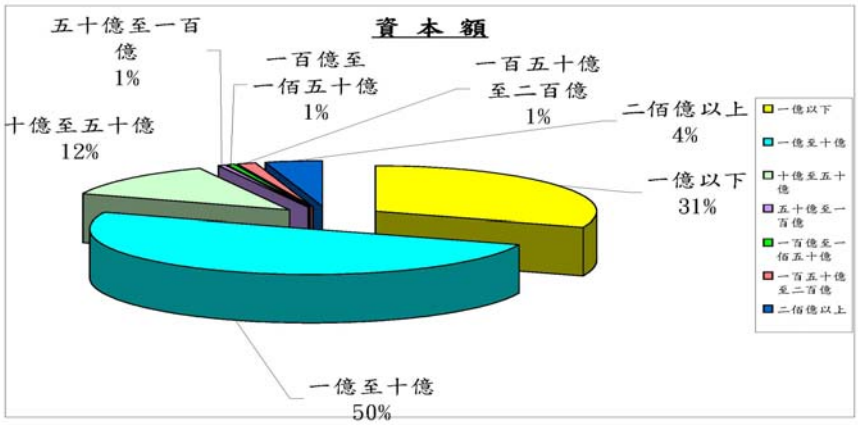
依據員工人數統計，100 人以下之企業佔 69%最多，詳見圖 19 所示



資料來源：本計畫自行整理

圖19 問卷調查－員工人數統計

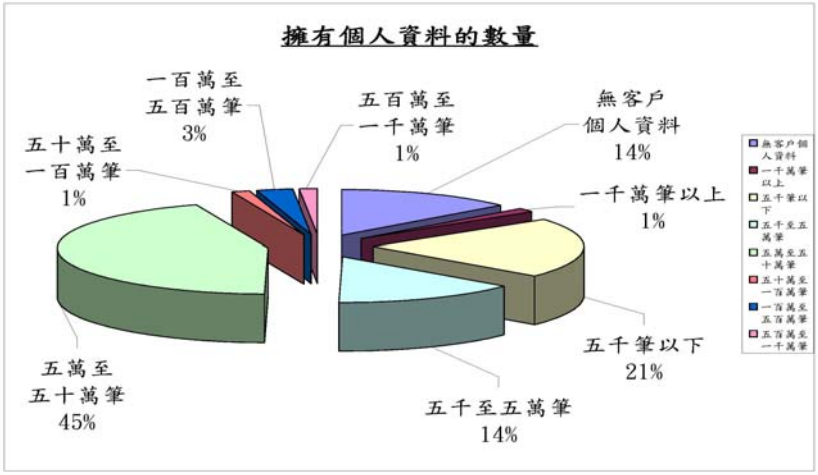
依據資本額統計，1 億元以下之企業佔 31%、10 億元以下之企業佔 50%，二者加總就佔總數之 81%，詳見圖 20 所示。



資料來源：本計畫自行整理

圖20 問卷調查－資本額統計

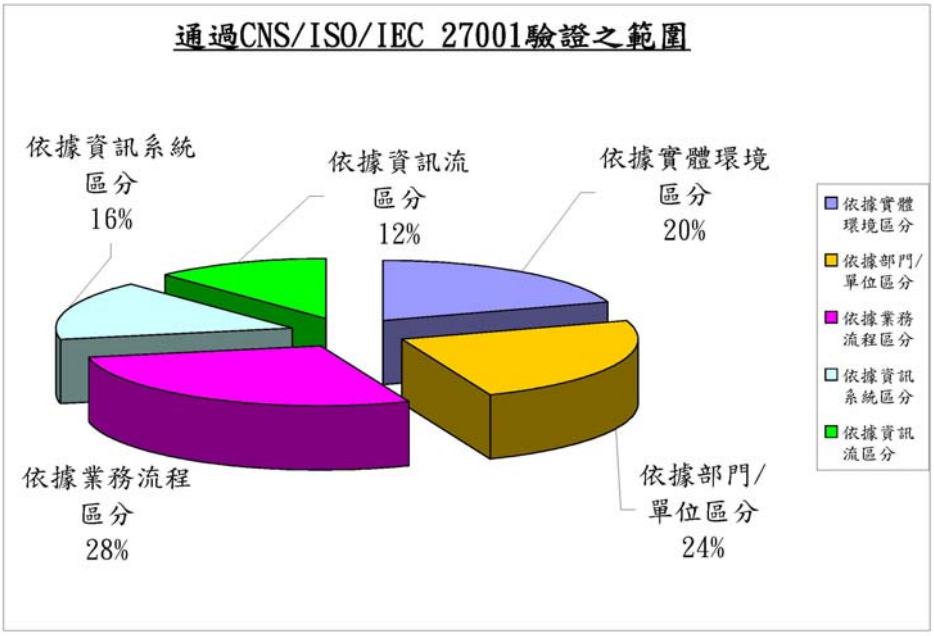
依據個人資料數量統計，以 5 萬至 50 萬筆佔 45%為最高，宣稱無客戶個人資料者佔 14%，詳見圖 21 所示。



資料來源：本計畫自行整理

圖21 問卷調查－個人資料數量統計

已通過 ISMS 驗證之企業，其範圍統計，依據業務流程區分者佔 28%為最高，依據部門/單位區分者佔 24%，依據實體環境區分者 20%，依據資訊系統區分者佔 16%，其中尚有 12%係依據個人資料資訊流申請通過驗證，最為特殊，詳見圖 22 所示。



資料來源：本計畫自行整理

圖22 問卷調查－通過 ISMS 驗證之範圍統計

3.4.5.2. 企業資訊環境

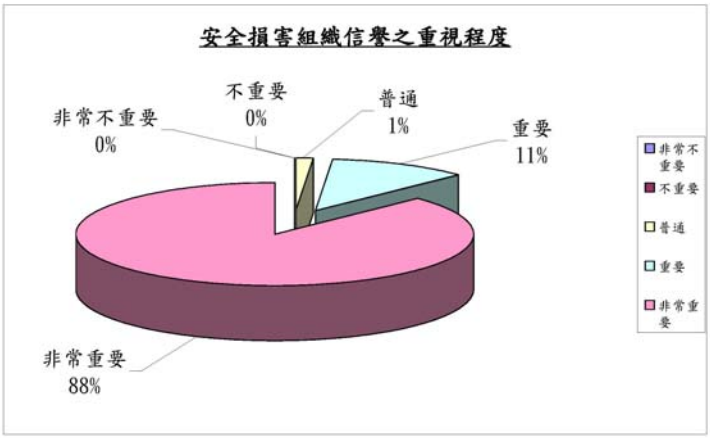
分別針對以下 19 項問項，調查通訊傳播事業等對於企業資訊環境之認知程度，期望能夠找出影響企業導入資通安全管理系統之影響因素，依據認知比例高低，依序排列，詳見表 16 所示。顯見通訊傳播事業對於組織信譽、人員傷亡、個資保護、業務運作及資料保護遭受損害之重視程度，較為欠缺的是對於資安資源投入比例、擁有資訊設備與員工的比例、營運過程之風險進行評鑑作業、系統化的方法實施資安管理及安全概念融入公司組織文化等。

表16 通訊傳播事業對於企業資訊環境之認知程度統計表

項次	類別	非常重要	比例	參閱圖示
1	安全損害組織信譽之重視程度	**130**	**87.25%**	詳見圖 23
2	安全造成人員傷亡之重視程度	**124**	**83.22%**	詳見圖 24
3	對於客戶個人資料之保護程度	**115**	**77.18%**	詳見圖 25
4	對於安全影響業務運作之重視程度	**103**	**69.13%**	詳見圖 26
5	資料保護受到損害之重視程度	**97**	**65.10%**	詳見圖 27
6	對於安全相關法律規程之遵循程度	**88**	**59.06%**	詳見圖 28
7	營運業務所需之資訊化程度	**83**	**55.70%**	詳見圖 29
8	對上述資訊系統之依賴程度	**80**	**53.69%**	詳見圖 30
9	主管機關的政策對於貴公司資源投入資訊安全的影響程度	**74**	**49.66%**	詳見圖 31
10	法律對於貴公司落實資訊安全意願的影響程度	**73**	**48.99%**	詳見圖 32
11	對委外作業安全之重視程度	**71**	**47.65%**	詳見圖 33
12	營運安全包含人員、實體、系統及營運持續等重視之程度	**65**	**43.62%**	詳見圖 34
13	對於員工之安全認知訓練程度	**63**	**42.28%**	詳見圖 35
14	對於營運安全維護，訂定明確之權責區分與作業程序之程度	**60**	**40.27%**	詳見圖 36
15	以系統化的方法，實施資安管理程度	**54**	**36.24%**	詳見圖 37

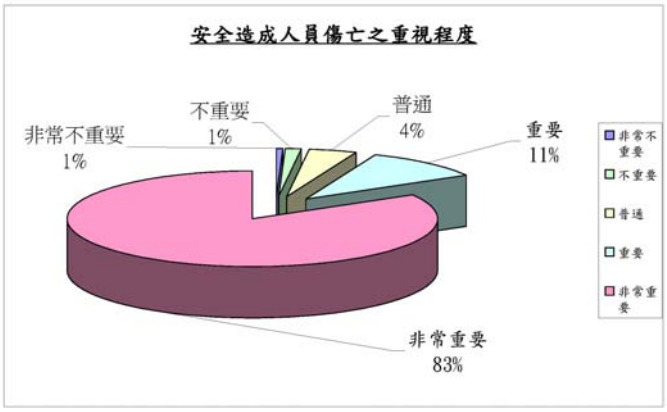
項次	類別	非常重要	比例	參閱圖示
16	安全概念已融入貴公司組織文化之程度	**54**	**36.24%**	詳見圖 38
17	對於企業營運過程之風險進行評鑑作業之程度	**48**	**32.21%**	詳見圖 39
18	擁有資訊設備與員工的比例	**46**	**30.87%**	詳見圖 40
19	對於資訊安全資源投入比例	**43**	**28.86%**	詳見圖 41
合計 149 家廠商				

資料來源：本計畫自行整理



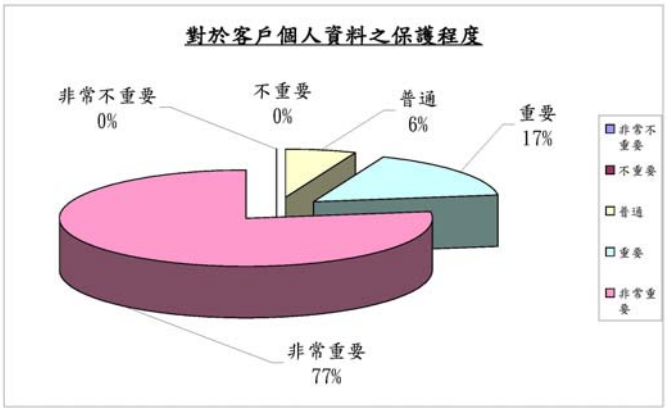
資料來源：本計畫自行整理

圖23 問卷調查－安全損害組織信譽之重視程度統計



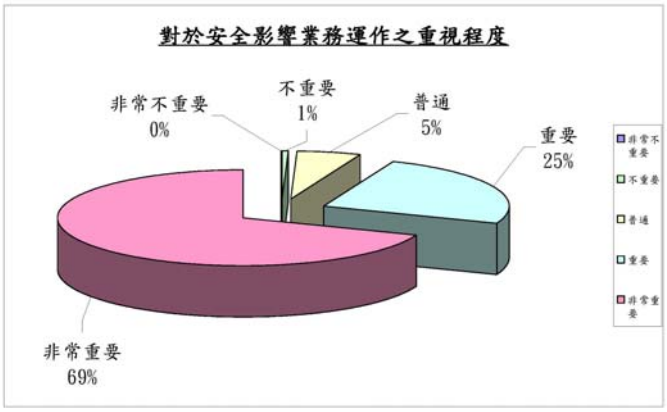
資料來源：本計畫自行整理

圖24 問卷調查－安全造成人員傷亡之重視程度統計



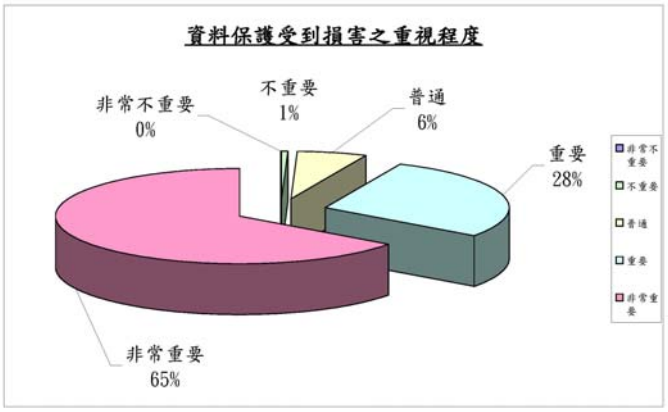
資料來源：本計畫自行整理

圖25 問卷調查－個人資料保護之程度統計



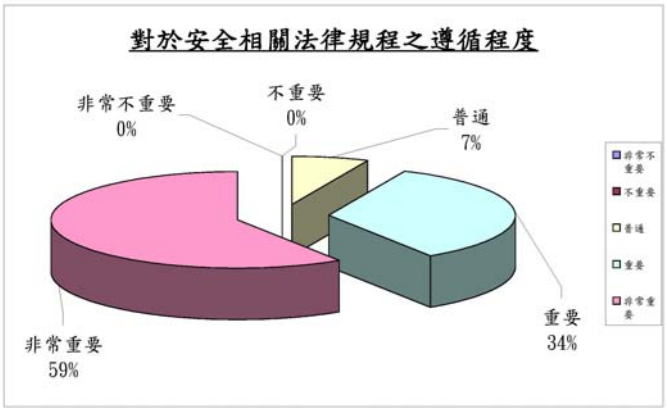
資料來源：本計畫自行整理

圖26 問卷調查－安全影響業務運作之重視程度統計



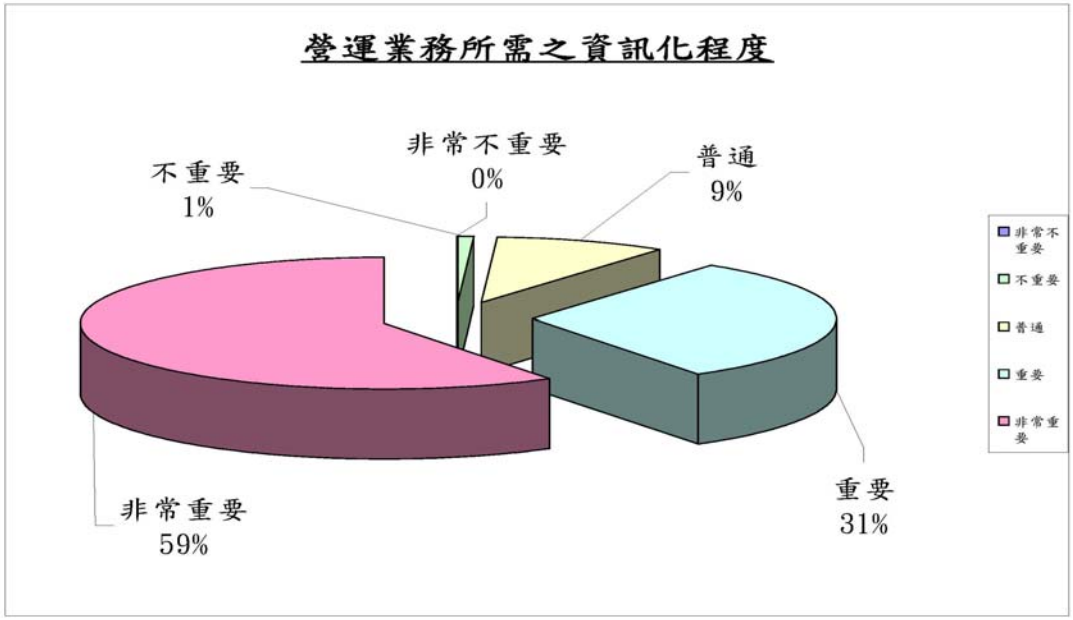
資料來源：本計畫自行整理

圖27 問卷調查－資料保護受到損害之重視程度統計



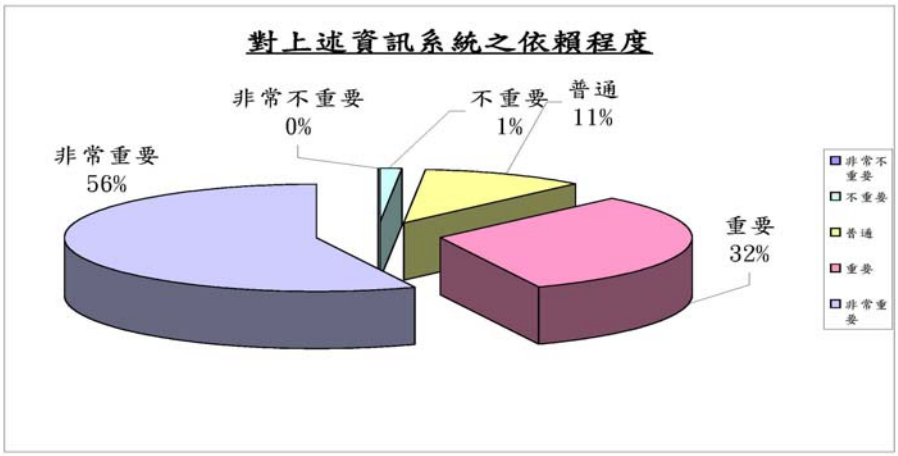
資料來源：本計畫自行整理

圖28 問卷調查－安全相關法律規程之遵循程度統計



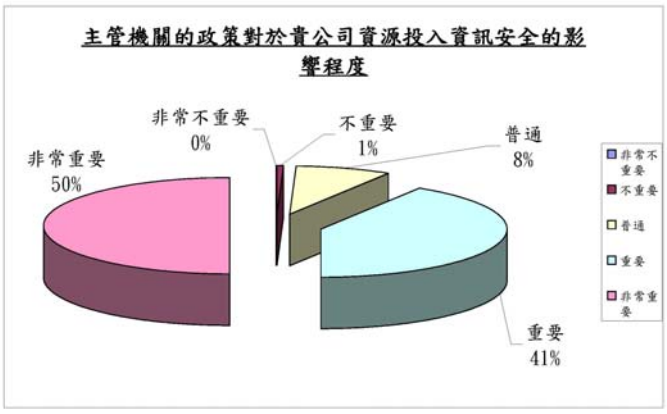
資料來源：本計畫自行整理

圖29 問卷調查－營運業務所需資訊化程度統計



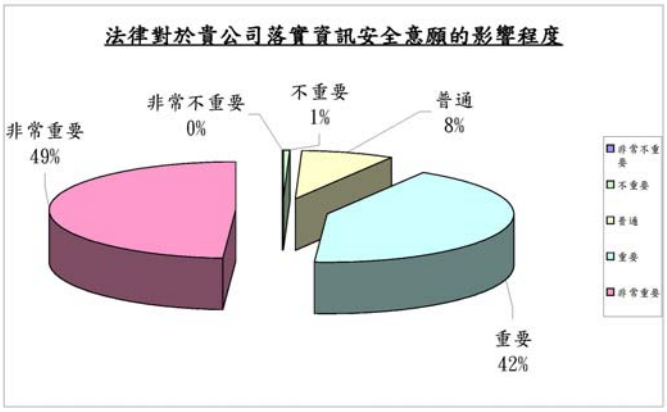
資料來源：本計畫自行整理

圖30 問卷調查－對上述營運資訊系統之依賴程度統計



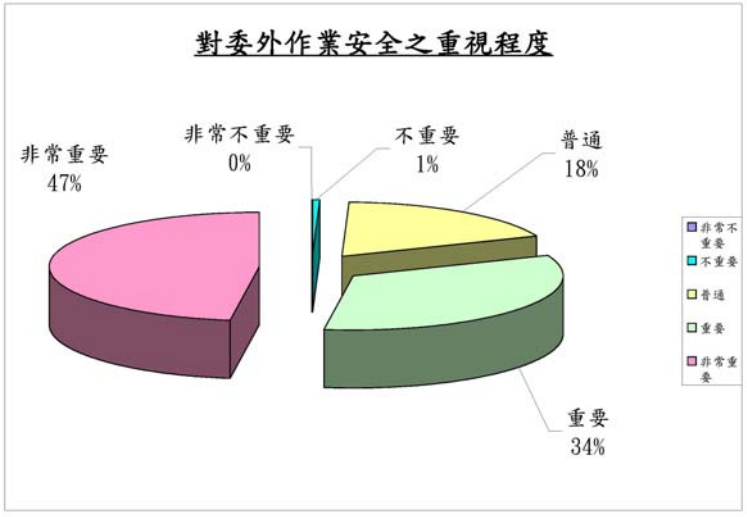
資料來源：本計畫自行整理

圖31 問卷調查－主管機關政策對於資源投入資安之影響程度統計



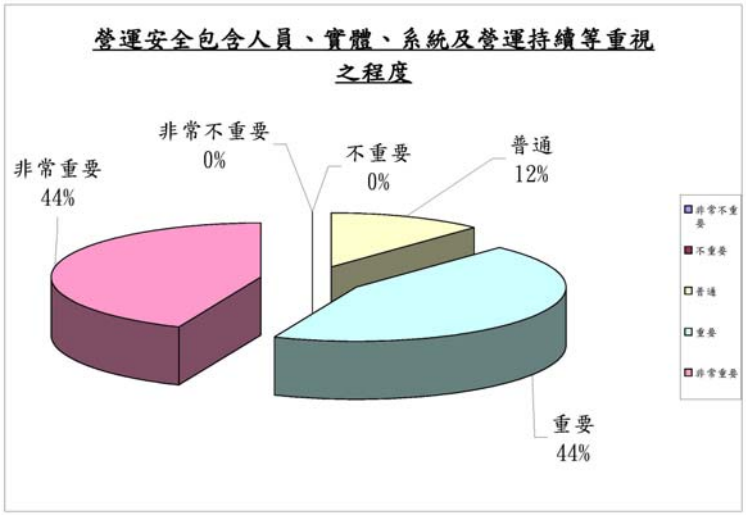
資料來源：本計畫自行整理

圖32 問卷調查－法律對於落實資訊安全意願之影響程度統計



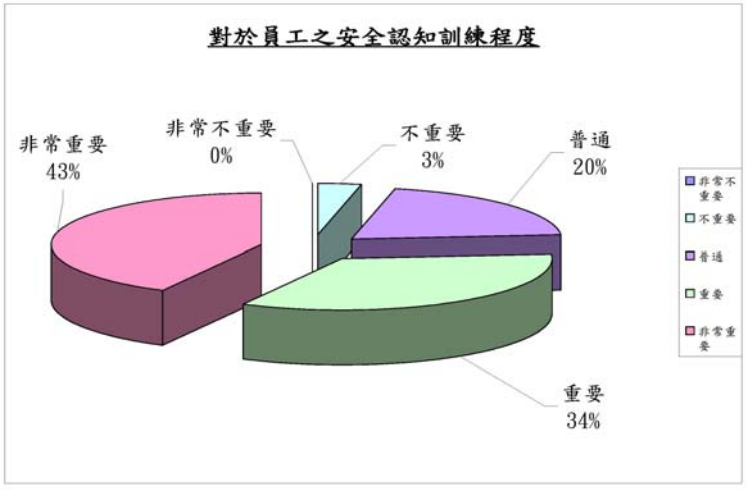
資料來源：本計畫自行整理

圖33 問卷調查－委外作業安全重視程度統計



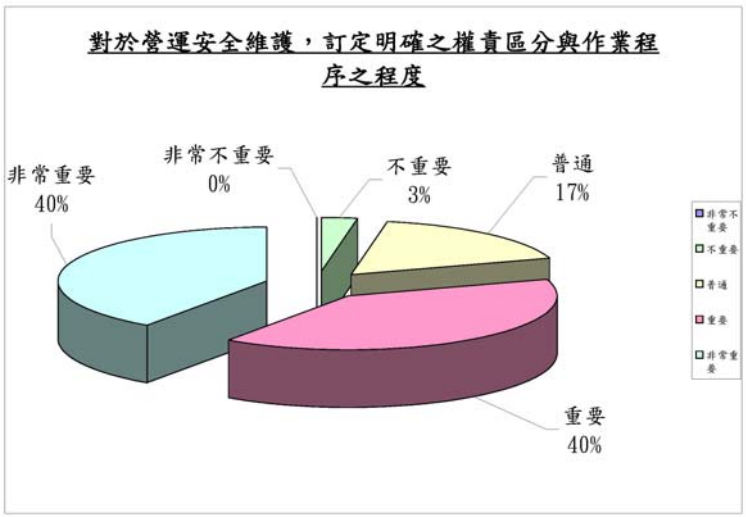
資料來源：本計畫自行整理

圖34 問卷調查－營運持續重視之程度統計



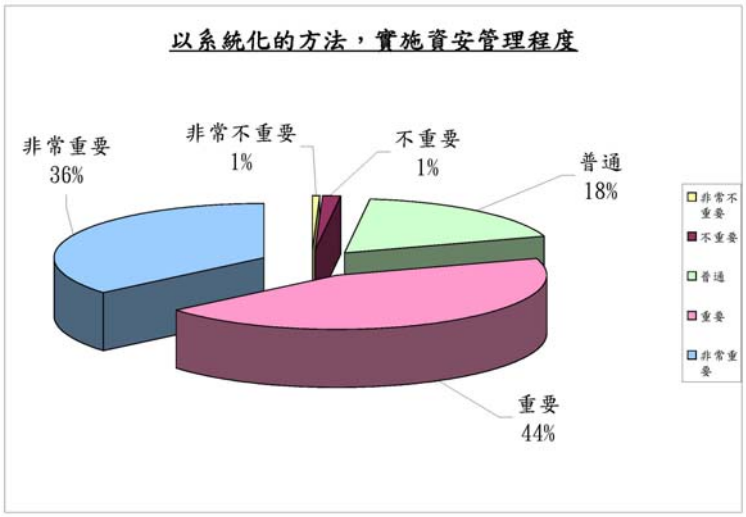
資料來源：本計畫自行整理

圖35 問卷調查－員工安全認知訓練之程度統計



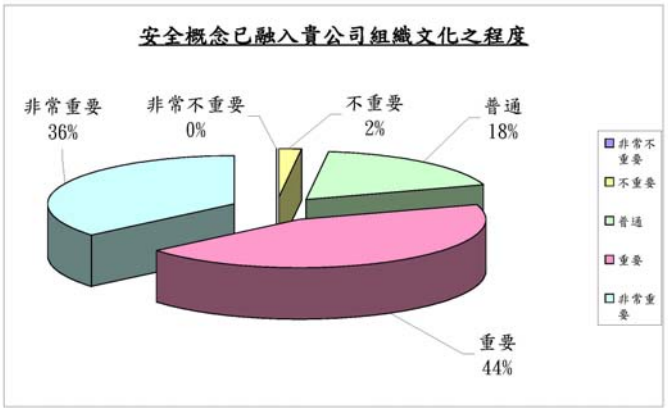
資料來源：本計畫自行整理

圖36 問卷調查－明確安全權責區分之程度統計



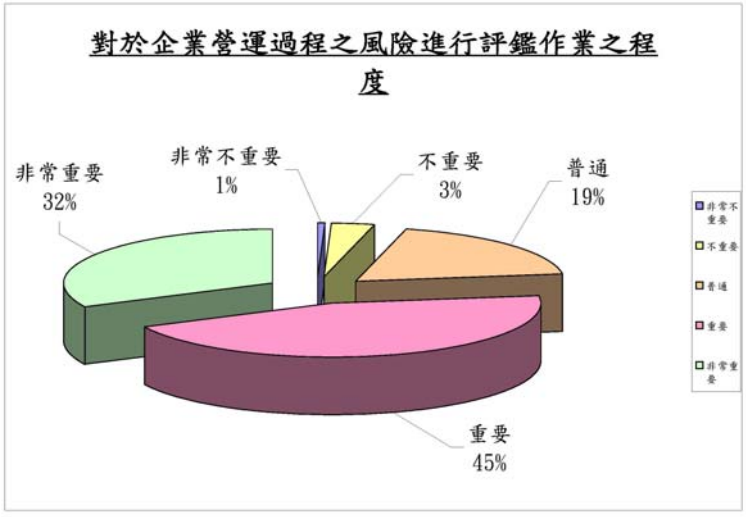
資料來源：本計畫自行整理

圖37 問卷調查－系統化方式實施資訊安全管理統計



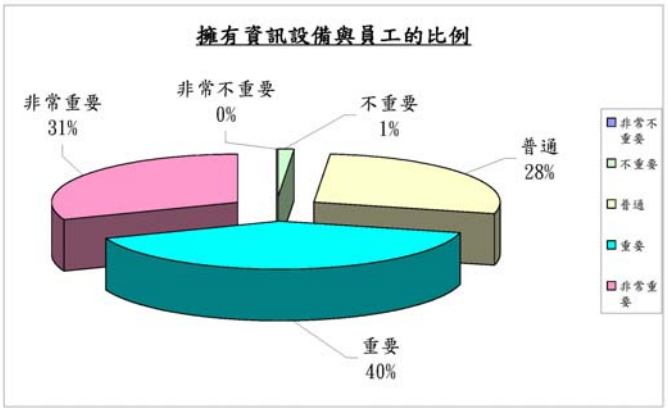
資料來源：本計畫自行整理

圖38 問卷調查－安全概念融入組織文化之程度統計



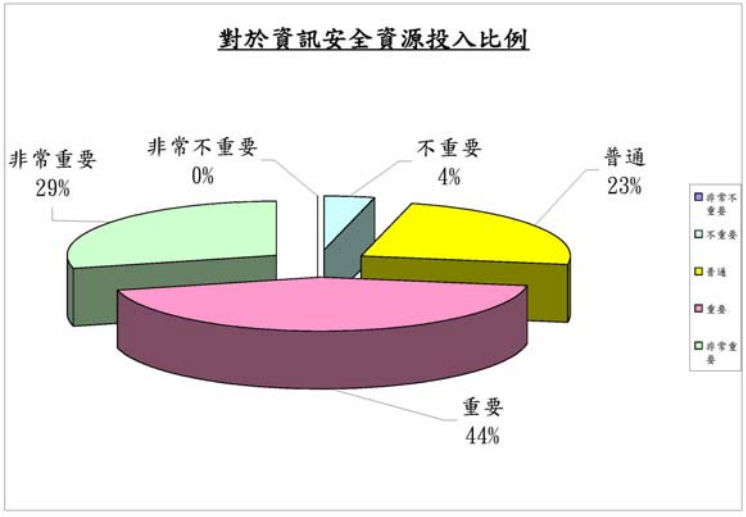
資料來源：本計畫自行整理

圖39 問卷調查－風險評鑑作業之程度統計



資料來源：本計畫自行整理

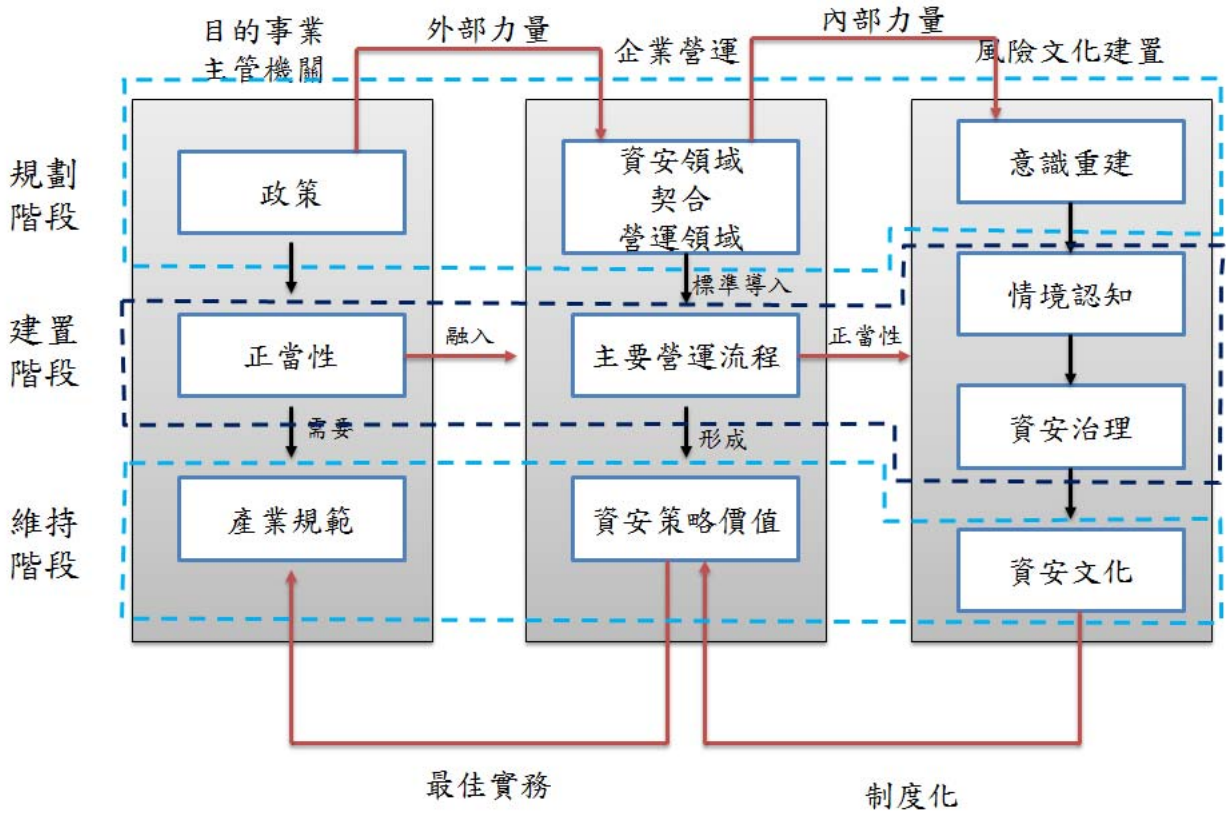
圖40 問卷調查－資訊設備與員工比例統計



資料來源：本計畫自行整理

圖41 問卷調查－資訊安全資源投入比例統計

3.4.6. 結構化方程模式分析



資料來源：本計畫自行整理

圖42 風險意識文化建置整體過程

本計畫之個案研究發現：當政府擬定或通過新的法規或政令時，將對企業營運產生外部趨動之動能(例如使組織產生建置 ISMS 之動機或壓力)，促使企業面臨改變(例如資安標準之導入)並迫使企業改變或遵循法規與政令的正當性之形成。

本計畫將個案研究發現之風險意識文化建置整體過程，依個案導入 ISMS 之過程，劃分為規劃階段、建置階段及維持階段，並以此三階段為結構化方程模式之自變項(外因潛在變項)，探討組織成員對組織資訊環境之認知；亦即，在組織導入 ISMS 的過程中，規劃、建置及維護等階段是否具有交互影響性。故本計畫提出下列研究假說，詳見表 17 所示。

表17 結構化方程模式之研究假說

H1	在建置 ISMS 的過程中，規劃階段與建置階段互有相關性
H2	在建置 ISMS 的過程中，建置階段與維持階段互有相關性
H3	在建置 ISMS 的過程中，維持階段與建置階段互有相關性

3.4.6.1. 研究變數定義與衡量

本計畫之結構化方程模式分析乃藉由個案研究之發現為依據，以李克特五點量表發展問卷，以 1 到 5 代表非常不重要至非常重要，測量問卷填答者對於企業資訊環境所認知的重要程度。

3.4.6.1.1. 規劃階段

本計畫之個案研究發現：政府擬定或通過新的法規或政令時，將對企業營運產生外部趨動之動能(例如使組織產生建置 ISMS 之動機或壓力)，促使企業面臨改變(例如資安標準之導入)，詳見表 18 所示。

表18 規劃階段－結構方程模式之變項命名

外因潛在變項	問卷編號	問卷摘要	觀測變數
規劃階段(F1)	B1SD	營運業務所需之資訊化程度	資訊化(F11)
	B2SD	對上述資訊系統之依賴程度	系統依賴度(F12)
	B3SD	擁有資訊設備與員工的比例	設備與員工比例(F13)
	B15SD	資料保護受到損害之重視程度	資料保護受損(F14)
	B16SD	對於安全影響業務運作之重視程度	影響業務運作(F15)
	B17SD	對於安全相關法律規程之遵循程度	法規遵循(F16)
	B18SD	安全造成人員傷亡之重視程度	人員傷亡(F17)
	B19SD	安全損害組織信譽之重視程度	組織信譽(F18)

資料來源：本計畫自行整理

3.4.6.1.2. 建置階段

本計畫之個案研究發現：組織營運的相關業務，可能因資安事件的發生造成營運的損失時，組織會自發性的導入相關資安標準，而其導入範圍將涵蓋組織目前關鍵的營運流程。在執行營運業務時，將正確的認知與行為帶入工作情境當中，使之達到資安意識與工作情境之結合，並由組織內部系統化的控制措施與管理機制，使個人層次提升至整體資安的意識，以維護組織整體的資訊安全。亦即，使得組織對於資安管控更具整體性，以降低風險發生時的營運損失,增強營運持續運作的穩定性,詳見表 19 所示。

表19 建置階段－結構方程模式之變項命名

外因潛在變項	問卷編號	問卷摘要	觀測變數
建置階段(F2)	B6SD	以系統化的方法，實施資安管理程度	系統化管理(F21)
	B7SD	對於企業營運過程之風險進行評鑑作業之程度	風險評鑑(F22)
	B10SD	對於營運安全維護，訂定明確之權責區分與作業程序之程度	權責區分(F23)
	B8SD	營運安全包含人員、實體、系統及營運持續等重視之程度	營運持續(F24)

資料來源：本計畫自行整理

3.4.6.1.3. 維持階段

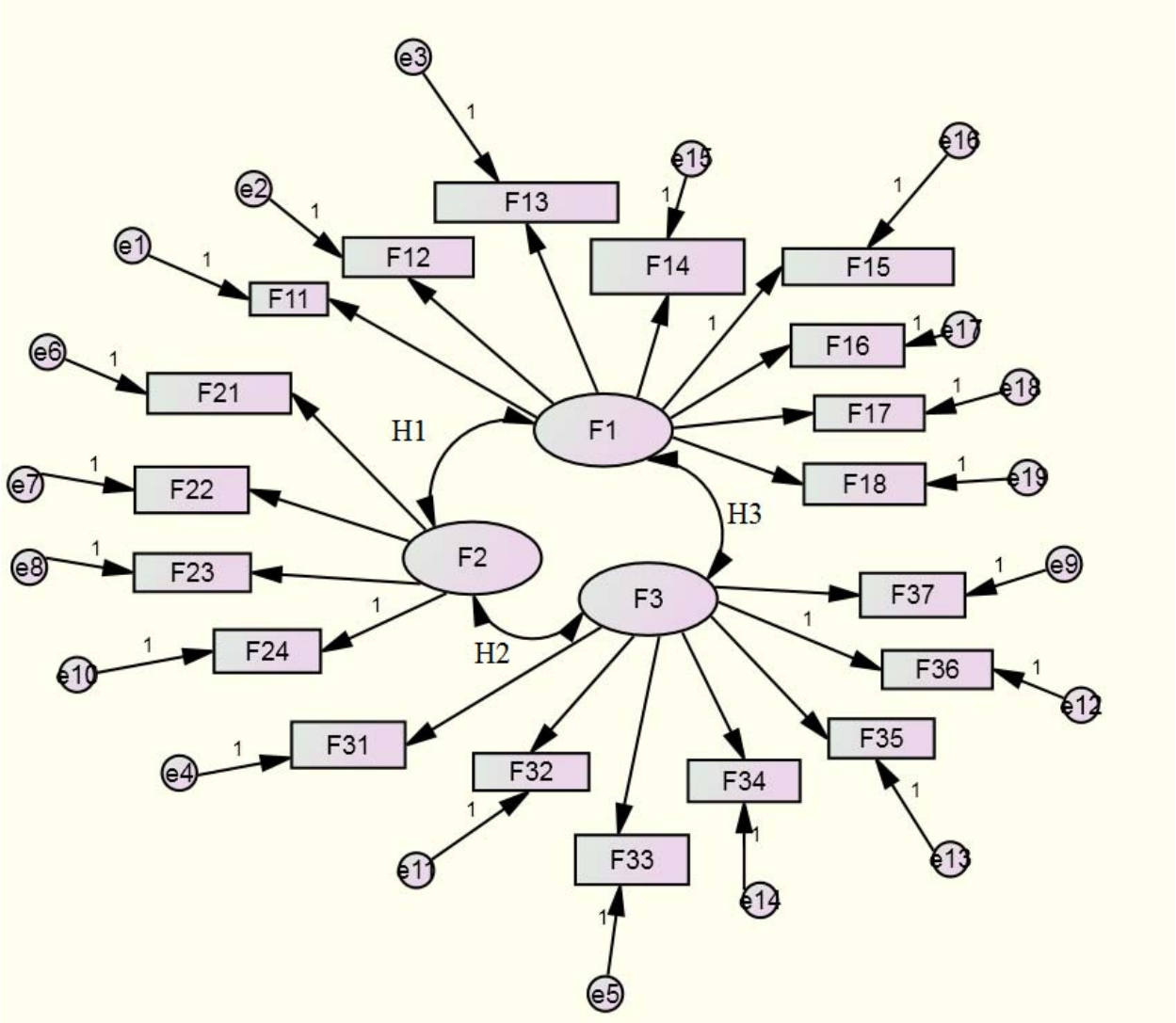
本計畫之個案研究發現：組織成員若落實 ISMS 的制度與流程，將改變舊有缺乏資安思維的作業流程與行為準則。最後，將資安標準所提及的準則與規範，在組織內部進行制度化；亦即，將 ISMS 內化為組織制度，並產生資安策略的價值，並提供產業或政府最佳實務之典範，詳見表 20 所示。

表20 維持階段－結構方程模式之變項命名

外因潛在變項	問卷編號	問卷摘要	觀測變數
維持階段(F3)	B9SD	對於員工之安全認知訓練程度	認知訓練(F31)
	B4SD	對委外作業安全之重視程度。	委外安全(F32)
	B5SD	對於資訊安全資源投入比例	資源投入(F33)
	B11SD	對於客戶個人資料之保護程度	個人資料(F34)
	B12SD	安全概念已融入貴公司組織文化之程度	資安文化(F35)
	B13SD	法律對於貴公司落實資訊安全意願的影響程度	法律影響(F36)
	B14SD	主管機關的政策對於貴公司資源投入資訊安全的影響程度	主管機關政策(F37)

資料來源：本計畫自行整理

3.4.6.2. 模式修正



資料來源：本計畫自行整理

圖43 本計畫修正前 SEM 模型

本計畫為使整體結構化模式趨於配適(fit)，剔除不顯著變項之模式，故將觀測變數之路徑因素負荷量未達 0.7 以上者予以剔除(張紹勳，2001)，詳見圖 43 所示。

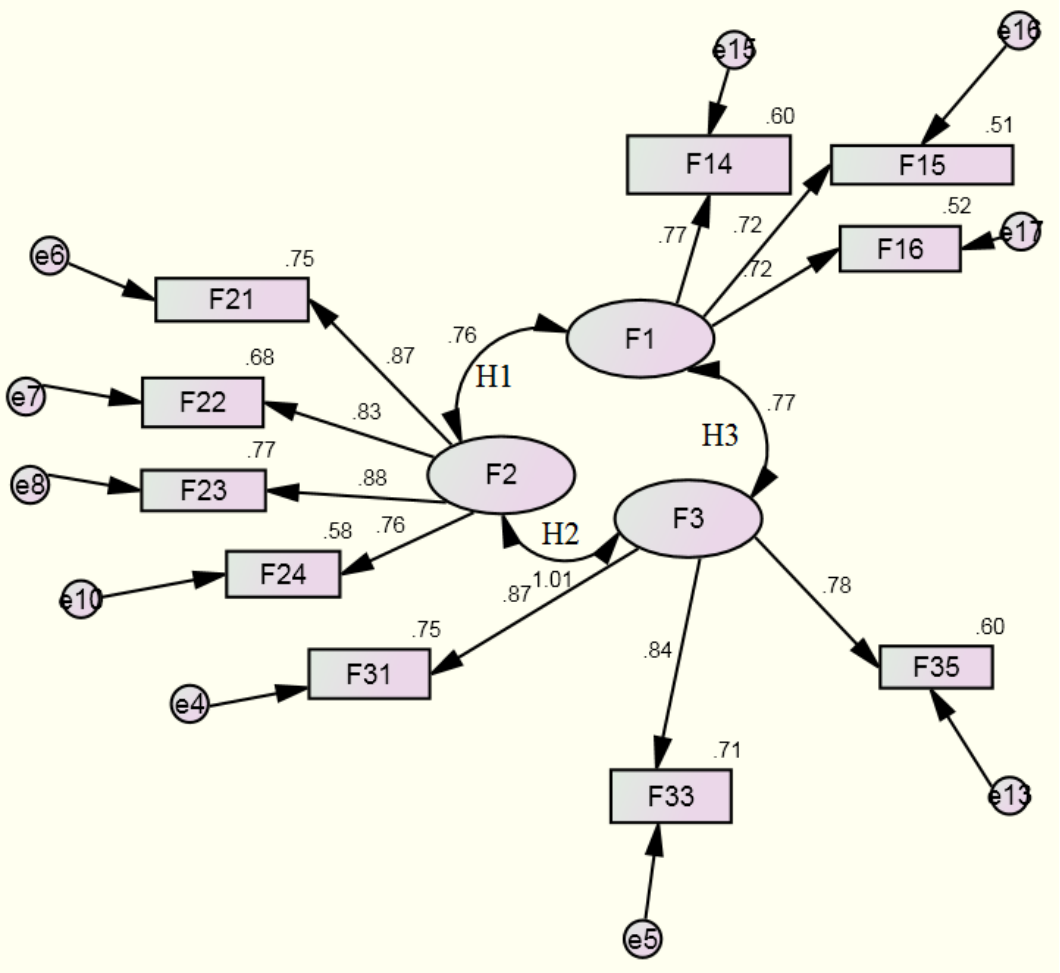
亦即，測量系統信度，標準化測量路徑係數都要大於 0.7(陳順宇，2007)，詳見表 21 所示。

表21 結構方程模式變項之判斷

外因潛在變項	觀測變數	因素負荷量	判斷標準
規劃階段(F1)	資訊化(F11)	0.43	剔除
	系統依賴度(F12)	0.43	剔除
	設備與員工比例(F13)	0.54	剔除
	資料保護受損(F14)	0.76	保留
	影響業務運作(F15)	0.74	保留
	法規遵循(F16)	0.74	保留
	人員傷亡(F17)	0.65	剔除
	組織信譽(F18)	0.60	剔除
建置階段(F2)	系統化管理(F21)	0.88	保留
	風險評鑑(F22)	0.81	保留
	權責區分(F23)	0.86	保留
	營運持續(F24)	0.77	保留
維持階段(F3)	認知訓練(F31)	0.73	保留
	委外安全(F32)	0.71	保留
	資源投入(F33)	0.85	保留
	個人資料(F34)	0.64	剔除
	資安文化(F35)	0.77	保留
	法律影響(F36)	0.67	剔除
	主管機關政策(F37)	0.59	剔除

資料來源：本計畫自行整理

剔除不顯者變項後之結構化方程模式，詳見圖 44 所示。



資料來源：本計畫自行整理

圖44 本計畫修正後 SEM 模型

規劃階段主要為資料保護受損(F14)：資料保護受到損害之重視程度；影響業務運作(F15)：對於安全影響業務運作之重視程度；法規遵循(F16)：對於安全相關法律規程之遵循程度。

建置階段主要為系統化管理(F21)：以系統化的方法，實施資安管理程度；風險評鑑(F22)：對於企業營運過程之風險進行評鑑作業之程度；權責區分(F23)：對於營運安全維護，訂定明確之權責區分與作業程序之程度；營運持續(F24)：營運安全包含人員、實體、系統及營運持續等重視之程度。

維持階段主要為認知訓練(F31)：對於員工之安全認知訓練程度；資源投入(F33)：對於資訊安全資源投入比例；資安文化(F35)：安全概念已融入

公司組織文化之程度。

3.4.6.3. 信度檢測

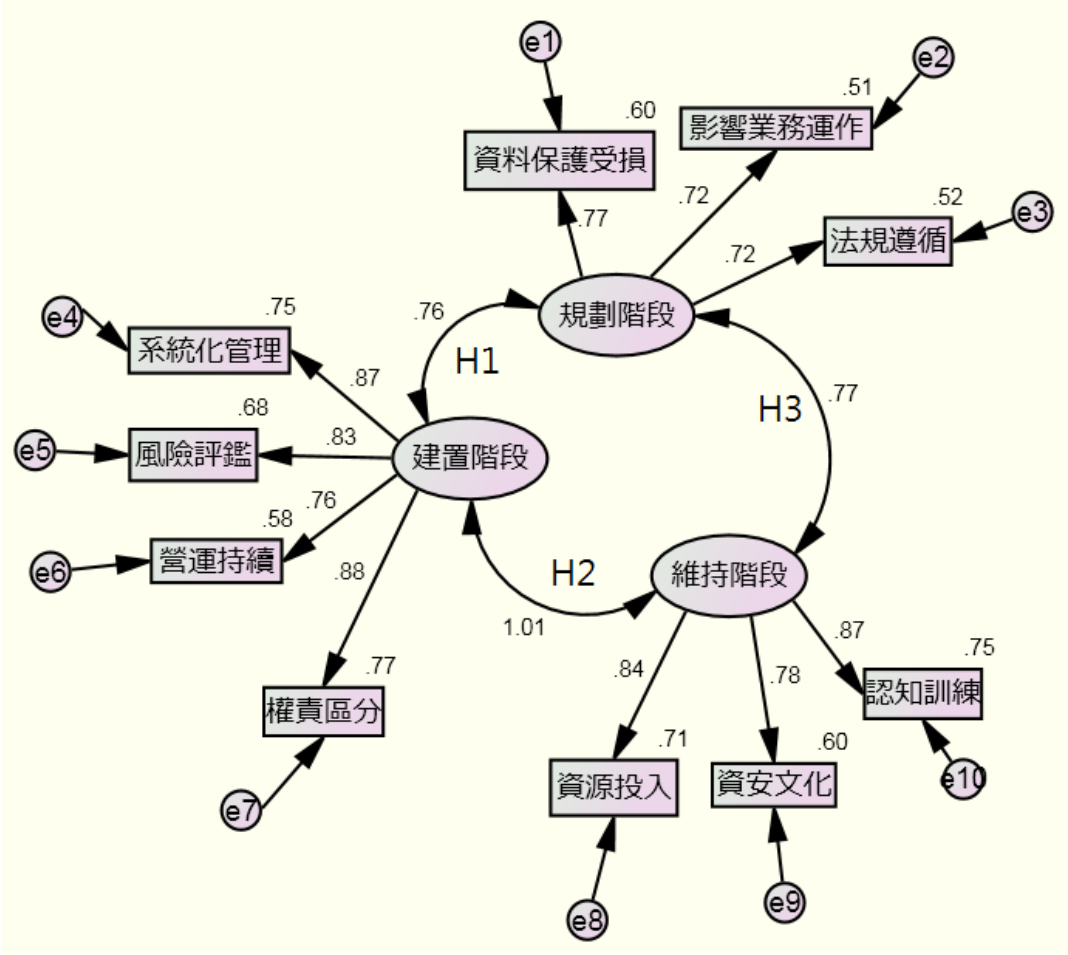
本計畫針對收集到的 149 份有效樣本針對問卷第一部分實施信度分析，透過各構面之信度分析所得信度係數，各因素的α值皆有適當的水準，各項皆大於 0.7，顯示具有相當高的內部一致性，詳見表 22 所示。

表22 問卷信度分析

構面	子構面	Cronbach's α
規劃階段	資料保護受損	0.784
	影響業務運作	
	法規遵循	
建置階段	系統化管理	0.898
	風險評鑑	
	權責區分	
	營運持續	
維持階段	認知訓練	0.870
	資源投入	
	資安文化	

資料來源：本計畫自行整理

3.4.6.4. 模式適配度分析



資料來源：本計畫自行整理

圖45 本計畫實證模型

3.4.6.4.1. 整體模式適配度

在適配度指標的判斷上除 RMSEA 值、AGFI 值及 CN 值未達標準外，其餘適配度的指標所呈現的統計量均達到標準值，可見整體模式的適配度尚稱理想；亦即，模式之路徑圖與實際觀察資料之適配度尚可，故本計畫所提的因果模式圖假設與研究假說獲得統計上的支持，詳見表 23 所示。

表23 整體模式適配度說明表

統計檢定量	適配的標準或臨界值	檢定結果數據	模式適配判斷
絕對適配度指數			
卡方值	P<0.05(達顯著水準)	84.923	是
卡方比值率	<3	2.654	是
GFI 值	>0.90 以上	0.900	尚且適當
RMR 值	<0.05	0.024	是
RMSEA 值	<0.08	0.106	否
增值適配度指數			
AGFI 值	>0.90 以上	0.828	否
NFI 值	>0.90 以上	0.924	是
RFI 值	>0.90 以上	0.894	尚且適當
IFI 值	>0.90 以上	0.951	是
TLI 值	>0.90 以上	0.931	是
CFI 值	>0.90 以上	0.951	是
簡約適配度指數			
PGFI 值	>0.50 以上	0.524	是
PNFI 值	>0.50 以上	0.657	是
PCFI 值	>0.50 以上	0.676	是
CN 值	>200	94	否
模式內在品質			
估計的參數	P<0.05		是
誤差變異	均達顯著且沒有負的誤差變異	均達顯著且沒有負的誤差變異	是
因素負荷量	0.50<值<0.95	0.72 至 0.88	是

資料來源：本計畫自行整理

3.4.6.4.2. 模式內在適配度

本計畫以最大概似法(Maximum Likelihood Estimates)求出之非標準化的各項估計值，而在所有的估計參數 P 中，任一估計參數均達到顯著水準($p<0.05$), 顯示模式的內在品質良好，詳見表 24 所示。

表24 非標準化之各項估計值

		Estimate	S.E.	C.R.	P
風險評鑑	<--- 建置階段	0.976	0.073	13.400	***
營運持續	<--- 建置階段	0.724	0.063	11.565	***
權責區分	<--- 建置階段	1.000			
系統化管理	<--- 建置階段	0.976	0.066	14.681	***
法規遵循	<--- 規劃階段	1.011	0.132	7.639	***
資安文化	<--- 維持階段	1.000			
認知訓練	<--- 維持階段	1.233	0.103	11.921	***
保護受到損害	<--- 規劃階段	1.107	0.138	7.998	***
資源投入	<--- 維持階段	1.150	0.101	11.412	***
影響業務運作	<--- 規劃階段	1.000			

註：***，表示其值小於 0.001

資料來源：本計畫自行整理

本計畫以最大概似法求出標準化後的各項估計值，而潛在變數與其指標變數間的因素負苛量均在 0.70 以上，表示模式的內在品質良好，詳見表 25 所示。

表25 標準化之各項估計值

			Estimate
風險評鑑	<---	建置階段	0.826
營運持續	<---	建置階段	0.759
權責區分	<---	建置階段	0.877
系統化管理	<---	建置階段	0.865
法規遵循	<---	規劃階段	0.724
資安文化	<---	維持階段	0.777
認知訓練	<---	維持階段	0.868
保護受到損害	<---	規劃階段	0.772
資源投入	<---	維持階段	0.840
影響業務運作	<---	規劃階段	0.717

資料來源：本計畫自行整理

規劃、建置及維持階段，三組間的共變異數為 0.239、0.206、0.433，p 值小於 0.001，均達到顯著水準，詳見表 26 所示。

表26 自變項間之共變異數

	Estimate	S.E.	C.R.	P
建置階段 <--> 規劃階段	0.239	0.042	5.689	***
規劃階段 <--> 維持階段	0.206	0.038	5.477	***
建置階段 <--> 維持階段	0.433	0.062	7.035	***

註：***，表示其值小於 0.001

資料來源：本計畫自行整理

變數「建置階段」與變數「規劃階段」的相關為 0.760、變數「規劃階段」與變數「維持階段」的相關為 0.770、變數「建置階段」與變數「維持階段」的相關為 1.011，故三組潛在變數間的相關均達顯著，亦即研究假說

成立，詳見表 27 所示。

表27 自變項間之相關係數

	Estimate
建置階段 <--> 規劃階段	0.760
規劃階段 <--> 維持階段	0.770
建置階段 <--> 維持階段	1.011

資料來源：本計畫自行整理

3.4.7. 研究發現

本計畫採用結構化方程模式驗證規劃階段、建置階段及維持階段之因果關係，並進一步確認整體模型的適合度，並經過驗證模式的路徑分析時，三條假設路徑均可成立。研究假說之結果詳見表 28 所示。

表28 結構化方程模式之統計推論

	研究假說	統計推論
H1	在建置 ISMS 的過程中，規劃階段與建置階段互有相關性	成立
H2	在建置 ISMS 的過程中，建講階段與維持階段互有相關性	成立
H3	在建置 ISMS 的過程中，維持階段與規劃階段互有相關性	成立

資料來源：本計畫自行整理

因此，組織在建置 ISMS 的過程中，將進行「規劃」、「建置」及「維護」等階段，且各階段間具有交互影響的作用。例如規劃階段時之過程或產出將會影響建置階段與維持階段，而目前組織進行之建置階段或維護理階段的產出，將會影響組織進行下一次更大規模的規劃階段；亦即，在建置 ISMS 對於企業來說無法一蹴即成，必需進行規劃、建置及維護等階段性的任務，企業需經由不斷地階段性循環，以完成 ISMS 的建置。

規劃階段，包含「資料保護受損」、「影響業務運作」及「法規遵循」；

換言之，組織成員在建置 ISMS 之規劃的認知，即是避免組織的資料保護措施受到損害與避免資安風險的發生影響組織正常營運，且需遵循安全之相關法律規程進行規劃。

建置階段，包含「系統化管理」、「風險評鑑」、「營運持續」及「權責區分」；換言之，組織成員在建置 ISMS 時建構的認知，即是藉由系統化的方法，將組織營運的過程進行風險評鑑，以建置 ISMS 與實施資安管理制度，並建立明確的權責區分與作業程度，以利於組織面臨已知或未知風險時能維持營運。

維持階段，包含「認知訓練」、「資源投入」及「資安文化」；換言之，組織成員在管理 ISMS 的認知，即是高層資源的投入與整體員工的資安認知訓練所形成的資安文化。

3.4.8. 重要度績效分析法

本計畫應用 Martilla and James[41]所提出的重要度績效分析法(Importance Performance Analysis, IPA)分析概念，藉由問卷的填答以調查組織對於資安控制措施的認知程度與內部實際的實施程度。本計畫 IPA 分析步驟如下所述。

- 步驟一：由問卷填答者針對資安控制措施各項目 j 評價其重要程度，並比較此控制措施在組織內部的相對實施程度，評分標準採用李克特五點尺度，各為 1-5 分。
- 步驟二：針對各填答問卷之認知重要程度之評估值與相對實際的實施程度之評估值進行編碼。設 b_{jp} 與 c_{jp}, p=1, 2, …, n 分別代表決策群體第 p 個成員賦予資安控制措施 j 之認知重要程度評估值與相對實際實施程度評估值，並針對各資安控制措施 j 之問項進行編碼，b_{jp} 與 c_{jp} 的範圍最低為 1，最高為 5；$1 \le b_{jp} \le 5$ 與 $1 \le c_{jp} \le 5$。
- 步驟三：以幾何平均數彙整決策群體之平均意見，且使用幾何平均數

$G = \sqrt[n]{\prod_{i=1}^{n} x_i} = \sqrt[n]{x_1 \cdot x_2 \cdots x_n}$較算數平均數能突顯平均彙整之結果。定義第 j 個資安控制措施之認知重要程度評估值與相對內部實際實施程度評估值的幾何平均數分別為：

– $b_j = (\prod_{p=1}^{n} \quad \prod_{p=1}^{n} \quad b_{jp})^{1/n}$

– $c_j = (\prod_{p=1}^{n} \quad \prod_{p=1}^{n} \quad c_{jp})^{1/n}$

- 步驟四：以內部實際實施程度為水平軸，認知重要程度為垂直軸，將各項資安控制措施之評比分數標示於象限中，並將此象限分成四部分：

  – 象限一：繼續維持(Keep Up the Good Work)

  – 象限二：優先改善(Concentrate Here)

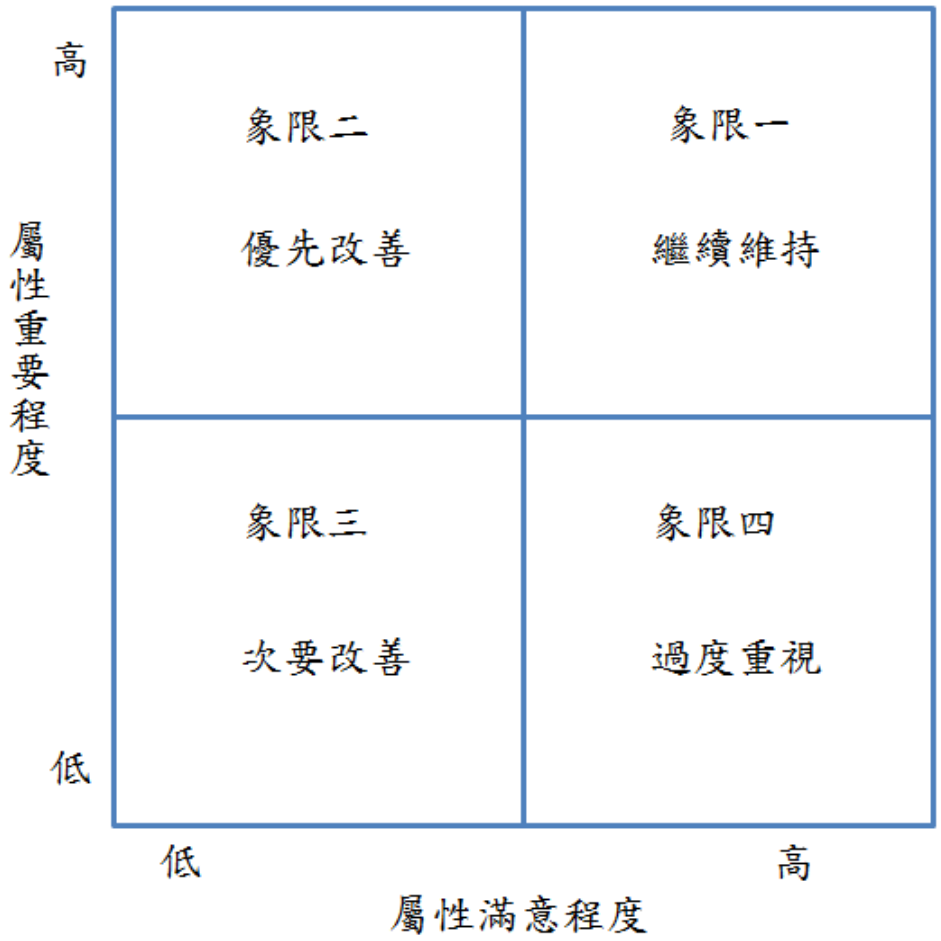
  – 象限三：次要改善(Low Priority)

  – 象限四：過度重視(Possible Overkill)

本計畫之 IPA 分析法採用高門檻值，即在認知重要程度評估值與相對內部實際實施程度評估值以超過李克特尺度 4(前 80%)，亦即各項資安控制措施之認知重要程度評估值與相對內部實際實施程度評估值皆需大於普通，代表該組織對於資安確實有良好的認知與具規模的實施資安控制措施，故：

- 「繼續維持」之設定標準($b_j \geq 4$ 與 $c_j \geq 4$)
- 「優先改善」之設定標準為 $b_j \geq 4$ 與 $c_j < 4$
- 「次要改善」之設定標準為 $b_j < 4$ 與 $c_j < 4$
- 「過度重視」之設定標準為 $b_j < 4$ 與 $c_j \geq 4$

重要度--滿意度矩陣，詳見圖 46 所示：



資料來源：[41]

圖46 重要度--滿意度矩陣

- 象限一，表示認知重要程度與實際實施程度皆相對偏高，此部分的資安控制措施應繼續維持，視為組織競爭優勢所在。
- 象限二，表示認知重要程度高，但實際實施程度低，此部分為該組織應優先改善其資安控制措施。
- 象限三，表示認知重要程度與實際實施程度皆相對偏低，故為次要改善之部分。
- 象限四，表示認知重要程度低，但實際實施程度高，代表目前該組織過度重視其資安控制措施，應將組織資源移至其他極需改善的部分。

然而，落入四大象限中的資安控制措施僅代表其應改善之排列順序，

不代表控制措施在該組織重要性的程度。

3.4.8.1. 第一階段問卷與重要性分析說明

本計畫第一階段問卷採用李克特五點尺度(Likert's 5-point scale)評分方式，分別由填答者針對問項之重要程度與實施程度給予評分，本問卷評估尺度為 1，代表非常不重要或完全沒有實施，程度依序遞增，評估尺度為 5，代表非常重要或完全落實實施。

問卷調查期間為民國 100 年 5 月。在問卷發放與回收方面，共發放 937 份，有效回收問卷共 211 份，故有效回收率為 23.03%。問卷填答之第一類電信約佔 28.4%；第二類電信佔 33.2%；傳播事業佔 38.4%。

3.4.8.1.1. 信效度分析

本研究在抽取共用因素時，採用主成分分析(Principal Component Analysis)，由 p 個變項產生 p 個成分，並選取變異量大者為重要成分，忽略變異量小而不重要之成分(Gorsuch, 1988)，以進行效度建構與資料簡化，詳見表 29 所示。

本研究因素分析之過程，簡述以下步驟：

- 步驟一：計算變項間相關矩陣：以原始資料為數據，交由電腦轉化為相關矩陣，以進行因素分析。
- 步驟二：估計因素負荷量：以主成分分析法為因素抽取的方法。而 SPSS 使用手冊中，建議多採用主成分分析法進行因素分析。
- 步驟三：決定轉軸方法：以最大變異法(Varimax)為轉軸方法。其目的在於改變問卷題項各因素負荷量之大小。
- 步驟四：決定因素與命名：轉軸後決定因素之數量，以較少的因素層面，獲得較大的解釋能力。

表29 因素分析法之信效度

因素構面	題號	衡量變項	因素負荷量	特徵值	解釋變異量%	累計解釋變異量%	α信度係數
因素一	C11.1SD	委外廠商定期稽核	0.856	6.535	27.230	27.230	0.938
	C19.1SD	稽核日誌紀錄異常	0.828				
	C19.2SD	記錄管理者與操作者活動	0.827				
	C11.2SD	委外變更管理評鑑風險	0.818				
	C20.1SD	正式註冊與註銷程序	0.763				
	C21.2SD	使用者桌面淨空與螢幕淨空	0.677				
	C25.1SD	防範使用行動計算及通信設施風險	0.636				
	C30.1SD	軟體套件變更限制	0.594				
	C24.2SD	資訊與系統存取控制敏感性系統有隔離	0.500				
因素二	C17.2SD	工作場域間傳送資訊保護	0.833	5.642	23.510	50.740	0.941
	C33.2SD	資安事故中學習	0.795				
	C17.1SD	建立保護協議	0.763				
	C33.1SD	資安事故管理責任與程序	0.720				
	C32.1SD	資安事件適切的通報管道	0.707				
	C32.2SD	通報可疑的資安弱點	0.680				
	C26SD	新系統資安控制措施	0.631				
	C16.2SD	正式的汰換程序	0.539				

因素構面	題號	衡量變項	因素負荷量	特徵值	解釋變異量%	累計解釋變異量%	α信度係數
	C16.1SD	管理可攜式媒體	0.514				
因素三	C1SD	管理階層支持	0.818	3.417	14.236	64.976	0.879
	C5SD	聘僱契約陳述資安責任	0.734				
	C2SD	第三方的協議	0.722				
	C4SD	機密等級的標示	0.667				
因素四	C18.2SD	防止不完整傳輸未經授權複製	0.954	2.375	9.895	74.871	0.989
	C18.1SD	保護未經授權的揭露與修改	0.948				

資料來源：本計畫自行整理

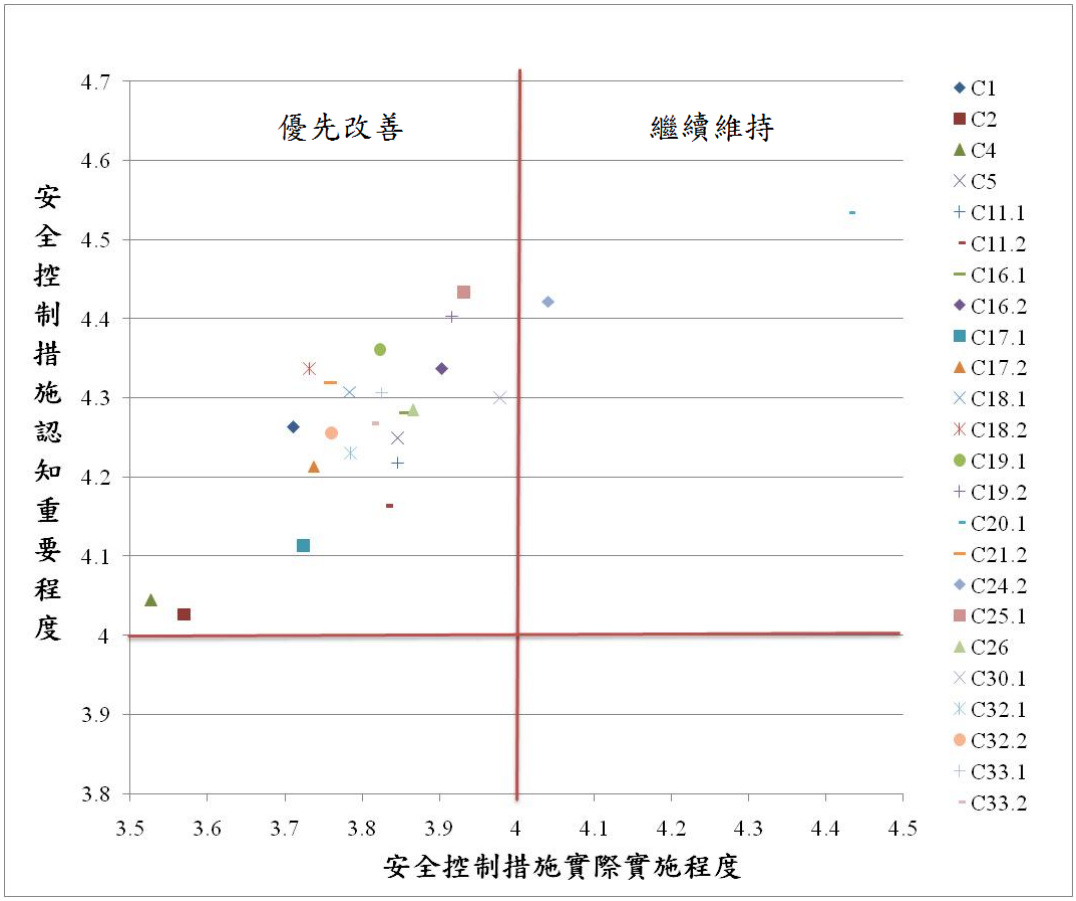
因素一之信度係數為 0.983、因素二之信度係數為 0.941、因素三之信度係數為 0.879、因素四之信度係數為 0.989。當信度係數值愈接近 1，表示量表或測驗的信度愈高，故本研究各因素之信度係數皆已達至高可信度。

由 62 個題項共萃取出四個因素構面(24 個題項)，累積解釋變異量為 74.871%，且各題項在所屬的因素構面中，其因素負荷量皆大於 0.5，同時在其他因素構面中皆小於 0.5，故在因素分析方法下，將問卷題項分成四個構面乃具備構念效度。

3.4.8.2. 第二階段問卷與重要度績效分析說明

本計畫之問卷由資安標準文件所提及之資安控制措施由專家意見選出 62 項題項，並針對其認知重要程度與實際實施程度進行評估，以檢核這些資安控制措施於組織內部是否重視？或是否落實？

經由因素分析之後，將 62 項問項簡化為 24 個題項，最後經 IPA 分析後顯示共有 22 項落入「優先改善」之區域，其餘 2 項落入「繼續維持」之區域，詳見圖 47 所示。



資料來源：本計畫自行整理

圖47　IPA 分析

問項落入優先改善區域與繼續維持區域之 IPA 分析結果，詳見表 30 所示。

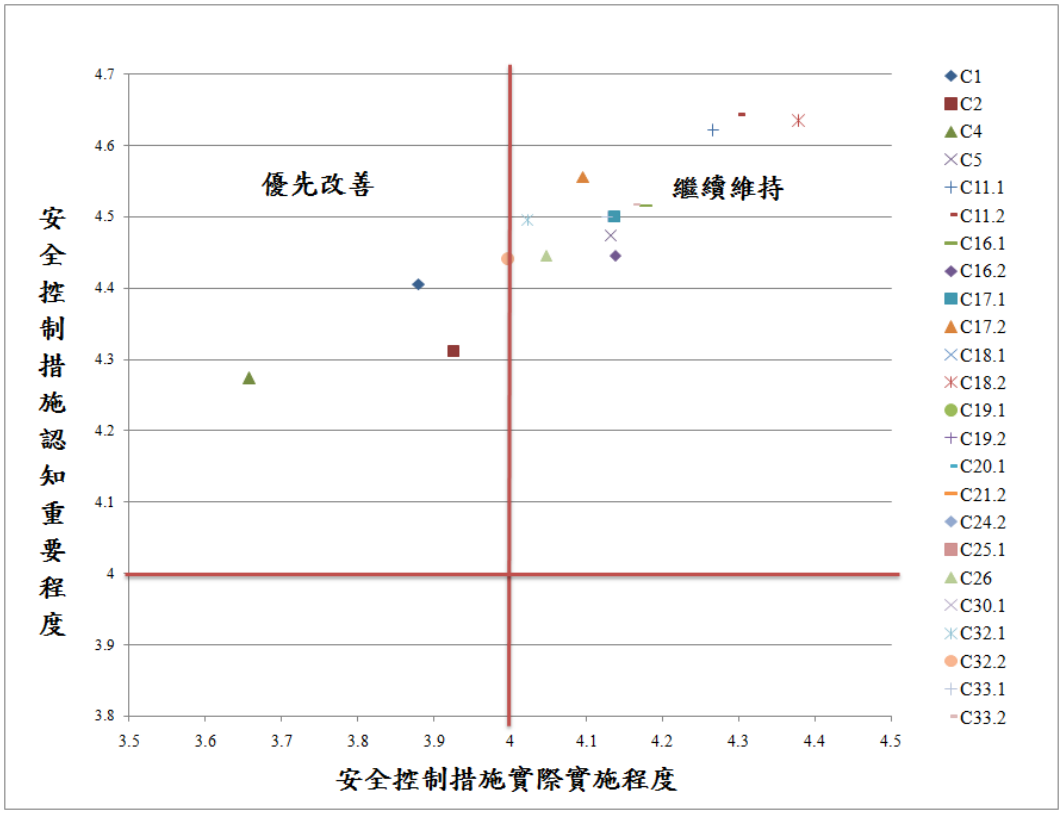
表30 IPA 分析結果

安全領域	題號	衡量變項	幾何平均數		分析結果
			認知程度	實施程度	
資訊安全組織	C1SD	管理階層支持	4.263	3.711	優先改善
	C2SD	第三方的協議	4.026	3.570	優先改善
資產管理	C4SD	機密等級的標示	4.045	3.527	優先改善
人力資源安全	C5SD	聘僱契約陳述資安責任	4.249	3.846	優先改善
	C11.1SD	委外廠商定期稽核	4.218	3.846	優先改善
	C11.2SD	委外變更管理評鑑風險	4.163	3.832	優先改善
通訊與作業管理	C16.1SD	管理可攜式媒體	4.281	3.856	優先改善
	C16.2SD	正式的汰換程序	4.337	3.903	優先改善
	C17.1SD	建立保護協議	4.113	3.724	優先改善
	C17.2SD	工作場域間傳送資訊保護	4.213	3.738	優先改善
	C18.1SD	保護未經授權的揭露與修改	4.307	3.783	優先改善
	C18.2SD	防止不完整傳輸未經授權複製	4.337	3.731	優先改善
存取控制	C19.1SD	稽核日誌紀錄異常	4.361	3.823	優先改善
	C19.2SD	記錄管理者與操作者活動	4.402	3.916	優先改善
	C20.1SD	正式註冊與註銷程序	4.534	4.430	繼續維持
	C21.2SD	使用者桌面淨空與螢幕淨空	4.319	3.759	優先改善
	C24.2SD	資訊與系統存取控制敏感性系統有隔離	4.422	4.040	繼續維持
	C25.1SD	防範使用行動計算及通信設施風險	4.433	3.932	優先改善
資訊系統獲取、開發及維護	C26SD	新系統資安控制措施	4.284	3.866	優先改善
	C30.1SD	軟體套件變更限制	4.300	3.979	優先改善
資安事故管理	C32.1SD	資安事件適切的通報管道	4.230	3.785	優先改善
	C32.2SD	通報可疑的資安弱點	4.255	3.761	優先改善
	C33.1SD	資安事故管理責任與程序	4.306	3.825	優先改善
	C33.2SD	資安事故中學習	4.268	3.813	優先改善

資料來源：本計畫自行整理

第一類電信事業對於資訊安全之控制措施，明顯可以看出已落實之程

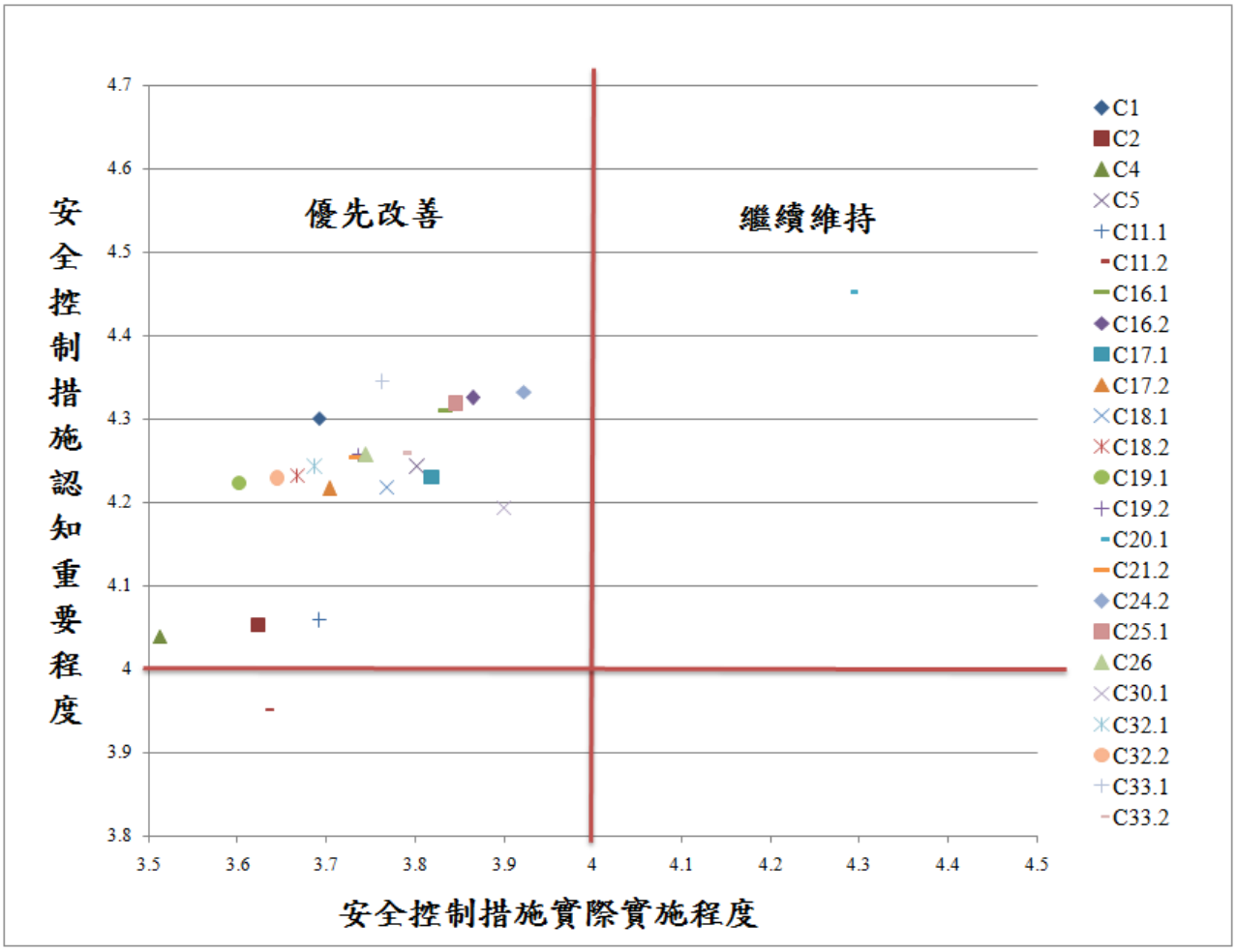
度較高，可能是基於產業之特性，原本就對於電信系統之機密性、完整性及可用性之要求較高，詳見圖 48 所示。



資料來源：本計畫自行整理

圖48　第一類電信 IPA 分析

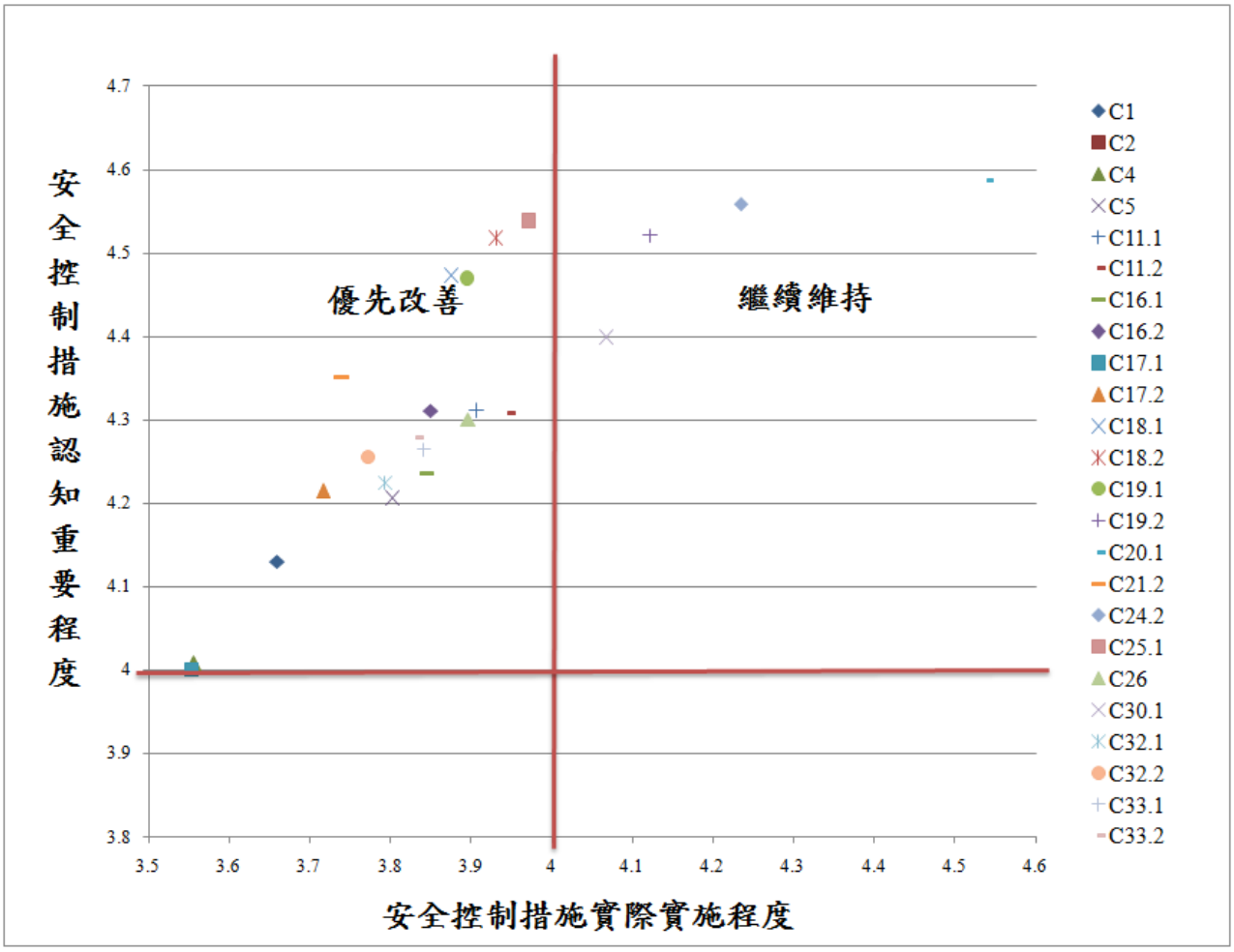
第二類電信事業對於資訊安全控制措施之認知程度，基本上是認為重要的，但是落實程度則有待改善，大部分之問項均落於優先改善象限，顯見與第一類電信事業有明顯之落差，詳見圖 49 所示。



資料來源：本計畫自行整理

圖49　第二類電信 IPA 分析

傳播事業事業對於資訊安全控制措施之認知程度，基本上是認為重要的，但是落實程度則有待改善，大部分之問項均落於優先改善象限，顯見與第一類電信事業有明顯之落差，但落實程度略高於第二類電信事業，詳見圖50所示。



資料來源：本計畫自行整理

圖50　傳播事業 IPA 分析

3.4.9. 研究發現

電信與傳播產業雖然大部分尚未導入資安標準與建置 ISMS，但仍對資安具有相當程度的瞭解，至於其瞭解或認知是否符合資安標準的要求，亦即檢核企業是否擁有正確的資安認知，同時檢核企業是否確實落實資安控制措施。因此，本計畫問卷設計乃著眼於資安認知與落實程度進行考量。

本計畫經由 IPA 分析後發現，落入「優先改善」區域之 22 個問項，大多數源於「資訊安全組織」、「資產管理」、「人力資源安全」、「通訊與作業管理」、「存取控制」、「資訊系統獲取、開發及維護」與「資訊安全事故管

理」等安全領域。因此，將針對上述安全領域之落入「優先改善」區域之問項進行建議，建議可以列為目的事業之最小限資安需求控制項目。

- 資訊安全事故管理：組織應建立資安管理的責任、程序及溝通管道，當資安事件發生時，組織成員才能依職務權責迅速通報與並處理資安事件，以降低損害。
- 存取控制：組織應建立金鑰管理制度，以確保成員在使用資訊設備時敏感性資訊不被洩露，如桌面與螢幕淨空政策並防範行動運算與通訊之風險。
- 人力資源安全：組織應告知所有使用資訊系統與設備之人員，包括員工、承包商及第三方使用者，訂定明確的規章管理辦法或契約，告知其資安責任。
- 資產管理：組織應依據分類結果標示機密等級與實施保護措施。
- 資訊系統獲取、開發及維護：組織應監控與定期稽核委外廠商所提供之服務與報告，並管理委外所造成之變更與變更後之風險評鑑。
- 通訊與作業管理：組織應對內部的工作場域間所傳送的資訊加以保護，並對外部之單位建立保護協議，並對可攜式的媒體(如：隨身碟)進行控管，建立內部的儲存媒體汰換程序，以防止敏感資訊被洩露。

3.5.個人資料保護法

3.5.1. 法案修正重點

「電腦處理個人資料保護法」於 84 年 8 月 1 日公布施行，當初規範非公務機關之適用主體有行業類別之限制，僅限於徵信業、醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業等八種行業，一般行業與個人均不受規範，保護之客體亦只限於經電腦處理之個人資料，不包括非經電腦處理之個人資料，對於保護個人資料隱私權益之規範顯有不足，故法

務部自 90 年起即積極進行相關修法工作，整理國內學界與實務界之修法意見，並參酌各國個人資料保護之立法例，經召開多次公聽會與研討會後，研擬「電腦處理個人資料保護法修正草案」，報請行政院審查，行政院院會業於 93 年 9 月 8 日通過，並函送立法院審議。

法務部所擬電腦處理個人資料保護法修正草案(修正後名稱為「個人資料保護法」)，歷經多年審查、協商及立法院「屆期不續審」，終於在 99 年 4 月 27 日三讀通過，使本法在保障個人資料隱私並兼顧新聞自由平衡下邁向新的里程碑。新法強化了個人資料揭露、查詢及更正等的自主控制，同時新法也採認「亞太經濟合作論壇(APEC)隱私保護綱領」所揭示的預防損害、告知及蒐集限制等原則，納入規範，以迎接個人資料保護全球化時代的來臨。

各目的事業主管機關均應積極履行法定監督職責，以確實防制個人資料之外洩，共同織起個人資料保護網絡，打造一個安全、安心及信賴的資訊生活環境。茲將法案修訂重點摘述如后：

3.5.1.1. 保護客體與適用主體的擴大

本次修正主軸在於擴大保護客體為所有個人資料(包含電腦處理與人工紙本的個人資料)，同時打破行業別限制，包括所有的法人、團體及個人對個人資料之蒐集、處理及利用均受規範，填補舊法對於個人資料保護不足的缺口，對於憲法保障個人資訊隱私權之目標，向前邁進一大步。

3.5.1.2. 隱私保護與新聞自由之平衡

本法乃個人資料保護之基本法律，惟對新聞自由的尊重，乃現代民主國家的重要表徵，為兼顧「個人隱私」與「新聞自由」之平衡，對於大眾傳播業者基於新聞報導之公益目的而蒐集個人資料，自得免為告知當事人；另外，與公共利益有關或個人資料取自於一般可得之來源者，非公務機關對個人資料亦得為蒐集或處理。

3.5.1.3. 民眾網路使用行為疑慮之釐清

有關臉書與部落格等張貼有他人合影的照片行為，如屬社交活動或家庭生活之目的範圍內，依新修正通過之個資法第 51 條第 1 項規定可排除本法適用，回歸民法適用。另外，對於在公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料，基於便利性與合照本身之共同使用合法目的亦甚明確，故亦排除在本法之適用範圍外。有關人肉搜索行為等，如非屬個資法第 51 條第 1 項社交活動或家庭生活之目的範圍內，仍應依第 19 條與第 20 條規定為蒐集、處理或利用；如屬公共利益有關或個人資料取自於一般可得之來源，則均屬合乎個資法蒐集或處理個人資料之規定。

3.5.1.4. 民、刑事及行政責任的加重與提高

修法的另一個重點，在於調整民事、刑事及行政罰責任內涵，同一事件民事損害賠償最高總額提高至新臺幣 2 億元，被害人不易或不能證明其實際損害額時，得請求法院依侵害情節以新臺幣 5 百元以上 2 萬元以下計算，且為方便當事人提起救濟，新法增加團體訴訟機制。刑事責任主要對於意圖營利之違法行為，提高刑責至 5 年以下有期徒刑得併科新臺幣 1 百萬元以下罰金，並改為非告訴乃論。行政裁罰部分，則提高罰鍰額度。

3.5.1.5. 特種個人資料蒐集限制

有關醫療、基因及犯罪前科等個人資料之保護，必須在符合法律明文規定的嚴格要件下，始得蒐集、處理或利用該等敏感性資料。

3.5.1.6. 其他重要修正

新法對於當事人之書面同意，有明確之定義，未來直接或間接蒐集個人資料前，原則上需盡到對當事人之「告知義務」。個人資料一旦外洩，資料保有者依法需查明後通知當事人，以防止損害擴大。另外，各行業利用個人資料首次行銷時，新法賦予當事人表示拒絕接受行銷之權利，且各行

業應提供表示拒絕接受行銷之方式並支付所需費用。

3.5.2. 相關重要條文摘錄

99 年 5 月 26 日總統令公布：將「電腦處理個人資料保護法」名稱修正為「個人資料保護法」；並修正條文，公布之。其中：

第五十五條規定，本法施行細則，由法務部定之。

第五十六條規定，本法施行日期，由行政院定之。

故個資法雖總統令公告，惟尚待法務部制定施行細則，後由行政院訂定正式施行日期。

由於新法擴大非公務機關之適用範圍，且在行政管理上亦相對提高其監督密度，另規定有相當高額之損害賠償金額，以每人每一事件新臺幣 5 百元以上 2 萬元以下計算，對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣 2 億元為限，但因該原因事實所涉利益超過新臺幣 2 億元者，以該所涉利益為限，引起各界戒慎恐懼，深怕萬一觸法，恐無力負擔高額之賠償金額。

以下摘錄本法相關法律授權與法定義務之重要條文，以使各界瞭解後續應遵行之權利與義務，以便儘早準備因應：

3.5.2.1. 法律授權

3.5.2.1.1. 主管機關職權

第二十七條 中央目的事業主管機關得指定非公務機關訂定「個人資料檔案安全維護計畫」或「業務終止後個人資料處理方法」。

前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。

上述條文明確律定「中央目的事業主管機關『得』指定非公務機關訂

定『個人資料檔案安全維護計畫』或『業務終止後個人資料處理方法』，雖非強制規定，但可明確推斷非公務機關應擬定「個人資料檔案安全維護計畫」，以資採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

3.5.2.1.2. 行政檢查

第二十二條 中央目的事業主管機關或直轄市、縣(市)政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。

針對非公務機關應特別注意，個資法除規定有損害賠償責任，多數人都忽略了主管機關的行政檢查權，以及伴隨行政檢查之後，馬上會面臨到的行政處分，包括裁處罰鍰與公布非公務機關之違法情形，及其姓名或名稱與負責人，亦即未經司法程序三審定讞，非公務機關即可能面臨信譽上之損失。

3.5.2.1.3. 行政處分

第二十五條 非公務機關有違反本法規定之情事者，中央目的事業主管機關或直轄市、縣(市)政府除依本法規定裁處罰鍰外，並得為下列處分：

一、禁止蒐集、處理或利用個人資料。

二、命令刪除經處理之個人資料檔案。

三、沒入或命銷毀違法蒐集之個人資料。

四、公布非公務機關之違法情形，及其姓名或名稱與負責人。

中央目的事業主管機關或直轄市、縣(市)政府為前項處分時，應於防制違反本法規定情事之必要範圍內，採取對該非公務機關權益損害最少之

方法為之。

3.5.2.1.4. 行政檢查結果公布

第二十六條 中央目的事業主管機關或直轄市、縣(市)政府依第二十二條規定檢查後，未發現有違反本法規定之情事者，經該非公務機關同意後，得公布檢查結果。

3.5.2.1.5. 行政罰鍰

第四十八條 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰：

一、違反第八條或第九條規定。

二、違反第十條、第十一條、第十二條或第十三條規定。

三、違反第二十條第二項或第三項規定。

四、違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。

3.5.2.2. 法定權利義務

3.5.2.2.1. 當事人權利

第三條 當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：

一、查詢或請求閱覽。

二、請求製給複製本。

三、請求補充或更正。

四、請求停止蒐集、處理或利用。

五、請求刪除。

3.5.2.2.2. 告知事項

第八條 公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：

一、公務機關或非公務機關名稱。

二、蒐集之目的。

三、個人資料之類別。

四、個人資料利用之期間、地區、對象及方式。

五、當事人依第三條規定得行使之權利及方式。

六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

3.5.2.2.3. 當事人之請求

第十條 公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。

第十一條 公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。

第十三條 公務機關或非公務機關受理當事人依第十條規定之請求，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。

公務機關或非公務機關受理當事人依第十一條規定之請求，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。

3.5.2.2.4. 查詢收費標準

第十四條 查詢或請求閱覽個人資料或製給複製本者，公務機關或非公務機關得酌收必要成本費用。

中央目的事業主管機關訂有收費標準者，應依其規定之標準收費，國家通訊傳播委員會，已於中華民國 99 年 10 月 19 日通傳營字第 09941062940 號令訂定「電信業及傳播業受理當事人查詢或請求閱覽個人資料或製給複製本收費標準」，規定電信業與傳播業受理當事人查詢或請求閱覽個人資料者，免予收費；請求製給複製本者，每件得酌收工本費新臺幣 10 元。

3.5.2.2.5. 個資檔案安全維護

第二十七條 非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

3.5.2.2.6. 損害賠償責任

第二十八條 公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。

第二十九條 非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。

3.5.2.2.7. 連帶罰鍰

第四十九條 非公務機關無正當理由違反第二十二條第四項規定者(拒絕接受行政檢查)，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣二萬元以上二十萬元以下罰鍰。

第五十條 非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。

3.5.3. 施行細則內容摘錄

表31 個資法施行細則內容摘錄

項次	內容概述
第三條	本法第二條第一款所稱得以間接方式識別該個人之資料，指僅以該資料不能識別，而與其他資料對照，並依此能識別該特定個人者。但查詢困難、需耗費過鉅或耗時過久始能特定者，不在此限
第四條	本法第二條第一款所稱病歷，應指下列各款資料： 一、醫師依醫師法執行業務所製作之病歷。 二、各項檢查、檢驗報告資料。 三、其他各類醫事人員執行業務所製作之紀錄。(衛生署提供) 本法第二條第一款所稱醫療之個人資料，指由醫事人員對個人罹患精神病、傳染病、性病、或其他足使個人人格遭受貶抑或歧視之疾病、傷害或殘缺所為診察、診斷或治療等行為所產生之個人資料。(衛生署提供) 本法第二條第一款所稱基因之個人資料，指由一段去氧核醣核酸構成，為生物控制特定功能之遺傳單位。(衛生署提供) 本法第二條第一款所稱性生活之個人資料，指性取向或性慣行之個人資料 本法第二條第一款所稱健康檢查之個人資料，指對於無明顯疾病症狀，非出於對特定疾病診斷或治療之目的，以醫療行為所為診察行為之全部或一部之總稱。(衛生署提供) 本法第二條第一款所稱犯罪前科之個人資料，指經法院判決有罪確定之紀錄
第五條	本法第二條第二款所稱依系統建立之個人資料，指經有組織之整理且可分類檢索之個人資料 本法第二條第二款所稱個人資料檔案，包括備份檔案及軌跡資料
第七條	本法第二條第四款所稱刪除，指使已儲存之個人資料自個人資料檔案中消失。但為事後查核、比對之安全或證明需要而留存之軌跡資料者，不在此限 本法第二條第四款所稱內部傳送，系指公務機關或非公務機關內部之資料傳遞
第十條	受公務機關或非公務機關委託蒐集、處理或利用個人資料之團體或個人，應依本法規定為之 前項情形，當事人行使本法之權利，應向委託機關為之

項次	內容概述
第十一條	委託他人蒐集、處理或利用個人資料之全部或一部時，委託人應對受託人為適當之監督 前項監督至少應包含下列事項： 一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間 二、受託人就個人資料安全、個人資料稽核、設備管理及其它安全維護事項所採取措施 三、再有受託者，其約定 四、受託人或其受僱人違反個人資料保護法規或委託契約條款時，應向委託人通知之事項 五、委託人對受託人保留指示之事項 六、委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除 七、委託人就委託事項應定期確認，其結果記錄之 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反本法或基於本法所發布之命令規定之情事，應立即通知委託人
第十二條	本法所稱適當安全維護措施或安全維護事項或適當之安全措施，係指公務機關或非公務機關為防止個人資料被竊取、竄改、損毀、滅失或洩漏，以善良管理人之注意義務，採取技術上與組織上之必要措施 前項必要措施，應包刮下列事項： 一、成立管理組織 二、界定保有個人資料之範圍 三、個人資料現況評估及短中長期因應措施 四、個人資料蒐集、處理及利用之程序 五、當事人行使權利之處理程序 六、資料安全 七、資料稽查 八、存取記錄與證據保存 九、人員管理與教育訓練 十、設備管理 十一、緊急應變措施及通報 十二、改善建議措施 十三、其他安全維護事項 第一項必要措施，以所須支出之費用與所欲達成之個人資料保護目的符合適當比例者為限
第十四條	本法第七條所稱書面意思之表示，以電子文件為之者，依電子簽章法之規定為之
第十五條	本法第七條第二項所謂單獨所為之書面意思表示，該意思表示如與其他意思表示於同一書面為之者，應以特別表明之方式為之

項次	內容概述
第十六條	依本法第八條及第九條所定告知之方式，得以書面、電話、傳真、電子郵件或其他通信方式為之
第十九條	本法(第九條第二項第四款、第十六條但書第五款、第十九條第一項第四款及第二十條但書第五款規定)所定資料經過處理後或依其揭露方式無從識別特定當事人，指個人資料以代碼、匿名或其他需費過鉅或耗時過久之方式始能予以辨識者
第二十三條	當事人依本法第十一條第一項規定向公務機關或非公務機關請求更正或補充其個人資料時，應提出足資釋明之證據
第二十四條	本法第十一條第二項至第四項所稱停止蒐集、處理或利用，指就該個人資料予以凍結(封鎖或封存)而產生停止蒐集、處理或利用之法律效果 公務機關或非公務機關依本法第十一條第三項主動或依當事人之請求，刪除該個人資料，有法令規定或契約約定之保存期限、有理由足認刪除將侵害當事人值得保護之利益、儲存方式特殊治不能刪除或耗費過鉅始能刪除或其他因執行職務或業務所必須或經當事人書面同意之情形之一者，得已停止處理或利用代替刪除
第二十六條	本法第十二條所定查明，係指確知公務機關或非公務機關違反本法規定致個人資料被侵害之事實 本法第十二條所定適當方式通知，係指查明後即時地以電話、信函、傳真、電子郵件、電子簡訊或其他通信方式通知。但耗費過鉅者，得以網際網路、刊載新聞紙、處所是當位置揭示或其他公告方式為之 本法第十二條通知當事人之內容，應包括第三人非法獲知個人資料之方式及降低負面影響之應對措施與建議
第二十九條	公務機關依本法第十七條規定為公開時，應於個人資料檔案蒐集、處理或利用後一個月內為之。變更時，亦同 前項公開方式應予以特定，並避免任意更換
第三十二條	保有個人資料檔案之公務機關，依本法第十八條規定，必須防止個人資料被竊取、竄改、毀損、滅失或洩漏，並應指定專人辦理安全維護事項 前項所稱專人，係指具有個人資料管理及維護之專業能力，且足以承擔機關日常性資料安全管理維運之人員 公務機關為使專人具有辦理安全維護事項之能力，應辦理或使專人接受專業之教育訓練
第三十五條	本法第十九條第一項第二款所稱類似契約之關係，指下列情形之一者： 一、非公務機關與當事人間於契約成立前，為訂定契約或進行交易為目的，所為接觸，磋商所形成之信賴關係 二、契約姻無效、撤銷、解除、終止或履行而消滅時，非公務機關與當事人為行使權利，履行義務或確保個人資料完整之目的所形成之聯繫關係
第四十五條	依本法第二十八條或第二十九條規定請求賠償者，以該違法行為在本法修正施行後者為限

項次	內容概述
第四十八條	依本法第五十四條所定告知之方式，得以書面、電話、傳真、電子郵件或其他通信方式為之。但告知所耗費之成本與當事人主張之個人資料隱私權益不相當者，告知得以網際網路、刊載新聞紙、處所適當位置揭示或其他公告方式為之，且留存相關紀錄，以供查驗

3.5.4. 台灣個人資料保護與管理制度簡介

臺灣個人資料保護與管理制度規範 (Taiwan Personal Information Protection and Administration System, TPIPAS) (以下稱「本制度規範」) 係由經濟部商業司所推動，是使事業以「PDCA 方法論」，建立一套將個人資料保護與事業營運連結之系統化管理制度。

本制度規範旨在提升事業對於個人資料之保護與管理能力，降低營運風險，並創造可信賴之個人資料保護與隱私環境。本制度規範係對於事業之個人資料管理制度進行內部控管、外部評量及用以核發事業「資料隱私保護標章」(Data Privacy Protection Mark, DP Mark)之依據。

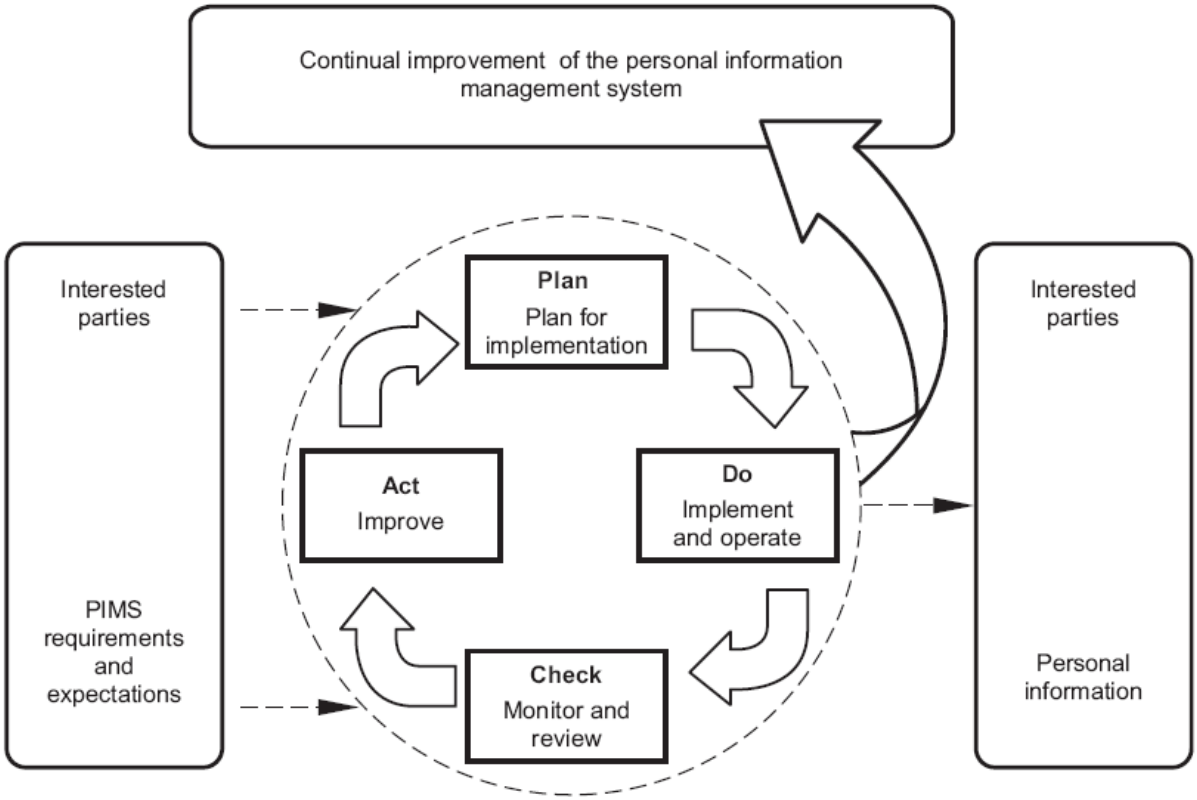
本制度規範之架構以「PDCA 方法論」為基礎。說明如下：

- 計畫：建立個人資料保護管理政策、目標及相關程序。
- 執行：個人資料管理制度之實施。
- 檢查：依據個人資料保護管理之政策、目標及要求，評估與監督流程及其產出，並將結果回報給最高管理階層加以審查。
- 行動：採取措施以持續改善個人資料管理制度之績效。

其架構參考日本之日本工業標準委員會(Japanese Industrial Standards Committee，以下簡稱 JISC)負責制定之 JISQ 15001「個人情報保護管理程序－要求事項」(Requirements for Compliance Program on Personal Information Protection)。係參照 ISO/IEC 270001 資訊安全管理系統之「Plan(規劃)、Do(執行)、Check(檢查)、Act(改進)」核心概念，將個人資料保護規範列入團體標準，作為國內適用於電子商務業者，提升個人資料

保護措施之規範。

其架構與英國之個人資料保護標準(BS 10012:2009 Data protection – Specification for a personal information management system)，PDCA 循環相類似，詳見圖 51 所示，如何規範個人資料之蒐集、處理及利用，以避免侵害人格權，並促進個人資料之合理利用。



資料來源：BS 10012

圖51 個人資料管理之 PDCA 循環

3.5.5. 特定隱私保護措施(Privacy-Specific Safeguards)

美國 NIST SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information，建議之特定隱私保護措施，主要用於協助組織蒐集、處理及利用個人資料，針對個人資料的機密性提供保護的機制，而這些機制通常不會被運用於其他的資料類別，但卻是非常重要的，

提供我們如何建立個資保護策略之重要思維，茲摘述如后：

3.5.5.1. 個人資料之蒐集、利用及保存最小化原則

個人資料已有法令規範，違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。雖然有其但書：

- 公務機關其損害因天災、事變或其他不可抗力所致者，不在此限。
- 非公務機關能證明其無故意或過失者，不在此限。

但是舉證責任倒置，公務機關及非公務機關一旦被提起訴訟，要負舉證責任，惟舉證之所在，通常也代表可能敗訴之所在。故有關個人資料之蒐集、處理及利用應以執行業務所需之最小限為原則，過多與不當之個人資料蒐集、處理及利用，都將為組織帶來不必要之責任，宜審慎考量。個人資料蒐集氾濫之案例，常見於電子商務網站，經常於會員登錄時要求輸入身分證字號，原本僅是資訊人員欲將蒐集之個人資料納入資料庫管理，擬利用身分證字號的唯一性，做為資料庫檢索之主鍵值(Primary key)，一時的便宜行事，卻因此而背負不必要之責任，因為身分證字號屬於「政府資料中之辨識者」，具有直接辨識特定當事人之特徵，一旦揭露與可能造成侵害，就需擔負損害賠償責任。

3.5.5.2. 去識別類資訊(De-Identifying Information)

個資法第九條『基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限』免為告知資料來源，就是去識別類資訊（De-Identifying Information）的最佳例證；換言之，將個人資料中的「識別類」資料加以加密、去除或是遮蔽（obscured），使其無從識別特定當事人，就變成「非個人資料」，或許還存在著組織營運的敏感資訊，但已非個資保護之範疇，屬於資訊安全管理應該考量之議題，但已不在本文討論之範疇內。

去識別化資訊，可以利用編碼、演算法或代名技術，將識別資訊回復

(Re-identified)，以達到識別之目的，但是以上技術所應用之參數，不可採用來自於當事人的其他相關資料，並且此一將識別資訊回復之方法，只可以讓獲得授權的人員所知悉，不得揭露予其他非經授權之人知悉。此類常見的遮蔽技術係利用單向加密演算法，例如：HASH 演算法。

符合以下之條件，得以將利用去識別化資訊保護之個人資料衝擊等級降低：

- 識別回復機制(Re-identification)所採用之編碼、演算法或代名系統，必須是一個獨立的系統，受到妥善之保護，以防止未經授權的人存取「識別回復資訊」。
- 此一資料單元不可經由公開的紀錄或是其他合理可用的外部資訊，用來回復識別之資訊。

最常見的例子就是基於統計之目的，我們可以將客戶的交易紀錄，去除姓名、身分證字號、聯絡電話及電子郵件等，進行統計分析或是趨勢研判等；或是特殊病歷研究，可以將病人的「識別類」資訊移除，但是保留病歷號碼，並將之用預先編製的代名表替代，必須將代名表與病歷結合，才能夠還原識別資訊，當兩份文件分置時，都不具有機密性，無法識別特定當事人，亦無行為隱私資料，就不會發生揭露後侵害當事人權益之情事。

3.5.5.3. 匿名資訊(Anonymizing Information)

匿名資訊與前述之去識別類資訊最大之差異在於：採用匿名資訊者毋須再回復識別資訊，通常供統計分析領域之用，常用的作法例如：

- 資料一般化：使資料較具一般性，反應群組特質
- 資料的抑制：刪除部分的資料欄位或紀錄
- 引進資料雜訊：加入少量變數至所選擇的資料中
- 對調資料：將不同群組相同欄位的資料對換

- 用平均資料取代：將特定欄位的資料以平均值取代

3.5.6. 個人資料保護策略擬定

公務機關及非公務機關如違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。另第二十八條規定公務機關可以證明損害係因天災、事變或其他不可抗力所致者，不在此限。第二十九條非公務機關能證明其無故意或過失者，不在此限。

自個資法修訂以來，實務當中有相當多之討論在於如何證明其為無過失，惟過失之定義，民法並無明文規定，民法第二百二十條第一項所明定債務人就其故意或過失行為，應負責任。

學者通說認為債務人欠缺注意之行為，即為過失：

債務人就其過失行為所應負之責任，謂之過失責任。民法對於民事責任以填補被害人之損害為目的，除法律別有規定外，不以故意與過失，作為區別責任之標準。如民法第一百八十四條第一項前段規定「因故意或過失，不法侵害他人權利者，負損害賠償責任」。在特種情形下，雖無過失亦應負責。

至於債務人注意之欠缺，因其程度之差異，有三種過失種類：

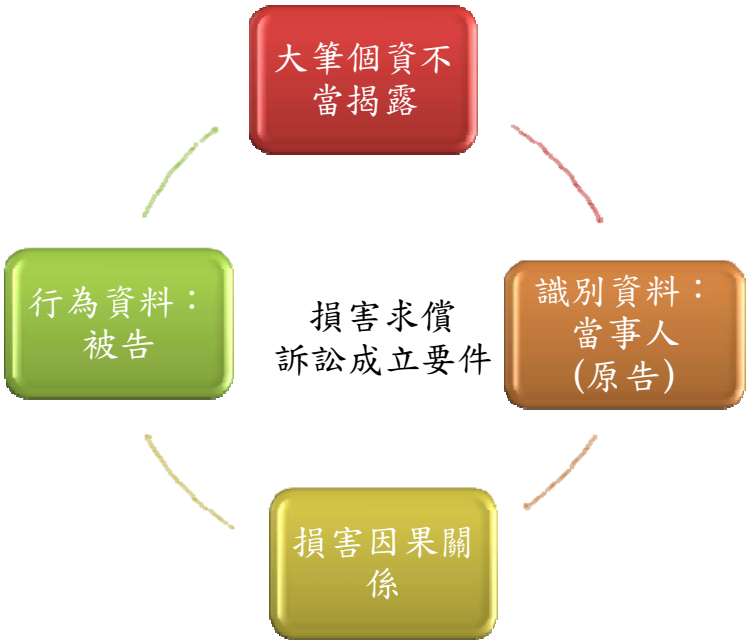
- 抽象過失：即應盡善良管理人之注意，亦即依交易上一般觀念認為有相當知識經驗與誠意之人之注意，而欠缺者。
- 具體過失: 即應與處理自己事務為同一注意，而欠缺者。
- 重大過失：即顯然欠缺普通人之注意者。

其中以抽象之過失，注意程度最高。故債務人之責任最重；具體之過失，注意程度較低，債務人之責任亦較輕。重大過失，注意程度較低，故債務人之責任最輕。

個資法第四章損害賠償及團體訴訟，除依本法規定外，公務機關適用

國家賠償法之規定，非公務機關適用民法之規定，亦即個資法之損害賠償為告訴乃論，一旦原告與被告之損害因果關係被推定成立，則被告需負責舉證，故有關個資保護之策略應採避免訴訟成立方為上策。因為一旦提起訴訟，對於公務機關與非公務機關而言，信譽立即受損，絕非遲來的正義可以彌補。

有關個資損害求償訴訟成立要件，首當有個資不當揭露之事實，尤其是有大筆資料之揭露，如超過 20 筆以上，即可達到團體訴訟之門檻，且於揭露之個人資料中，可以直接或間接識別特定當事人，則會有原告產生，若所揭露之個資當中存在有當事人之行為資料，足以證明當事人之損害與被告之間的因果關係，則損害求償訴訟便成立，此時被告便需負責舉證，否則便要負擔賠償責任，詳見圖 52 所示。個資保護策略便要有步驟的將損害因果關係加以阻斷，表面上看來是為防止訴訟之成立，實質上是真正做到個人資料之保護，促進個人資料之合理利用與保證人格權。



資料來源：本計畫自行整理

圖52 損害賠償訴訟成立要件

3.5.7. 個資保護安全控制措施

以下所列舉之安全控制措施係參考 NIST SP 800-122，引用 NIST SP 800-53，或行政院研考會所編撰之「安全控制措施參考指引」之建議，通訊傳播事業應根據以下說明，清查未實施的控制措施，並加以補強，對於已實作的控制措施，也要設法度量控制措施的有效性。

表32 個資保護安全控制措施

安全控制代碼	安全控制名稱	安全控制說明
AC-3	存取控制之執行	本中心可透過對存取控制政策的建構及存取控制之執行(例如使用存取控制表)，以達到控制個資存取的目的。控制存取之執行還包括對儲存資料的加密，以防止因遺失可攜式行動裝置而導致政府資料外洩的嚴重後果
AC-5	職責分工	本中心在設計存取個資的控制時，亦可採用職責分工的概念，將工作流程於資訊系統中適當切割，以避免違反獨立性原則的情況發生
AC-6	最低限度存取	本中心應要求其使用者在執行某項(些)業務時，僅使用與業務相關的最低限度存取及功能(例如讀、寫、執行)，同時並確認使用者僅能接觸最低數量的個資
AC-17	遠端存取	本中心可採用禁止或限制遠端存取的方式，控制對個資的接觸。對於核准之遠端存取，亦要確認個資在傳輸過程中予以妥善加密
AC-21	使用者資訊共享	本中心於提供合約規範下的資訊共享時，應使用自動控制機制比對(確認)存取授權符合存取控制
AC-19	可攜式行動裝置之存取控制	本中心對於禁止或限制個資的存取，可透過對可攜式行動裝置的使用控制來達成。由於其便於攜帶的特質，較桌上型電腦更容易產生遺失資料的風險。部分組織採取有限度地使用可攜式行動裝置。當進行遠端存取重要個資時，應確認高風險之個資不會離開本中心實體保護範圍。即使個資之遠端存取經過授權核准，本中心也會確認所使用之行動裝置受到適當的保護以與定期接受掃描
AU-2	事件監控	本中心可透過事件監控及早發現因未經授權而存取個資的行為所造成的個資外洩情形

安全控制代碼	安全控制名稱	安全控制說明
AU-6	定期稽核與報告	本中心可透過定期資訊系統稽核、稽核資料分析和報告適當層級主管，以及早發現與處理違反個資安全之異常行為
IA-2	使用者身分識別與證明	使用者於存取個資時應透過適當的識別與證明使用者身分。識別方式的強度取決於個資的重要性，例如美國聯邦政府要求個資遠端存取應採用二元識別方式(two-factor authentication)，並需於帳號於一段時間未使用後重新登入
MP-2	媒體存取	本中心可限制個資透過媒體存取，媒體亦包括具有資料儲存能力之可攜式行動裝置
MP-3	存放個資媒體等級標示	本中心應明確標示存有個資的電子或非電子媒體，並規劃媒體應如何處理與配置
MP-4	妥善存放個資儲存媒體	本中心應確認妥善存放儲有個資的電子及非電子媒體。這些媒體經確認不再使用後，應使用適當技術、方式及流程予以適當銷毀或消磁
MP-5	妥善運輸個資儲存媒體	本中心應確認存有個資的電子及非電子媒體，於本中心之外運輸時能得到妥善的保護，譬如將存有個資之資料進行加密或將媒體存放於上鎖的運送箱等方式
MP-6	媒體淨化	本中心對存有個資之電子及非電子媒體於報廢或回收加工時應確認妥善處理。例如對電子媒體要確認其已被徹底消磁
SC-9	傳輸保密	為確保個資保密及防止個資外洩，本中心於個資傳輸前，應確認其已經過妥善加密
SC-28	硬碟及備份資料保護	本中心對於儲存於硬碟及備份媒體中的個資應以適當方式予以加密，以達成個資保密及防止外洩的目標
SI-4	資訊系統與網路監控	本中心應適當監控其資訊系統及內部網絡，以即時偵測個資於內部網路之異常傳輸

資料來源：NIST SP800-122

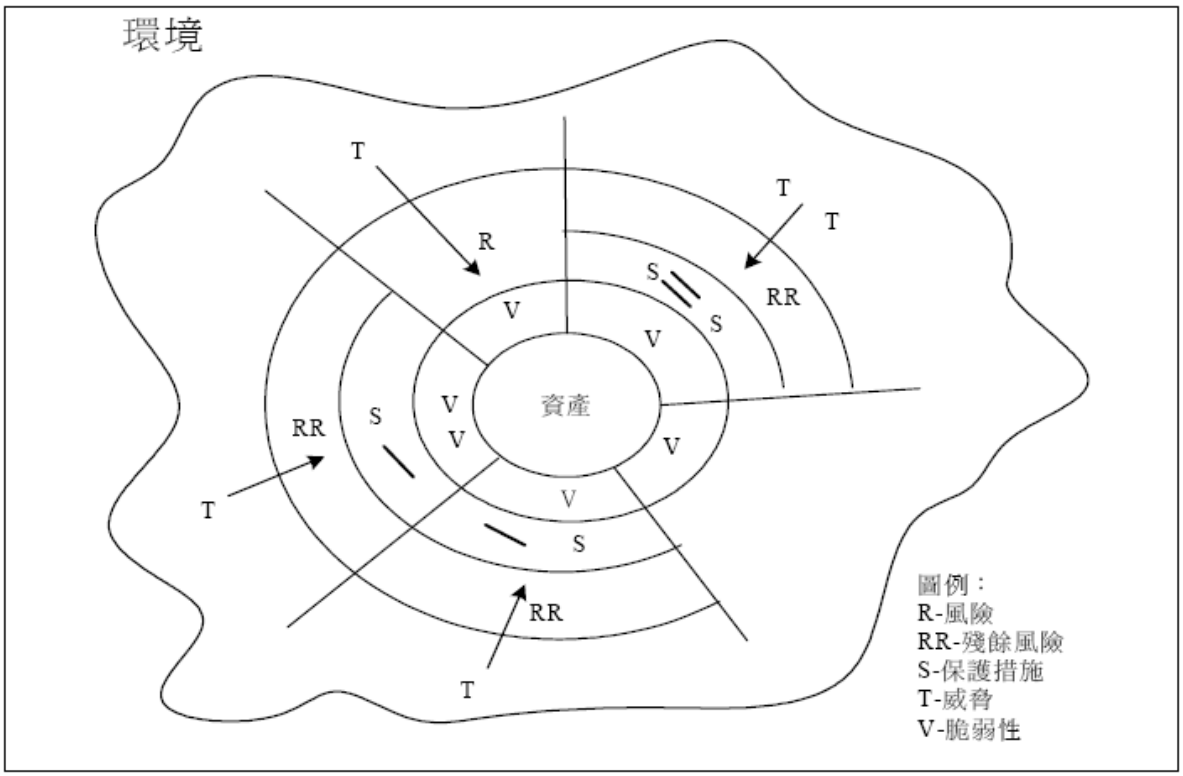
4. 研究分析

4.1.風險概念與模型

「風險」一詞有很多種層面的定義，反映出不同的風險意義與不同的人、事、物。其中一種最足以有效定義風險係 ISO 所提供：「可能對一個或群組資產可能之弱點產生威脅，以致產生損失或傷害資產。風險之影響或相關損害係指可能對企業產生之損失/破壞價值及估計威脅發生機率」。

「風險評鑑」是針對某一資產遭受到威脅時，在考慮系統脆弱性下，假設發生資產失效後，對企業營運產生風險水準之評估。一般「資訊安全風險評鑑」是針對資產之機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)等 3 項指標進行評鑑。

上述中之安全元件關係，詳見圖 53 所示。圖中的資產可以是單一資產或一群資產的集合，資產本身具有若干可被利用之特性，稱之為脆弱性(v)，而外在環境中存有若干之威脅(T)，一旦有威脅可以利用脆弱性，便會對資產造成衝擊，即構成風險(R)，而威脅經常隨時間不斷改變，且僅有一部分被知曉而成為已知。

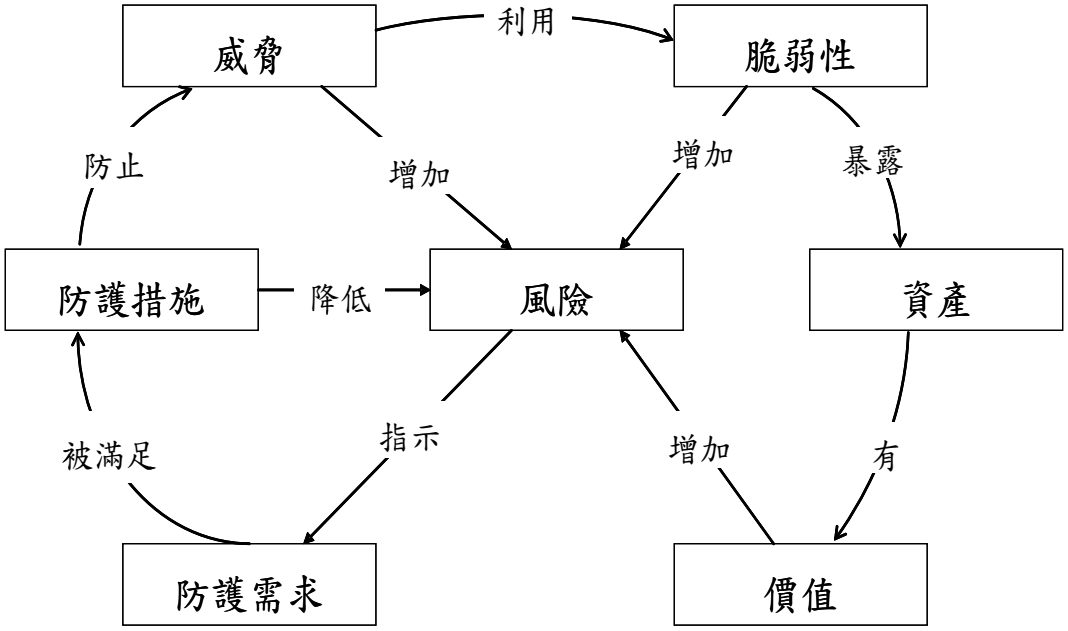


資料來源：CNS 14929-1 資訊技術安全概念與模型

圖53 安全元件關係圖

相反的，若是有脆弱性存在，但是卻沒有威脅可以利用該脆弱性，亦不會對資產造成衝擊。依據不同之威脅或脆弱性之組合，我們可以採取不同程度之控制措施(或稱之為保護措施 S)，消弭脆弱性或是拒止威脅，一旦控制措施有效性可以確保，則風險程度便會降低，剩餘之風險稱之為：殘餘風險(RR)。

以下模型係闡述以風險為核心之觀點，風險管理管理各要素之關聯，詳見圖 54 所示，風險之高低取決於資產的價值，以及資產脆弱性受到威脅的利用的程度，造成對資產價值的衝擊。組織應依據風險之高低決定防護需求，惟有防護措施被滿足，才可以有效將風險降低。其為一動態模式，隨著外界威脅的產生，系統須適時增加防護措施。



資料來源：CNS 14929-1 資訊技術安全概念與模型

圖54 風險管理關係圖

4.2.風險分析策略選項

在開始任何風險分析工作之前，組織宜有一適當之策略供此項分析作業，風險分析策略應確保所選擇之作法適合於該環境，且盡全力將安全聚焦在真正需要之處。以下各選項描述三種不同的風險分析作法。每一選項間之基本差別在於風險分析的深度。由於對通資系統做詳細的風險分析(Detailed Risk Analysis)成本往往過高，而對嚴重風險只給予極少的重視亦不具效益，故需要諸選項之間考量風險與成本的平衡。常用的三種風險分析策略選項，摘述如后：

4.2.1. 基準作法(Baseline Approach)

4.2.1.1. 作法簡介

不需對組織內風險不高的資產逐一清查風險，直接引用國內外標準或指引，選擇所需的基準安全(Baseline)。可藉由選擇防護措施而將基準安全

應用到所有資訊系統。

4.2.1.2. 選擇基準作法的特色

- 只需最少量的資源做風險評鑑與管理每一防護措施實作，因而減少時間與花費在選擇防護措施的工作量。
- 若某組織的多數系統係在一共同的環境下運作且安全需求相近，由於相同或類似的基準防護措施無需太大的工作量便可被許多系統採用，基準防護措施為具成本效益的解決方案。

4.2.1.3. 選擇基準作法應注意事項

- 如果基準等級設得太高，在某些資訊系統上的安全等級可能會太超過，因而造成資源的浪費。
- 如果基準設得太低，在某些資訊系統上可能會有安全程度不足的情況，造成其高度曝露於風險中。
- 在管理與安全攸關的變更時可能會有困難，例如：若將某系統升級，可能難以評鑑原始基準防護措施是否仍充足。

4.2.1.4. 建議

若某組織的所有資訊系統只有低等級的安全需求，則此作法可能為最具成本效益之策略。多數組織將需要符合某些最低的標準以保護敏感資料，並且遵循法律與條例(例如：個人資料保護法)。在此個案中，必須選擇出反映大多數資訊系統所要求之保護程度的基準。無論如何，若組織內各系統的營運敏感性、規模及複雜度均不同，欲以一套共同標準應用到所有系統，既不合邏輯，又不具成本效益。

4.2.2. 詳細風險評鑑(Detailed Risk Analysis)

4.2.2.1. 作法簡介

詳細風險評鑑包含深入的識別資產與估價、威脅對資產的評鑑及脆弱性的評鑑，據以分析風險所造成的衝擊與其可能性。從這些活動所得結果隨後將使用在評鑑風險，然後去識別正確的安全防護措施。選擇詳細風險評鑑作法的特色。

- 所有系統均能識別出對該系統適當的防護措施。
- 詳細風險評鑑所得結果可被用在安全變更的管理。

4.2.2.2. 選擇詳細風險評鑑作法應注意事項

- 由於所有資訊系統會以相同的方式詳細考量，需要大量時間去完成分析，關鍵系統之安全需要被提出時可能已太遲。
- 此作法將產生大量的分析資料，若對所有資訊系統要求以相同的方式詳細考量，將造成資料維護的負擔，也容易發生相同風險卻有不一致的評價結果。

4.2.2.3. 建議

此作法將需要大量的時間完成分析，不適合對所有資訊系統執行詳細風險評鑑，可以局部用於重要性較高的資訊系統。

4.2.3. 組合式作法(Combined Approach)

4.2.3.1. 作法簡介

首先對所有資訊系統作初步的高階風險評鑑(High Level Risk Analysis)，每一個案集中在資訊系統的營運價值，以及它被曝露在哪些嚴重風險處。對於被識別成對組織營運為重要及/或被曝露在高風險處的資訊系統，宜優先進行詳細風險評鑑。對其他所有資訊系統，則選擇基準作法。這個組合式作法，將花費在識別防護措施的時間與工作量降至最低之間的良好平衡，而仍確保各高風險系統都受到適當的保護。

4.2.3.2. 選擇組合式作法的特色

- 在投入大量時間與資源之前，先進行一初期迅速且簡單的風險評鑑作法(高階風險評鑑)，將可得到一種廣被接受的風險評鑑計畫。
- 能迅速建立一個組織安全計畫的策略構圖，此策略構圖將成為良好的輔助規劃。
- 資源與金錢可被最有效的運用，最需要受到保護的系統將會被優先提出，且後續各項作為行動將會更為成功。

4.2.3.3. 選擇組合式作法應注意事項

- 如果初期的風險評鑑是在高階，潛在的結果較不精確，某些較重要的系統可能被識別成不需要執行詳細風險評鑑。無論如何，這些系統仍將受到基準安全的保護。而且，這些系統可在必要時被重新訪查，以檢查是否需要比基準作法更多的防護措施。

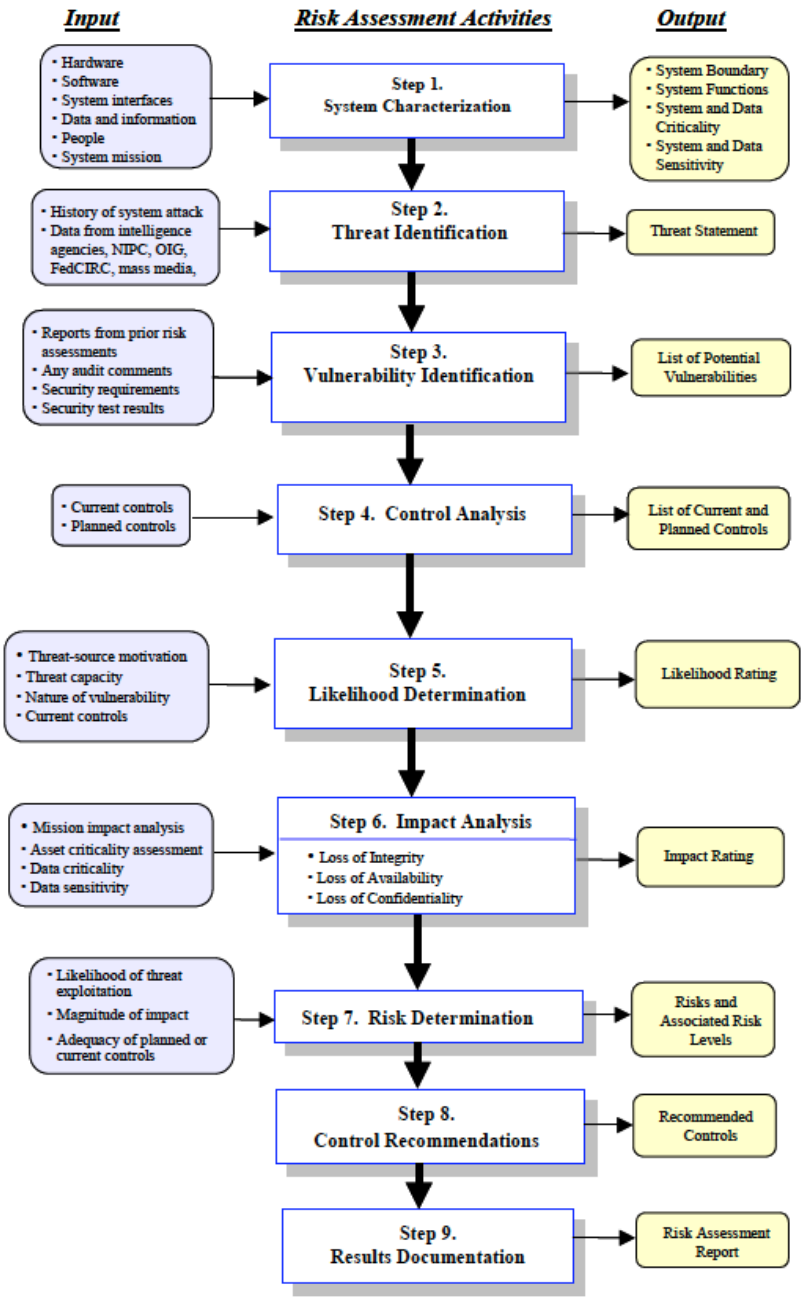
4.2.3.4. 建議

先使用高階風險評鑑，再組合上基準作法與詳細風險評鑑是平衡風險與資源兩者最適合的作法，此為大多數組織最有效的作業方法。且CNS14929 亦建議採用此作法。

4.3.美國聯邦風險管理架構

4.3.1. NIST SP 800-30 Risk Management Guide

美國國家標準學會(National Institute of Standards and Technology, NIST)於 2002 年制定 NIST SP 800-30 Risk Management Guide for Information Technology Systems，強調風險管理應納入於系統發展生命週期之中，首要工作便是進行風險評鑑，其流程詳見圖 55 所示。此階段之風險評鑑方法，主要還是依據前述之風險模型，進行詳細之風險評鑑作業，包含識別威脅、弱點並進行衝擊分析。



資料來源： NIST SP 800-30

圖55 Risk Assessment Methodology Flowchart

4.3.2. FIPS 199 聯邦資訊系統分類分級標準

於 911 恐怖攻擊事件之後，美國政府制定了「聯邦政府資訊安全管理

法案(Federal Information Security Management Act of 2002, FISMA)，積極發展更有效率之資訊安全管理架構與方法，改採基準法，首先推動的便是訂定聯邦資訊系統分類分級標準(Standards for Security Categorization of Federal Information and Information Systems)，結合衝擊分析的概念，區分為低、中、高三級，分別考量喪失機密性、完整性及可用性後，對於組織可能之衝擊程度，快速的訂出資訊系統之安全等級，詳見表 33 所示。

表33 FIPS 199 安全等級區分表

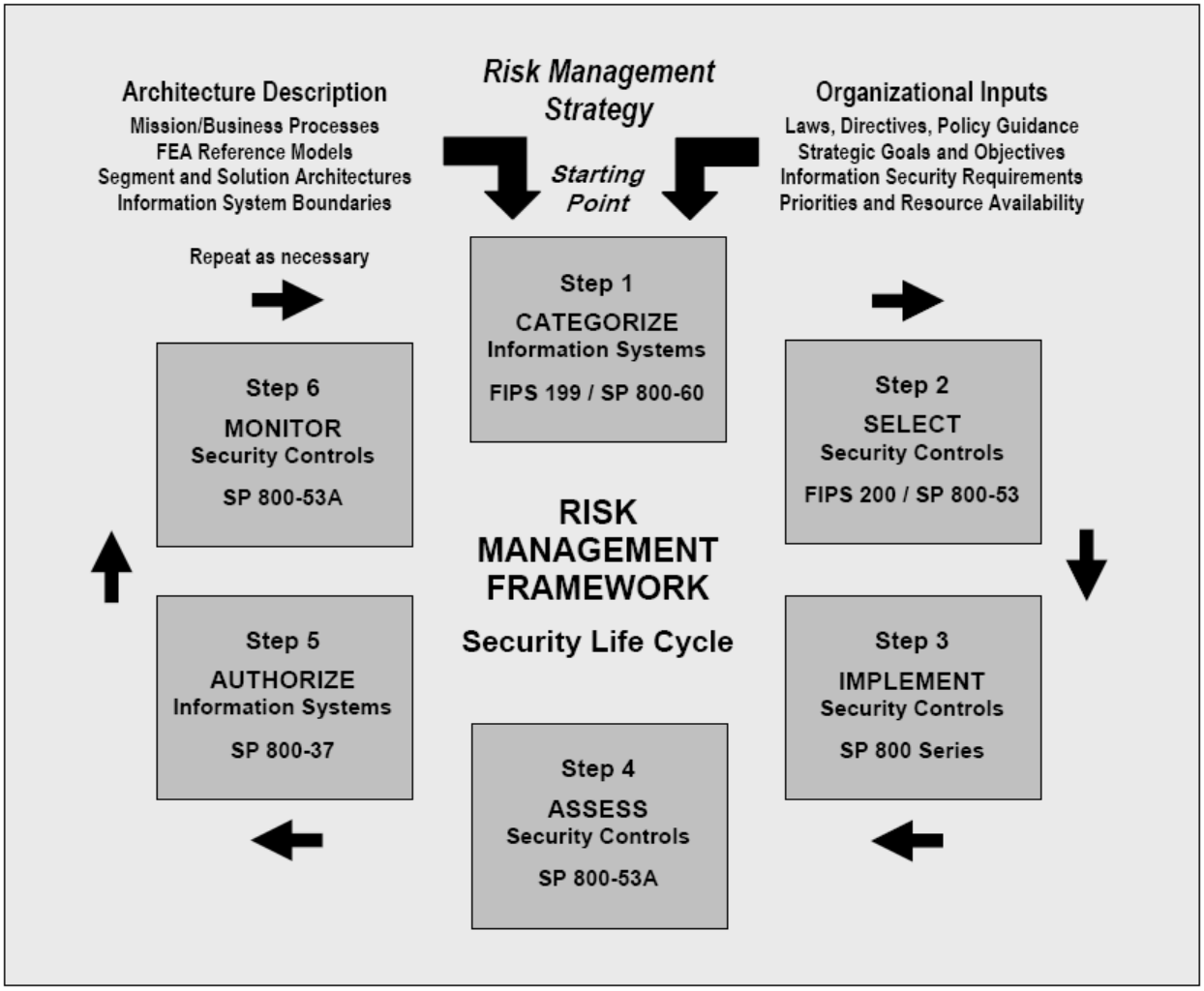
Security Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for pro-tecting personal privacy and proprietary informa-tion.	The unauthorized disclo-sure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclo-sure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclo-sure of information could be expected to have a **severe or catastrophic** adverse effect on organ-izational operations, or-ganizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and in-cludes ensuring informa-tion non-repudiation and authenticity.	The unauthorized modifi-cation or destruction of information could be ex-pected to have a **limited** adverse effect on organ-izational operations, or-ganizational assets, or individuals.	The unauthorized modifi-cation or destruction of information could be ex-pected to have a **serious** adverse effect on organ-izational operations, or-ganizational assets, or individuals.	The unauthorized modifi-cation or destruction of information could be ex-pected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reli-able access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organ-izational operations, or-ganizational assets, or individuals.

資料來源： NIST FIPS 199

4.3.3. NIST 風險管理框架

依據前述之安全等級分類分級之結果，FIPS 200 規定了不同安全等級

之資訊系統，應依據 NIST SP 800-53 所建議之控制措施，選擇適用之控制措施並加以實作，其風險管理框架，詳見圖 56 所示。



資料來源： NIST SP 800-53

圖56 Risk Management Reamework of NIST

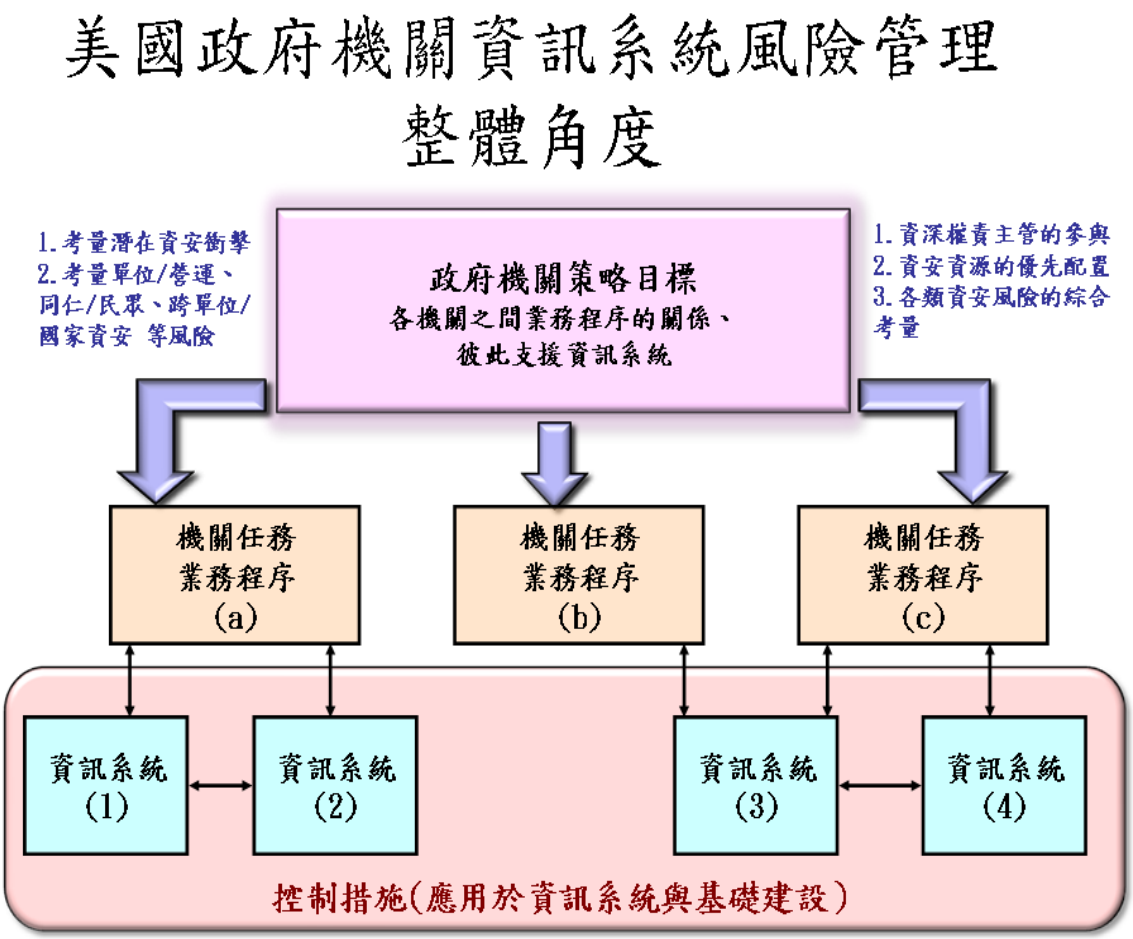
其著眼主要是因為詳細風險評鑑作業耗時費力，但是聯邦政府中不乏組資結構相近、業務性質雷同者，故採用資訊系統分類分級方法，將資訊系統區分為低、中、高三級之安全基準，各自套用不同等級之控制措施，是一種兼顧效率與效能之作法，範例詳見表 34 所示。

表34 NIST 安全防護基準表(範例)

CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2)	AC-6 (1) (2)
AC-7	Unsuccessful Login Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P2	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11	AC-11
AC-12	Session Termination (Withdrawn)	---	---	---	---
AC-13	Supervision and Review—Access Control (Withdrawn)	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P1	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking (Withdrawn)	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4) (5) (7) (8)	AC-17 (1) (2) (3) (4) (5) (7) (8)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (2) (4) (5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (1) (2) (3)	AC-19 (1) (2) (3)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	User-Based Collaboration and Information Sharing	P0	Not Selected	Not Selected	Not Selected
AC-22	Publicly Accessible Content	P2	AC-22	AC-22	AC-22

NIST SP800-39 的發展乃是 NIST 首先將「風險管理」與「風險評鑑」分成兩個步驟來討論，過去「NIST SP800-30(資訊科技系統風險管理參考

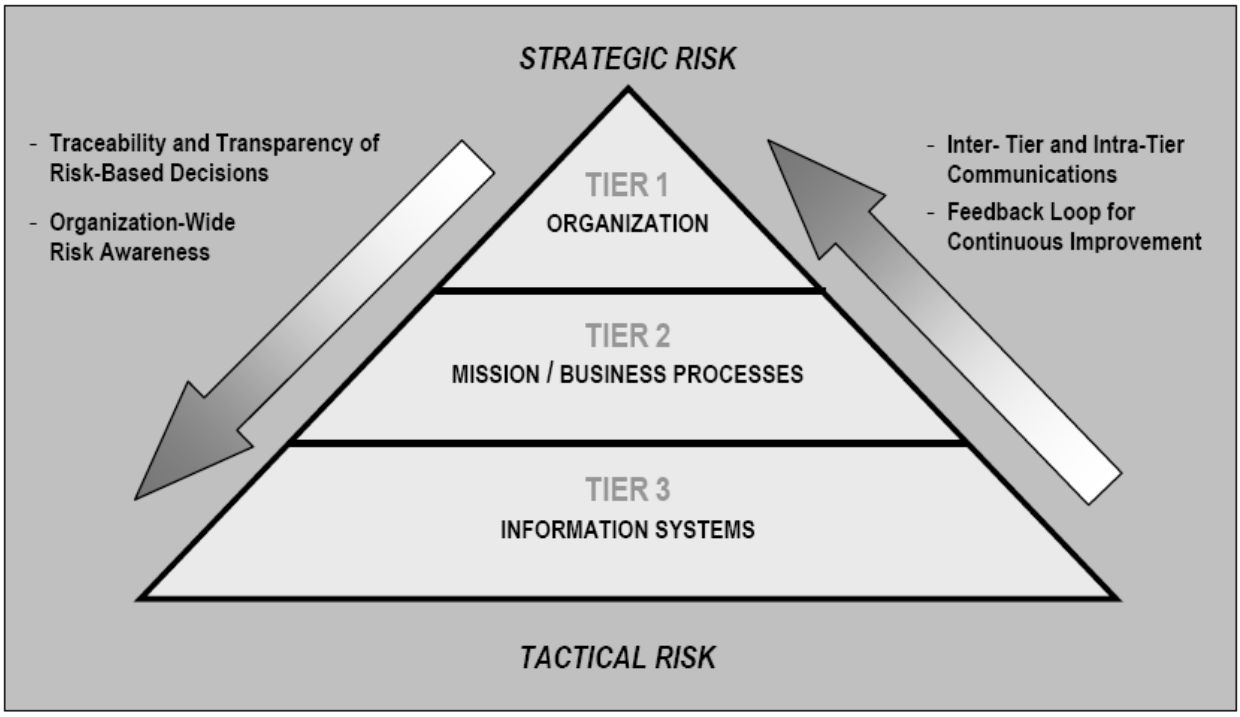
指引)」，隨著 NIST SP800-39 的發展已被修訂成侷限於「風險評鑑作業」，而「風險管理作業」則改以 NIST SP800-39 為主，同時 NIST SP800-39 也說明美國政府機關之資訊系統風險管理整體角度，詳見圖 57 所示。



資料來源：NIST SP800-39

圖57 美國政府機關資訊系統風險管理整體角度思考圖

至 2011 年 3 月，NIST 公布最新版之 SP 800-39 Managing Information Security Risk－Organization, Mission, and Information System View，參考了 ISO 31000、IEC/ISO 31010、ISO/IEC 27001 及 ISO/IEC 27005 等國際標準之內容，提出多階層之風險管理框架，詳見圖 58 所示。分別從組織、營運及資訊系統等層級，逐步評鑑組織所可能面臨之風險，架構上看似與 ISO 31000 不同，但是內容上已經納入對應之作法。



資料來源： NIST SP 800-39

圖58 Multi-Tiered Organization-Wide Risk Management

4.4.我國資訊安全管理制度發展歷程

91 年底，資安會報以推動資通安全工作目標，作為推展政府機關(構)各項資安服務作業之主要依據，針對單位層級、編制及投資金額等區分縱向之等級，並依各機關(構)之屬性(國防、行政、學術、事業)區分橫向之類別，運用於政府機關(構)各項資安服務作業，不同資安等級之機關(構)提供不同的資安服務。經學者專家研討與相關單位之檢討建議，首先應以政策目標為依據，所需保護的標的物是涉及國家安全與民眾權益有關之重要資料防護，並將易混淆之影響資安事件等級區分予以釐清，以管理手段考量主、客觀之形勢，明確律定資安等級之規範訂定。

4.4.1. 資安等級區分方式

於 94 年資安會報(94 年 9 月 28 日資安發字第 94100802 號函)頒訂「政府機關(構)資訊安全責任等級分級作業施行計畫」，以機關之重要性作為區分等級之標準，透過評估各單位的資訊能力、重要性、機敏性及保護標的，明確區分其資訊安全責任等級，計區分為 A 級：重要核心、B 級：核心、C 級：重要、D 級：一般等四級，其資安等級區分方式，詳見表 35 所示。

表35 政府機關資安等級區分方式

等級區分	區分方式
A 級 (重要核心)	中央一、二級單位(總統府、行政院、考試院、審計部等) 涉及國家安全之重要機敏系統(行政院跨部會平臺、公文交換、稅務電子閘門、自然人憑證管理、刑案資訊整合系統等)
B 級 (核心)	具有影響社會秩序、民眾隱私之敏感資料維運機關 部分之中央一、二級機關 各部會之署局單位 各縣市政府、警察局、地方稅捐單位
C 級 (重要)	部分中央一、二級機關(蒙藏委員會、消保會、體委會) 涉及地方社會秩序、人民財產安全之重要資訊維運單位 各部會之地方性作業單位(台中行政執行處、工業區服務中心) 地區性氣象站、管理處(竹子湖氣象站、中區糧食管理處) 各縣市議會、衛生局、文化局、消防局等
D 級 (一般)	地方鄉、鎮、區公所、代表會；事務所；衛生所；托兒所；體育館及鄉村里民代表會等等 地區性氣象站

4.4.2. 資安等級應執行之工作事項

依據上述之資訊安全責任等級，律訂應執行之資安工作事項，詳見表 36 所示：

表36 各類資安系統等級應執行之工作事項表

作業名稱 / 內容 / 等級	防禦機制強度	防護縱深	ISMS 推動作業	稽核方式	資安教育訓練(主官、主管、技術、一般)	專業證照
A 級	強度等級 4	NSOC 直接防護/自建 SOC、IDS、防火牆、防毒	96 年通過第三者認證	每年至少執行 2 次內稽	每年至少(4,6,18,4 小時)	96 年資安專業鑑定 2 張
B 級	強度等級 3	SOC(Optional)、IDS、防火牆、防毒	97 年通過第三者認證	每年至少執行 1 次內稽	每年至少(4,6,16,4 小時)	96 年資安專業鑑定 1 張
C 級	強度等級 2	IDS、防火牆、防毒	各單位自行成立推動小組規劃作業	自我檢視	每年至少(2,6,12,4 小時)	資安專業訓練
D 級	強度等級 1	防火牆、防毒	推動 ISMS 觀念宣導	自我檢視	每年至少(1,4,8,2 小時)	資安專業訓練

上表之內容主要依據機關之安全等級，於縱深防禦機制，分別建立安全監控中心、防火牆、入侵偵測及防毒系統等。於 ISMS 推動作業，要求 A、B 級機關應通過第三者認證，C 級機關自行成立推動小組規劃作業，D 級單位則應加強安全觀念宣導。

4.4.3. 防禦機制強度

上述之要求事項，期達到防禦機制強度(Strength Mechanism Level，簡稱 SML)所要求之防護能力，詳見表 37 所示。

表37 資訊安全機制強度等級

等級	內　　容
強度等級 1	經由良好的資訊安全作業可達成的基本強度，用以防衛不複雜的威脅，應能保護低價的資訊資產
強度等級 2	中等強度，可以抵抗諸如個人發動之攻擊活動的複雜威脅，能夠保護中等價值的資訊資產
強度等級 3	高強度，用以防禦來自駭客組織的威脅，能夠保護高價值的資訊資產
強度等級 4	極高強度，用以防禦來自國家級的威脅，能夠保護極高價值的資訊資產

4.4.4. ISMS 推動作業之範圍

資安會報要求 A、B 級機關分別於 96、97 年通過 ISMS 第三方驗證，復於 98 年修訂規定，延期至 100 年完成，有關 ISMS 推動作業之範圍，詳見表 38 所示。

表38 ISMS 推動作業之範圍

類別	範圍說明
以部門別定義	將部門資訊及業務定為ISMS建置範圍(核心業務必須已涵蓋於所選定之部門內)，例如：信用卡中心的核心業務為核卡、發卡及相關後續服務，其達成核心業務服務所依賴之關鍵資產可能包括：核卡發卡電腦系統、客戶資料庫、參與人員等，其範圍包含業務部、核卡部、發卡部、資訊部
以系統別定義	將與此系統業務有關之人員或部門全部納入，其範圍應涵蓋要保護之核心業務服務及所依賴之關鍵資產
以產品/業務別定義	例如：以現金卡為 ISMS 範圍，則相關牽涉此業務之活動、人員或部門便需納入 ISMS 範圍，此方式適合資源有限或

類別	範圍說明
	分階段導入 ISMS 之組織
以實體區域定義	以某機關或大樓(某樓層)為 ISMS 建置範圍，此種定義方式應將此區域內所有系統業務有關之人員或部門全部納入，此方式適用於業務明確，且可於定義之區域內完全獨立作業者

4.4.5. 資訊安全責任等級分級作業流程修訂

資安會報為明確規範政府機關資訊安全責任等級分級作業流程，特於98 年 6 月 1 日修訂「政府機關(構)資訊安全責任等級分級作業施行計畫」，透過資訊安全管理，以防範潛在資安威脅，進而提升國家資通安全防護水準（資安會報 94 年 9 月 28 日資安發字第 94100802 號函作廢）。

要求各機關之資通安全作業權責之相關事項，請參考各政府機關(構)落實資安事件危機處理具體執行方案，要求機關首長應負該管單位全盤資安成敗之責，以期落實執行成效。並要求除遵行政院及所屬各機關資訊安全管理規範外，各機關(構)依其資安等級應執行之工作事項，增訂應檢測機關網站安全弱點，詳見表 39 所示。

表39 各機關(構)資安等級應執行工作事項表

區分	防護縱深	ISMS推動作業	稽核方式	資安教育訓練 一般主管、資訊人員、資安人員、一般使用者	專業證照	檢測機關網站安全弱點
A級	NSOC直接防護/SOC自建或委外、IDS、防火牆、防毒、郵件過濾裝置	通過第三者驗證	每年至少2次內稽	每年至少3、6、18、3小時 資訊人員、資安人員需通過資安職能鑑定	維持至少2張資安專業證照	每年2次
B級	SOC(選項)IDS、防火牆、防毒、郵件過濾裝置	通過第三者驗證	每年至少1次內稽	每年至少3、6、16、3小時 資訊人員、資安人員需通過資安職能鑑定	維持至少1張資安專業證照	每年1次
C級	防火牆、防毒、郵件過濾裝置	自行成立推動小組規劃作業	自我檢視	每年至少2、6、12、3小時	資安專業訓練	每年1次
D級	防火牆、防毒、郵件過濾裝置	推動ISMS觀念宣導	自我檢視	每年至少1、4、8、2小時	資安專業訓練	每年1次

資料來源：政府機關(構)資訊安全責任等級分級作業施行計畫

4.4.6. 資訊系統分類分級鑑別機制

資安會報於上述資訊安全等級分級計畫施行多年之後進行檢討，逐漸發現以機關為等級劃分之依據，有其不合理之處，因為 A 級機關也會有不重要之資訊系統，例如行政、總務等，D 級機關也會需要存取重要之資訊系統，例如：戶政、役政、地籍資訊系統等。遂開始進行以資訊系統為基準的分類分級方法研究。

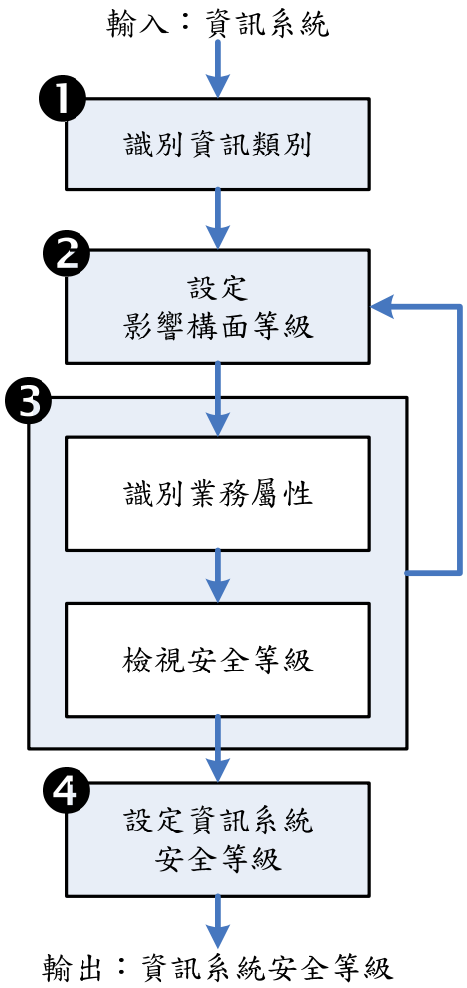
於 99 年 7 月 5 日資安發字第 0990100394 號函辦理。正式頒定「資訊系統分類分級與鑑別機制」，要求 A 級機關應於 99 年、B 級機關與學校應於 100 年前完成資訊與資訊系統鑑別作業，資安會報將定期調查執行情形。

本機制旨在鑑別資訊系統安全等級，協助機關掌握重點保護標的，並促使機關進行風險評鑑、有效運用資源，採行適當安全控制措施，以確保資訊系統之安全防護水準。適用於各級政府機關、公營事業機構、公立研究機構、學校等之資訊系統，惟資訊內容屬「國家機密保護法」所稱國家機密之資訊系統，除參考本機制外，亦應依據「國家機密保護法」相關規定辦理。

4.4.6.1. 鑑別機制處理程序

本機制處理程序詳見圖 59 所示，包含❶識別資訊類別、❷設定影響構面等級、❸識別業務屬性並檢視安全等級、❹設定資訊系統安全等級等四個處理步驟。各資訊系統均須依循處理程序填寫「安全防護要求等級評估表」，並由資訊單位彙整「資訊系統清冊」。

另外，本機制依處理程序須由業務承辦人、承辦單位主管、資安人員及資訊主管等相關人員會辦，最後並由資訊安全長核定資訊系統安全等級，以確保所鑑別安全等級符合機關安全需求。



❶：資訊類別即為施政分類，定義詳見行政院秘書處彙編「行政院施政分類架構」，資訊系統依其處理資料之性質，可包含多項資訊類別

❷：由業務承辦人依資料保護、業務運作、法律規章遵循、人員傷亡、組織信譽及其他等六大構面，分別評估對各資訊類別之影響衝擊，並據以設定影響構面等級

❸：由承辦單位主管依據資訊系統之業務屬性，檢視業務承辦人所設定安全等級之合理性

❹：資訊系統安全等級經承辦單位主管、資訊主管確認後，最後由資訊安全長核定

資料來源：資訊系統分類分級與鑑別機制參考手冊

圖59 資訊系統分類分級與鑑別機制處理程序

4.4.6.2. 鑑別機制處理程序步驟

上述鑑別機制處理程序步驟說明，詳見表 40 所示。

表40 鑑別機制處理程序步驟說明表

處理程序	工作項目	相關人員
輸入： 資訊系統	•輸入需要鑑別安全等級之資訊系統	承辦單位主管 (或其授權人員)

處理程序	工作項目	相關人員
步驟❶：識別資訊類別	•「安全等級評估表」之【資訊類別】欄位係參照行政院秘書處彙編「行政院施政分類架構」之施政分類，資訊類別以取至施政分類編碼第二層為原則，惟機關可視需要自行調整至第三層或更多層 •依系統涉及之業務範圍，由業務承辦人負責識別系統資訊所屬之資訊類別，並於【資訊類別】欄位以下拉式選單依次選擇資訊類別第一層、第二層編碼	業務承辦人
步驟❷：設定影響構面等級	•針對所選擇之各項資訊類別，由業務承辦人評估當發生資訊安全事故時，對資訊保護受到損害、影響業務運作、影響法律規章遵循、人員傷亡、損害組織信譽及其他等六大影響構面的衝擊程度，並參照「七、安全等級設定原則」填寫影響構面安全等級，安全等級區分為普、中、高三級，分別以 1、2、3 表示；對於不適用之影響構面，安全等級以 NA 表示 •各項資訊類別之安全等級為該資訊類別在六大影響構面安全等級最高者。因此，取各別六個影響構面安全等級值最高者即為該列【資訊類別安全等級】欄位值 •資訊系統安全等級為各項資訊類別安全等級最高者。因此，取各【資訊類別安全等級】欄位值最高者即為【資訊類別安全等級】欄位值	業務承辦人
步驟❸： 1.識別業務屬性 2.檢視安全	•由承辦單位主管識別資訊系統之業務屬性，並與「步驟❷：設定影響構面等級」之結果相勾稽，以檢視所設定安全等級之合理性 •資訊系統依其服務之業務屬性分為行政性業務、關鍵性業務、支援性業務等三類，說明如下： ◇**行政性業務：**係指機關內部輔助單位之業	承辦單位主管(或其授權人員)

處理程序	工作項目	相關人員
等級	務，若輔助單位工作與機關職掌相同或兼具業務單位性質，機關得視情形調整其業務屬性 ◇**關鍵性業務**：機關在遭遇衝擊時，須確保持續運作之核心業務，以及與民眾生活機能相關之關鍵基礎建設(如：水、電力、通訊電信、農產運銷、金融服務等)，均屬關鍵性業務 ◇**支援性業務**：機關內部業務單位之業務但非列核心業務者，屬支援性業務 •資訊系統安全等級與業務屬性通常具有高度關聯性，因此可進行勾稽如下： ◇於步驟❸-1 識別業務屬性為「行政性業務」或「支援性業務」，惟於步驟❷設定部分資訊類別安全等級為「高」級(即等級 3) ◇於步驟❸-2 識別業務屬性為「關鍵性業務」，惟於步驟❷設定各資訊類別安全等級均為「普」級(即等級 1) 如有上述情形者，機關須就其合理性進行確認，如確認無誤，則應於備註欄位說明原因 •本步驟所進行各項異動均須記錄異動原因	
步驟❹：設定資訊系統安全等級	•由資訊單位綜整各項資訊系統「安全等級評估表」，並製作「資訊系統清冊」，經資訊主管、承辦單位主管確認後，最後由資訊安全長核定資訊系統安全等級	資訊安全長、承辦單位主管、資訊主管、資安人員
輸出：資訊系統安全等級	•本程序所鑑別之資訊系統安全等級，可作為後續選擇安全控制措施之依據 •資訊系統安全等級列「高」者，可考量進一步實施詳細風險評鑑，俾利進行風險管理	

上述步驟最後之輸出，係決定資訊系統之安全等級，可作為後續選擇安全控制措施之依據，資訊系統安全等級列為「高」者，可考量進一步實

施詳細風險評鑑，俾利進行風險管理。是一種兼顧效率與安全需求之作法，適用於具經濟規模之政府機關採用，亦可彌補基準法之不足。

4.4.6.3. 安全等級設定原則

安全等級分為普、中、高三級，由機關依「資料保護受到損害」、「影響業務運作」、「影響法律規章遵循」、「人員傷亡」、「損害組織信譽」及「其他」等六大影響構面，分別考量資訊系統於發生資訊安全事故時可能造成的衝擊，即衡量資訊系統發生資料外洩、資料遭竄改及系統故障等情事時可能造成的後果嚴重程度，並據以評估、設定安全等級。安全等級設定原則，詳見表 41 所示。

表41 安全等級設定原則表

安全等級 / 影響構面	普 (等級 1)	中 (等級 2)	高 (等級 3)
1.資料保護受到損害	•一般性資料 •資料若外洩或遭竄改，不致影響個人權益或僅導致個人權益輕微受損	•敏感性資料 •資料若外洩或遭竄改，將導致個人權益嚴重受損	•機密性資料 •資料若外洩或遭竄改，將危及國家安全、導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損
2.影響業務運作	•系統容許中斷時間較長 •系統故障對社會秩序、民生體系運作不致造成影響或僅有輕微影響 •系統故障僅影響機關非核心業務執行效能，或造成核心業務執行效能輕微降低	•系統容許中斷時間較短 •系統故障對社會秩序、民生體系運作將會造成嚴重影響 •系統故障將造成機關核心業務執行效能嚴重降低	•系統容許中斷時間非常短 •系統故障對社會秩序、民生體系運作將會造成非常嚴重影響，甚至危及國家安全 •系統故障將造成機關核心業務執行效能非常嚴重降低，甚至業務停頓

安全等級 影響構面	普 (等級 1)	中 (等級 2)	高 (等級 3)
3.影響法律規章遵循	系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關違反法律規章並伴隨輕微不良後果	系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關違反法律規章並伴隨輕微不良後果	系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關從根本上違反法律規章
4.人員傷亡	-	若系統發生資訊安全事故，無法完全排除造成人員傷亡的可能性	若系統發生資訊安全事故，可能造成人員死亡，或非常可能造成人員肢體傷害的危險
5.損害組織信譽	若系統發生資訊安全事故，將導致機關形象、信譽受到輕微損害	若系統發生資訊安全事故，將導致機關形象、信譽受到嚴重損害	若系統發生資訊安全事故，將導致機關形象、信譽受到非常嚴重損害
6.其他	由機關視本身業務特性考量可能遭遇衝擊之其他影響構面(如：財物損失)，並依需求和本質自行設定分級基準		

4.5.研究心得

- 綜上所述，NCC 原頒訂之「電信事業資通安全管理手冊」之內容，其規劃思維係延續資安會報之規定採用基準法，將目的事業之資通安全需求，依據「資料保護受到損害」與「影響業務運作」之影響構面，分別評估影響構面之影響等級為A級或B級。方法上已做了相當程度之簡化。
- 考量業管之目的事業中，不乏業務項目雷同，組織結構相近者，故採行分類分級之方法，是兼顧行政效率與資安防護的適切作法，但是參考美國或是我國行政院資通安全會報之最新作法，均是將資通安全等級區分為普、中、高三級，再考量 3.1 節之通訊傳播事業特性分析，本研究所涵蓋之目的事業其業務屬性差異頗大，如：第一類電信及第二類電信，對於通信秘密之保護有嚴格之法令限制，對於機密性之要求其高，或如：

有線廣播電視業者等，擁有大量之電信、傳播機線設備，對於可用性要求極高者，但是也有如：廣播節目供應事業，著重於節目及廣告之管理，對於資訊安全管理之要求極低者，故建議針對資產群組宜區分為普、中、高三級，最後彙整成企業安全等級，區分為 A、B、C 三級，以針對不同之安全等級，建議適用之安全防護基準，較為妥適。

- 在資訊安全管理分類上屬於基準作法，世界各國政府資安防護體系，自 911 恐怖攻擊事件後，逐漸採用此類方式，尤其以美國為代表。

- 資安會報雖然規定 A、B 等級機關，應建置 ISMS 且通過第三方驗證，其推動範圍雖規定可依據：部門別、系統別、業務別或實體環境加以區分，但卻未規定機關之核心業務應予納入，亦未規定是否應涵蓋整體機關，導致大部分之機關，因應外部力量之要求，主要來自於上級主管機關之要求，僅有極小部分之單位或是實體環境申請 ISMS 驗證，通過之後即宣稱已獲得 ISMS 驗證，以偏概全，對於整體資安防護能力之提升助益有限。

- 資訊系統分類分級鑑別機制，將所有政府機關之業務納入，並區分為「關鍵性業務」、「支援性業務」及「行政性業務」，藉此掌握資訊系統與業務之關係，可以迅速釐清 ISMS 的邊界與範圍。

- 行政院之資訊系統分類分級鑑別機制，依據「資料保護受到損害」、「影響業務運作」、「影響法律規章遵循」、「人員傷亡」、「損害組織信譽」及「其他」等六大構面，分別考量資訊系統於發生資訊安全事故時可能造成的衝擊，藉此評定資訊系統之等級。得以視為營運衝擊分析或高階風險評鑑的一部分，本研究所進行之問卷調查初步分析，通訊傳播事業對於資訊安全之重視，首重對於「損害組織信譽」之衝擊，其餘構面則與行政院資通會報之方法相近，但是進一步進行因素分析之結果，卻發現目的事業組織信譽遭受影響，其原因係來自於「資料保護受損」、「影響業務運作」及「影響法律規章遵循」違反後之結果，且就主管機關之

立場，應著重於民眾之權益維護，與通訊傳播事業個別公司之信譽或是形象無關，故建議針對通訊傳播事業所擁有之資產群組，分類為「關鍵業務」、「支援業務」及「行政業務」，依據「資料保護受到損害」、「影響業務運作」及「影響法律規章遵循」三個構面，將資產群組之安全等級區分為「高」、「中」、「普」三級進行資產安全等級評估，才是目的事業真正關心的重點所在，亦可相對簡化目的事業之作業負擔。

- 本程序所鑑別之資訊系統安全等級，可作為後續選擇安全控制措施之依據，分別建議適用之安全防護基準，資產群組安全等級列「高」者，可考量進一步實施詳細風險評鑑，俾利進行風險管理。亦可兼顧詳細風險評鑑方法之優點。

- 國內已通過 CNS/ISO/IEC 27001 驗證之組織，分析其驗證範圍，僅有極少數以全組織通過驗證，通常僅侷限於資訊機房或資訊單位，更甚者僅有以單一伺服器作為驗證標的者，而未能將組織核心業務納入其中，似有規避敷衍、以偏概全之嫌，表面上符合資安會報之要求，但改善程度又遠不及於全機關，對於資安事故之防範成效未能有效提升，以達到資安會報防禦機制強度之要求水準。

- 就現今國內環境來看，並非每一組織皆將導入資訊安全標準視為全面性的策略，大部分組織將資訊安全標準的導入視為階段性任務，或強制性的被要求，通常僅單一部門導入與通過驗證，並未將標準之管理制度與準則擴大至整體組織，此係本計畫亟欲探索之現象，期能藉此規劃出適用於我國通訊傳播產業之資訊安全管理制度。

- ISO/IEC 27005 的歸納結論分別為「資訊風險管理的概念是【持續】的處理過程」以及「明確地指導政府機關(構)或企業組織如何有計畫的規律執行【資訊安全風險管理作業】」。

- 在 ISO/IEC 27005:2008 內容中說明組織自行可以根據其風險評鑑目標選擇其風險評鑑作法，同時在其【附錄 E】內容中舉例說明「高階風險

評鑑作法」與「詳細風險評鑑」兩種作法，其中每種作法各有其特色、適用狀況與注意事項，將於後續章節進行說明。

5. 結論與建議

5.1.結論

- 行政院之資訊系統分類分級鑑別機制，依據「資料保護受到損害」、「影響業務運作」、「影響法律規章遵循」、「人員傷亡」、「損害組織信譽」及「其他」等六大構面，分別考量資訊系統於發生資訊安全事故時可能造成的衝擊，藉此評定資訊系統之等級。得以視為營運衝擊分析或高階風險評鑑的一部分，本研究所進行之問卷調查初步分析，通訊傳播事業對於資訊安全之重視，首重對於「損害組織信譽」之衝擊，其餘構面則與行政院資通會報之方法相近，但是進一步進行因素分析之結果，卻發現目的事業組織信譽遭受影響，其原因係來自於「資料保護受損」、「影響業務運作」及「影響法律規章遵循」違反後之結果，且就主管機關之立場，應著重於民眾之權益維護，與通訊傳播事業個別公司之信譽或是形象無關，故建議針對通訊傳播事業所擁有之資產群組，分類為「關鍵業務」、「支援業務」及「行政業務」，依據「資料保護受到損害」、「影響業務運作」及「影響法律規章遵循」三個構面，將資產群組之安全等級區分為「高」、「中」、「普」三級進行資產安全等級評估，才是目的事業真正關心的重點所在，亦可相對簡化目的事業之作業負擔。

- 考量業管之目的事業中，不乏業務項目雷同，組織結構相近者，故採行分類分級之方法，是兼顧行政效率與資安防護的適切作法，但是參考美國或是我國行政院資通安全會報之最新作法，均是將資通安全等級區分為普、中、高三級，再考量 3.1 節之通訊傳播事業特性分析，本研究所涵蓋之目的事業其業務屬性差異頗大，如：第一類電信及第二類電信，對於通信秘密之保護有嚴格之法令限制，對於機密性之要求其高，或如：有線廣播電視業者等，擁有大量之電信、傳播機線設備，對於可用性要求極高者，但是也有如：廣播節目供應事業，著重於節目及廣告之管理，對於資訊安全管理之要求極低者，故建議企業安全等級宜區分為 A、B、

C 三級，以針對不同之安全等級，建議適用之安全防護基準，較為妥適。

- 通訊傳播事業對於資訊安全之重視程度，不因為員工人數或是資本額度而有所差異，相當重視組織之信譽，極力避免因為人員傷亡、侵犯個人隱私、資料保護受到損害而影響業務運作等，而降低顧客對於企業之信任。

- 欠缺系統化的方式推動資訊安全管理系統，整體資訊安全之營運績效無法呈現，未實施營運風險評鑑、導致資源投入比例無法提高，甚至安全概念無法融入組織文化。

- 影響企業資安資源投入比例高低之主要原因，來自於外部力量，主管機關的態度，對於產生行動之正當性具有決定性之影響；但是導入 ISMS 之後，能否具體落實，則有賴於企業於建構風險意識的過程，產生內部力量，形塑資安文化。

- 適用於產業所需之資安規範，將資安領域契合企業之營運領域，於主要營運流程中，強化資安作為，才能凸顯資安策略價值，使目的事業樂於配合。

- 目前通訊傳播事業相關資安作為，普遍認為重要，但是落實程度有待加強者，應列為後續稽核之重點項目。

- 協助業者建立資訊安全量測指標，將可有效提升控制措施之有效性。

5.2.建議事項

5.2.1. 資通安全管理機制影響構面、評估等級及實施範圍

通訊傳播事業宜依據下列步驟，實施高階風險評鑑作法(High-Level Risk Assessment)，評估資通安全等級，以定義資通安全範圍與邊界，確定資通安全需求水準，作為後續訂定風險處理優先順序之參考：

依據執照核發之營業項目範圍內，調查通訊傳播事業營運所需之資產

群組，若組織規模龐大者，得區分為不同之事業體或是部門，區分為以下三大類，分別進行資產群組之調查：

- 關鍵業務：包含下列項目：
  - 電信事業之電信設備、電信機線設備、微波電台、管線基礎設施及電信終端設備等。
  - 有線廣播電視事業之頭端、信號處理設備、分配線網路、分配中心、光纖投落點及訂戶終端設備等。
  - 無線廣播(電視)事業之電臺、轉播站、節目中繼電臺、纜線、信號處理設備等。
  - 衛星廣播電視事業之地球電臺、衛星機構、衛星轉頻器等。
- 支援業務：指廣播電視節目供應業務、第二類電信轉售服務業務及支援通訊傳播事業營運所需之資訊處理設施，但非屬關鍵業務者，例如：客戶服務、帳務、會計系統，或是涉及客戶個人資料蒐集、處理及利用者。
- 行政業務：指通訊傳播事業內部輔助單位之業務項目，例如：人事、行政、總務等。

依據每一資產群組失效後之「衝擊影響程度」，評估資通安全等級，決定資通安全管理機制改善之優先順序，並每年定期更新。

表42 影響構面／安全等級評估

安全等級 影響構面	普 （等級 1）	中 （等級 2）	高 （等級 3）
1. 影響業務運作	• 系統容許中斷時間較長（如：超過 1 小時以上） • 系統故障對社會秩序、民生體系運作不致造成影響或僅有輕微影響	• 系統容許中斷時間短（如：1 小時以內） • 系統故障對社會秩序、民生體系運作將造成嚴重影響 • 系統故障將造成關鍵業務執行效能嚴重降低	• 系統容許中斷時間非常短（如：10 分鐘以內） • 系統故障對社會秩序、民生體系運作將造成非常嚴重影響，甚至危及國家安全 • 系統故障將造成關鍵業務執行效能非常嚴重降低，甚至業務停頓
2. 資料保護受到損害	• 一般性資料 • 資料若外洩或遭竄改，不致影響個人權益或僅導致個人權益輕微受損	• 敏感性資料 • 資料若外洩或遭竄改，將導致個人權益嚴重受損之資料	• 機密性資料 • 資料若外洩或遭竄改，將導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損
3. 法律規章之遵循	系統運作、資料保護、資訊資產使用等，若未遵循相關規範辦理，不會導致機關違反法規命令。	系統運作、資料保護、資訊資產使用等，若未遵循相關規範辦理，將導致機關違反法規命令，並伴隨輕微後果，如：行政處分或罰鍰等	系統運作、資料保護、資訊資產使用等，若未依循相關規範辦理，將導致機關從根本上違反法律，並導致嚴重不良後果，如：損害賠償、罰金或是刑責

5.2.2. 資通安全實施程序與風險評鑑模式之建議

5.2.2.1. 資通安全實施程序

ISO/IEC 27003 ISMS 專案實施程序之最終產物為 ISMS 專案計畫書，可供本計畫後續之工作項目「實施計畫參考範本」之參考。

ISMS 專案施行程序，詳見表 43 所示，詳細摘錄規劃 ISMS 階段之重點工作、活動項目、先備完成項目及產出文件，並註記該工作項目符合 ISO/IEC 27001 之要求項目。

表43 ISMS 專案施行程序檢查表

實施階段 ISO/IEC 27003	步驟編號	活動，參考 ISO/IEC 27003	步驟事前需求	文件輸出	參考對照 ISO/IEC 27001
1.獲得管理階層的承諾，啟動 ISMS 專案	1.	蒐集公司營運目標	無	公司營運目標清單	N/A
	2.	增進現有管理系統的瞭解	無	現有管理系統說明書	N/A
	3.	5.2 定義 ISMS 的目標，資訊安全需求與和營運需求	1, 2	綜整 ISMS 的目標，資訊安全需求與營運需求	N/A
	4.	蒐集適用於營運的相關管理規範與產業標準	無	綜整適用於營運的相關管理規章與產業標準	N/A
	5.	5.3 定義初步的 ISMS 範疇	3, 4	定義 ISMS 初步範疇說明書 定義 ISMS 扮演的角色與責任	N/A
	6.	5.4 建立管理認同的營運案例及專案計畫	5	營運案例與有目的的專案計畫	N/A

實施階段 ISO/IEC 27003	步驟編號	活動，參考 ISO/IEC 27003	步驟事前需求	文件輸出	參考對照 ISO/IEC 27001
	7.	5.5 獲得管理認同與委託，並啟動實施 ISMS 的專案	6	啟動專案實施 ISMS 的管理認同	N/A
2. 定義 ISMS 範疇和 ISMS 政策	8.	6.2 定義組織邊界	7	●解釋組織的邊界 ●組織的功能與結構 ●透過邊界做資訊交換 ●營運資訊資產流程，責任範疇與外部範疇	4.2.1a) (部分)
	9.	6.3 定義資訊、通訊、科技邊界	7	●解釋 ICT 邊界 ●解釋資訊系統與通訊網路，解釋內部、外部範疇	4.2.1a) (部分)
	10.	6.4 定義實體邊界	7	●解釋 ISMS 實體邊界 ●對組織與其地理特性做解釋，解釋內外部範疇	4.2.1a) (部分)
	11.	6.5 根據 ISMS 範疇完成邊界的定義	8,9,10	產生文件，解釋 ISMS 的範疇與邊界	4.2.1a)
	12.	6.6 發展 ISMS 政策	11	管理階層認可的 ISMS 政策	4.2.1b)
3.引導組織分析	13.	7.2 定義資訊安全需求支援 ISMS	12	●主要流程的清單、功能、位置、資訊系統及通訊網路	N/A
				組織對機密性、完整性及可用性之需求	N/A
				組織對法令、規章、契約及營運資訊安全	4.2.1.c) 1)部分

實施階段 ISO/IEC 27003	步驟編號	活動，參考 ISO/IEC 27003	步驟事前需求	文件輸出	參考對照 ISO/IEC 27001
				的需求	
				已知的組織弱點清單	4.2.1.d) 3)
	14.	7.3 識別 ISMS 範疇內的資產	13	主要組織流程解釋	N/A
				組織主要流程資訊資產清查	4.2.1.d) 1)
				關鍵流程/資產類別	N/A
	15.	7.4 產生資訊安全評鑑	14	●組織的實際資訊安全狀態與評鑑文件，包括已存在資訊安全控制 ●組織的評定與評估的缺陷	4.2.1.e) 2) 部分
4.引導風險評估和選擇性風險處置選擇	16.	8.2 引導風險評鑑	15	●風險評鑑範疇 ●風險確認評鑑方法和組織的風險管理策略全景一致 ●風險接受條件	4.2.1.c) 1)
	17.	8.3 選擇控制目標與控制項措施	16	高階風險評鑑文件	4.2.1.e) 3) 部分
				識別深度風險評鑑的需求	N/A
				深度風險評鑑文件	4.2.1.e) 3) 部分
				整合風險評結果	N/A
	18.	8.4 得到實施 ISMS 的管理階層認同	17	風險與風險處理識別選項	4.2.1.f)
				選擇性的風險降低控制目標與控制措施	4.2.1.g)

實施階段 ISO/IEC 27003	步驟編號	活動，參考 ISO/IEC 27003	步驟事前需求	文件輸出	參考對照 ISO/IEC 27001
	19.	管理階層認可殘餘的風險	18	管理認可提議的剩餘風險文件(應為 8.4 的輸出)	4.2.1.h)
	20.	實施與操作 ISMS 的管理認證	19	實施與操作 ISMS 的管理認證文件(應為 8.4 的輸出)	4.2.1.i)
	21.	準備可行性陳述	18	可行性陳述	4.2.1.j)
5.ISMS 設計	22.	9.2 設計組織安全	20	組織結構，其資訊安全相關角色與責任	5.1.c)
				•ISMS 相關文件識別 •ISMS 紀錄與其使用儲存指示範例	4.3
				資訊安全政策文件	ISO/IEC 27002; 5.1.1
				資訊安全政策與程序基準(可能開發特定政策的可行方案，程序等等…)	
	23.	9.3 設計 ICT 與實體安全	20, 21	•實施給 ICT 與實體資訊系統選擇性安全控制執行過程專案計畫	4.2.2.c) 部分
	24.	9.4 設計 ISMS 特別之資訊安全	22, 23	報告與管理回覆過程解釋程序	7.1
	25.			•稽核解釋，監控與測量	4.2.1.a) 部分 4.2.3.b) 部分;6

實施階段 ISO/IEC 27003	步驟編號	活動，參考 ISO/IEC 27003	步驟事前需求	文件輸出	參考對照 ISO/IEC 27001
	26.			●訓練與認知方案	5.2.2
	27.	9.5 產生最終 ISMS 專案計畫	25	為實施流程進行實施專案計畫的管理認可	N/A
	28.	最終 ISMS 專案計畫	28	ISMS 組織特別實施專案計畫含組織活動計畫執行，ICT 與 ISMS 特別實施根據 ISO/IEC 活動一樣好的 ISMS 需求結果中，實體資訊安全說明	N/A

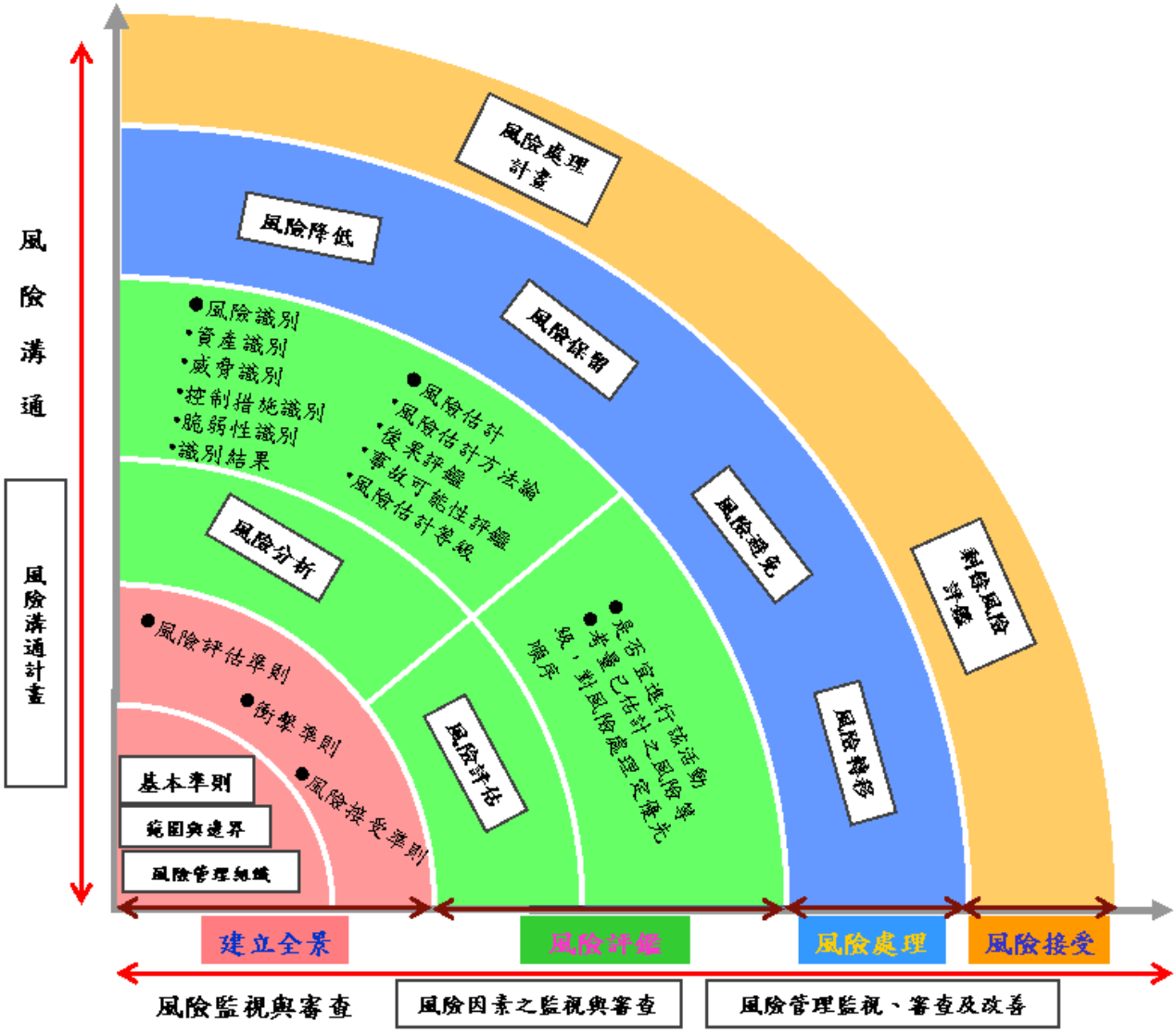
5.2.2.2. 風險評鑑模式

ISO/IEC 27005:2008 建議之風險評鑑模式，通常於兩個(或更多)循環中進行，首先實施「高階風險評鑑」，以識別出進一步評鑑之潛在高風險。下一循環再對涉及起始循環所揭露之潛在高風險作更深度考量，若此循環未能提供充分資訊以評鑑該風險，則要進行更詳細分析，可能是對整個範圍之某些部分，也可能使用不同之方法，完全由組織依據目標與風險評鑑之標的選擇其自身適用之風險評鑑作法。

前述 5.2.1 建議之資訊系統安全等級評估表(草案)：以資訊系統為區分之依據，考量其業務屬性，區分為：關鍵性業務、支援性業務及行政性業務，分別就：「資料保護受到損害」、「影響業務運作」、及「法規遵循」等構面，評定資訊系統安全等級，便是如以上所稱之「高階風險評鑑」。

經評定安全等級屬「高」級之資訊系統，則應進行詳細風險評鑑。建議之風險管理生命週期，詳如圖 60 所示。本風險管理生命週期係將 CNS/ISO/IEC 27005 之風險管理過程中中各項作業內容，區分為：建立全景、風險評鑑、風險處理及風險接受四個階段，對應其應執行之工作或是應產出之文件，依序由內向外逐項標記，以供讀者明瞭過程中之各項工作

細項。



資料來源：本計畫自行整理

圖60 風險管理生命週期

5.2.3. 資通安全管理之有效性量測方法與量測措施

ISO/IEC 27004:2009 提供發展與使用安全控制措施與測量方法之指引，用以評估 ISMS 實施 ISO/IEC27001 所描述控制措施之有效性，包含政策、風險管理、控制目標、流程及程序等之評估，協助鑑別哪些控制措施

需要改變或強化，但同時也特別強調沒有一種安全控制措施之測量方法可以完全保證安全。本標準之內容著重於測量模型、方法及過程之敘述，對於實務度量之技術，組織應根據所採行之安全控制措施，發展或採用適當的測量技術與工具,建議採用之資訊安全之測量構面樣板,詳見表 44 所示。

表44 資訊安全測量構面樣板

測量構面辨識	
測量構面名稱	測量名稱
事故識別碼	獨特特定組織事故識別碼
測量構面目的	說明介紹測量原因
控制措施/流程目標	控制措施/流程目標下的測量(已規劃或已實施）
控制措施(1)/流程(1)	控制措施/流程下的測量
控制措施(2)/流程(2)	可選擇：如果適用(已規劃或已實施)，如果允許可進一步將控制措施/流程群組化，包含在相同度量範圍之內
測量與屬性的目標	
測量目標	測量目標（實體）需經過測量方法描述它的屬性，測量目標可能包含流程、計畫、專案、資源、以及系統，或者是系統元件
屬性	測量對象的屬性或特徵，能藉由人為或自動化的方式分為定量或定性
基本度量值等級 (對於每個基本度量值 [1…n])	
基本度量值	基本度量值是指屬性條件和指定用於量化的測量方法。(例如：訓練人員數目、地點數、迄今為止累積的花費。）當資料被蒐集完畢，這些數值將被指定到一個基本度量值
測量方法	就特定級別而言，用於量化屬性的邏輯順序操作
測量方法類型	根據用於量化屬性的操作性質，有兩種方法可以區分： 主觀的：涉及人為判斷的量化 客觀的：基於數值規則的量化，如計數(Counting)

等級	數值或類型的有序集合，是能夠對應到基本度量值屬性。
等級類型	根據級別數值之間不同性質的關係，分作四種類型的等級：Nominal (名義)、Ordinal (次序)、Interval (等距)、Ratio (等比)
測量單元	特別數量，是經由定義且通過會議討論，任何其他同類型數量可被比較，用來表達兩個量的比例為數值
延伸測量規格	
延伸測量	延伸出兩個或多個基底度量功能的測量
測量功能	演算法或計算進行合併兩個或多個基底度量，級別與延伸測量的單元是基於級別與基本度量單元
指標等級	
指標	測量提供估計或是來自分析模型所需定義訊息之特定屬性的評價，而指標是分析與決策的基礎
分析模型	演算法或計算結合成相關決策的一或多個基底和延伸測量，是依據一個認知底下,或者假設基底和延伸測量及其行為的預期關聯會隨著時間更改
決策標準等級	
決策標準	門檻、目標或圖樣適用於確定採取行動、進一步調查，或描述在一個給定結果的信心水平的需要，決策標準將有助於解釋測量結果
測量結果	
指標詮釋	描述抽樣指標應該如何被解釋 (查看指標描述的樣本圖型)
報表格式	報告格式應該被確認且記錄存檔，描述對該組織或資訊所有者可能要記錄在檔案的觀察。報告格式將以視覺描繪測量結果，並提供了口頭解釋的指標，且報告的格式應該是客製化的形式
股東	
測量委託人	管理或其他利害關係人請求或要求相關的 ISMS 之效能

	(控管或集體控管)
測量審查人	驗證發展測量構面是否合適評估 ISMS 的效能(控管或集體控管)之人員或組織單位
資訊擁有者	擁有關於測量與屬性個體資訊，以及負責測量的人員或組織單位
資訊蒐集者	負責分析資料蒐集、記錄、儲存的人員或組織單位
資訊溝通者	負責分析資料與溝通管理結果的人員或組織單位
頻率/期間	
資料蒐集頻率	描述資料蒐集的頻率
資料分析頻率	描述資料分析的頻率
產出測量結果報表的頻率	描述測量結果產出報告的頻率(這個部分可能低於資料蒐集的頻率）
測量版本	測量版本的日期(到期或測量的有效性的更新）
測量期間	定義測量的時間區間
資料來源：ISO/IEC 27004:2009 附錄 A	

另建議之資訊安全測量構面範例，詳見 8.2 所示。

5.3.通訊傳播事業資訊通訊安全管理作業要點修訂

表45 通訊傳播事業資訊通訊安全管理作業要點修正條文對照表

修正規定	現行規定	說明
一、國家通訊傳播委員會（以下簡稱本會）為辦理通訊傳播事業資訊通訊安全（以下簡稱資通安全）管理作業，依本會組織法第三條第八款之規定，特訂定本要點	一、國家通訊傳播委員會（以下簡稱本會）為辦理電信事業資訊通訊安全（以下簡稱資通安全）管理作業，依本會組織法第三條第八款之規定，特訂定本要點	依據本會組織法第三條，增修業管之目的事業為：通訊傳播事業 本條酌作文字修正
二、為執行通訊傳播事業資通安全管理作業，應製作通訊傳播事業資通安全管理手冊 本手冊應符合保障通信安全及維護使用者權益之原則。其內容應包含下列各款事項： （一）資通安全管理標準 （二）資通安全等級評估 （三）資通安全管理機制 （四）資通安全教育訓練 （五）資通安全應變通報 （六）資通安全實施評鑑 本手冊之研訂，應邀集相關業者、專家或機構共同討論，並視實施情況檢討修正 本手冊訂定或修正完成，應循文書作業程序簽核並於本會網站公告	二、為執行電信事業資通安全管理作業，應製作電信事業資通安全管理手冊 本手冊應符合保障通信安全及維護使用者權益之原則。其內容應包含下列各款事項： （一）資通安全管理標準 （二）資通安全等級評估 （三）資通安全管理機制 （四）資通安全教育訓練 （五）資通安全應變通報 （六）資通安全實施評鑑 本手冊之研訂，應邀集相關業者、專家或機構共同討論，並視實施情況檢討修正。 本手冊訂定或修正完成，應循文書作業程序簽核並於本會網站公告	依據本會組織法第三條，增修業管之目的事業為：通訊傳播事業 本條酌作文字修正
三、為確保通訊傳播事業資料、系統及設備正常運作，本會應依本手冊所定事項，定期蒐集通訊傳播事業資通安全相關資訊，並適時給予通訊傳播事業協助、建議或採行其他合宜之輔導措施	三、為確保電信事業資料、系統及設備正常運作，本會應依本手冊所定事項，定期蒐集電信事業資通安全相關資訊，並適時給予電信事業協助、建議或採行其他合宜之輔導措施	依據本會組織法第三條，增修業管之目的事業為：通訊傳播事業 本條酌作文字修正
四、通訊傳播事業依據本手冊內容，應訂定「資通安全管理實施計畫」，其範本由本會提供		本條新增

修　正　規　定	現　行　規　定	說　　明
五、本會執行通訊傳播事業資通安全管理，認有必要時，得向通訊傳播事業索取文書、資料或物品，並得通知其到場陳述意見或到場實施勘驗 依前項規定實施勘驗時，應先以書面或其他適當方式，通知勘驗場所之使用者或可為代表之人在場。實施勘驗時，應作成紀錄，記載實施時間、處所及其他必要事項，並由在場之人簽名、蓋章或按指印 依第一項規定取得文書、資料或物品，如文書、資料或物品之提供者表明文書、資料或物品於調查程序完成應返還，應注意不得損及完整性；無需返還者，應妥善保存或為其他適切之處理 依第一項規定到場實施勘驗時，應維持勘驗物品及場所之完整	四、本會執行電信事業資通安全管理，認有必要時，得向電信事業索取文書、資料或物品，並得通知其到場陳述意見或到場實施勘驗 依前項規定實施勘驗時，應先以書面或其他適當方式，通知勘驗場所之使用者或可為代表之人在場。實施勘驗時，應作成紀錄，記載實施時間、處所及其他必要事項，並由在場之人簽名、蓋章或按指印 依第一項規定取得文書、資料或物品，如文書、資料或物品之提供者表明文書、資料或物品於調查程序完成應返還，應注意不得損及完整性；無需返還者，應妥善保存或為其他適切之處理 依第一項規定到場實施勘驗時，應維持勘驗物品及場所之完整	依據本會組織法第三條，增修業管之目的事業為：通訊傳播事業 本條酌作文字修正
六、電信業務申請「開放赴大陸投資業務項目」前，應將其資通安全管理之實施作業範圍報經本會核准後，向本會認可之資通安全管理機制驗證機構，就核准之作業範圍申請驗證，並取得符合 ISO/IEC27001 標準及通訊傳播事業資通安全管理手冊之 ISO/IEC27011 增項稽核表驗證合格證明 涉及國人個人資料之事項或業務部門、業務功能及系統等，例如電信業者之用戶資料庫、客服系統/客服中心、帳務系統/帳務中心等，均限制不得移往大陸設置營運或於當地投資、合作 電信事業依固定通信業務管理規則第七十條第一項第二	五、電信事業申請在大陸地區投資電信業務前，應將其資通安全管理之實施作業範圍報經本會核准後，向本會認可之資通安全管理機制驗證機構，就核准之作業範圍申請驗證，並取得符合 ISO/IEC27001 標準及電信事業資通安全管理手冊之 ISO/IEC27011 增項稽核表驗證合格證明 電信事業依固定通信業務管理規則第七十條第一項第二	本條序號修訂，內容修訂依據「在大陸地區從事投資或技術合作服務業禁止類經營項目」： 投資電信業（第二類電信事業之一般業務）受理審查原則如下： （一）開放赴大陸投資第二類電信事業一般業務，現階段適用範圍為大陸地區所稱之「存儲轉發業務、信息服務業務、在

修　正　規　定	現　行　規　定	說　　明
款或第七十二條之一，申請經營與大陸地區合作之電信業務者，應於系統審驗前，向本會認可之資通安全管理機制驗證機構，就核准之作業範圍申請驗證，並取得符合 ISO/IEC27001 標準及電信、傳播事業資通安全管理手冊之 ISO/IEC27011 增項稽核表驗證合格證明	款或第七十二條之一，申請經營與大陸地區合作之電信業務者，應於系統審驗前，向本會認可之資通安全管理機制驗證機構，就核准之作業範圍申請驗證，並取得符合 ISO/IEC27001 標準及電信事業資通安全管理手冊之 ISO/IEC27011 增項稽核表驗證合格證明	線數據處理及交易處理業務、因特網數據中心業務及因特網接入服務業務」 （二）赴大陸投資之臺灣業者應檢具已取得規範電信事業資訊安全管理系統（ISMS）之 ISO 27011 認證之證明文件 （三）涉及國人個人資料之事項或業務部門、業務功能及系統等，例如電信業者之用戶資料庫、客服系統/客服中心、帳務系統/帳務中心等，均限制不得移往大陸設置營運或於當地投資、合作 （四）赴大陸投資之臺灣業者，其出資不得以專門技術、專利權或著作財產權等涉及技術事項為之
七、本會應於網站公告業經本會認可之資通安全管理機制驗證機構名單	六、本會應於網站公告業經本會認可之資通安全管理機制驗證機構名單	本條序號修訂
八、本會應定期於網站公布業經資通安全管理機制驗證合格之通訊傳播事業名單	七、本會應定期於網站公布業經資通安全管理機制驗證合格之電信事業名單	本條序號修訂 依據本會組織法第三條，增修業管之目的事業為：通訊傳播事業

通訊傳播事業資訊通訊安全管理作業要點修正條文對照表英文版，詳如附件 3。

5.4.通訊傳播事業資通安全管理手冊修訂建議

相關修訂建議，詳如附件 4。

5.5.通訊傳播事業安全控制措施修訂建議

(1)通訊傳播事業資通安全管理內部稽核修訂對照表，詳如附件 6。

(2)通訊事業增項稽核修訂對照表，詳如附件 7。

(3)傳播事業增項稽核修訂對照表，詳如附件 8。

(4)通訊傳播事業個資保護控制措施內部稽核表，詳如附件 9。

6. 辦理資通安全管理機制座談會

本階段總計舉辦 6 場座談會與 1 場成果發表會，邀請具資通安全領域專業之專家學者與業者代表參與座談，以廣納各方意見，做為後續修改之方向。會議日期、內容及與會專家說明，詳見表 46 與表 47 所示：

表46 資通安全管理機制座談會場次表

日　期	工作內容
100/5/10(二) AM10:00	舉辦第 1 場資通安全管理機制座談會，邀請 30 家第一類電信事業業者出席，實到 16 家業者(24 人)，另有 6 位學者專家。(會議紀錄詳見附件 10)
100/5/10(二) PM2:00	舉辦第 2 場資通安全管理機制座談會，邀請 38 家第二類電信事業業者出席，實到 7 家業者(7 人)，另有 6 位學者專家。(會議紀錄詳見附件 11）
100/5/12(四) AM10:00	舉辦第 3 場資通安全管理機制座談會，邀請 45 家傳播事業業者出席，實到 15 家業者(15 人)，另有 8 位學者專家。(會議紀錄詳見附件 12）
100/8/12(五) AM10:00	舉辦第 4 場資通安全管理機制座談會，邀請 33 家第一類電信事業業者出席，實到 16 家業者(25 人)，另有 5 位學者專家。（會議紀錄詳見附件 13）
100812(五) PM2:30	舉辦第 5 場資通安全管理機制座談會，邀請 47 家第二類電信事業業者出席，實到 13 家業者(17 人)，另有 4 位學者專家。（會議紀錄詳見附件 14）
100/8/15(一) PM2:30	舉辦第 6 場資通安全管理機制座談會，邀請 46 家傳播事業業者出席，實到 7 家業者(8 人)，另有 5 位學者專家。（會議紀錄詳見附件 15）
100/10/17(一) PM2:00	舉辦研究成果發表會，邀請近 300 家第一類、第二類及通傳事業業者出席，實到 39 業者(41 人)，另有 2 位學者專

	家。(會議紀錄詳見附件 16)

資料來源：本計畫自行整理

表47 資通安全管理機制座談會參與專家名單

姓名	單位職稱
林子群	行政院國家資通安全會報技術服務中心顧問
方鴻春	行政院國家資通安全會報技術服務中心顧問
蕭瑞祥	淡江大學資訊管理學系教授
陳振楠	中國科技大學資訊管理系教授
侯望倫	南亞技術學院資訊管理學系助理教授
查士朝	台灣科技大學資訊管理學系助理教授
陳文政	淡江大學國際事務與戰略研究所助理教授
鄧永基	TUV 漢德技術監督服務(亞太)有限公司業務總監
黃廷弘	TUV 漢德技術監督服務(亞太)有限公司經理
李清賓	TUV 漢德技術監督服務(亞太)有限公司經理
陳家楨	TUV 漢德技術監督服務(亞太)有限公司經理
吳玉婷	漢德技術監督服務有限公司(TUV)經理
陳志明	勤業眾信聯合會計師事務所協理
舒世明	勤業眾信聯合會計師事務所經理
陳亮宏	勤業眾信聯合會計師事務所(Deloitte)副理
徐筱蕾	勤業眾信聯合會計師事務所副理
何星翰	SGS 台灣檢驗科技股份有限公司經理
郭廷偉	臺灣檢驗科技股份有限公司國際驗證服務部經理
林志明	臺灣檢驗科技股份有限公司國際驗證服務部副理
張美月	資拓宏宇國際股份有限公司顧問服務事業處協理
高林銓	資拓宏宇國際股份有限公司顧問
張榮鋒	環奧國際驗證有限公司臺灣區經理

姓名	單位職稱
陳昇智	環奧國際驗證有限公司主任稽核師
莊珮瑩	德欣寰宇股份有限公司副理
蔡長衍	中華電信(股)公司工程師
李世仁	中華電信(股)公司助理工程師
謝幸惠	中華電信(股)公司助理管理師
陳方元	中華電信(股)公司助理工程師
方偉昌	中華電信(股)公司助理研究員
鄭皓陽	中華電信研究所助理研究員
廖慧如	中華電信研究所助理研究員
楊宏盛	台灣大哥大股份有限公司經理
許嘉裕	遠傳電信股份有限公司經理
郭文雪	遠傳電信股份有限公司資深專員
黃天祥	大同電信股份有限公司協理
林炳坤	威達雲端電訊股份有限公司協理
白明宜	威達雲端電訊股份有限公司副理
裔式漁	北亞環球光纖通訊網絡股份有限公司總經理
蕭智仁	大豐有線電視(股)公司資訊室經理
周青禾	中華國際通訊網路(股)公司副理
陳佩青	中華國際通訊網路(股)公司工程師
何瑤先	全球光網電訊股份有限公司維運經理
張淑琪	威寶電信股份有限公司專案經理
洪誌謙	威寶電信股份有限公司專案副理
談民廉	台灣國際纜網通信股份有限公司技術經理
郭靜娟	台灣國際纜網通信股份有限公司高級專員
楊德冠	台灣國際纜網通信股份有限公司業務專員
潘秋雙	台灣國際纜網通信股份有限公司工程師

姓名	單位職稱
陳佑齊	國際環球通訊網絡股份有限公司工程師
邱毓容	台亞衛星通訊股份有限公司法務經理
張君毅	台亞衛星通訊股份有限公司副理
鄭存慈	台亞衛星通訊股份有限公司法務專員
陳忠義	亞太電信股份有限公司副理
張佳絹	亞太電信股份有限公司資深工程師
李宏信	全聯有線股份有限公司工程師
魏嘉互	屏南有線電視股份有限公司工程師
張鴻隆	天外天有線電視股份有限公司副理
林宗建	新海瓦斯(股)公司副課長
詹志敏	南頻電信股份有限公司資訊部協理
楊暐竣	協志聯合科技股份有限公司工程師
王銘鴻	協志聯合科技股份有限公司工程師
張伯昱	香港商第一線有限公司台灣分公司協理
陳裕榮	萬宙商信股份有限公司技術經理
林義澤	安源資訊股份有限公司系統工程師
黃日昇	凱擘(股)公司資訊室主任
崔大維	安源通訊(股)公司資訊室協理
張立寰	臺灣網路認證(股)公司組長
張行健	臺灣網路認證(股)公司稽核
盧振裕	台灣寬頻通訊顧問(股)公司資訊技術協理
游純真	全景電訊(股)公司
高瑞陽	台灣數位寬頻(股)公司組長
張智堯	台固媒體(股)公司專案副理
林逸楓	家樂福電信股份有限公司技術與營運經理
劉升元	神坊資訊(股)公司專員

姓名	單位職稱
王家權	神坊資訊(股)公司專員
羅文璣	統一超商股份有限公司法務經理
張之瑜	統一超商股份有限公司法務專員
姚愈金	統一超商股份有限公司商品經理
黃珍容	統一超商股份有限公司商品經理
黃朝安	是方電訊股份有限公司
鄭嘉豐	關貿網路股份有限公司專案經理
蕭國仁	大台北寬頻網路股份有限公司管理部經理
林仔玲	神通電腦股份有限公司工程師
兵伊坤	匯智資訊股份有限公司工程師
李柏孜	愛爾達科技股份有限公司公關經理
詹前程	台灣恩益禧股份有限公司主任
謝明宏	先啟資訊系統股份有限公司經理
林蘭馨	偉盟系統股份有限公司
汪坤福	寶潤資訊科技有限公司網管工程師
吳怡萱	願景電信事業股份有限公司法務
黃偉程	願景電信事業股份有限公司工程師
陳螢幟	台灣凱訊股份有限公司經理
竇恒泰	臺北廣播電臺技術員
莊勝鈞	臺灣電視事業股份有限公司工程師
施國輝	民間全民電視股份有限公司工程師
許振庭	財團法人公共電視文化事業基金會新媒體部工程師
黃靖如	三立電視股份有限公司資訊部組長
張書銘	國衛傳播事業股份有限公司
廖秋錦	緯來電視網股份有限公司副理
林志誠	英屬蓋曼群島商艾科思達亞洲多媒體股份有限公司IT經理

姓名	單位職稱
林健雄	三商多媒體股份有限公司副總經理
吳慧真	美商超躍有限公司台灣分公司副總監
李慶鈴	美商超躍有限公司台灣分公司行政專員
白健文	財團法人台北國際社區文化基金會總經理
沈榮樹	財團法人台北國際社區文化基金會經理
蔡玟瑛	新加坡商全球體育衛星電視(ESPN) 法務部經理
李德璀	東森電視事業(股)公司資訊管理室協理
褚志仁	霹靂國際多媒體(股)公司法務經理
許育仁	霹靂國際多媒體(股)公司主任
陳逸明	八大電視股份有限公司管理部資訊組組長
馬維新	中華電視股份有限公司資深工程師
林政緯	中華電視股份有限公司法務專員
宋梅倫	香港商亞太星空傳媒有限公司資訊部經理
謝景仁	台灣藝術電視台工程部副理
吳豪章	星際傳播股份有限公司 MIS 助理
蕭翔文	全球商業網技術處資訊管理部主任

資料來源：本計畫自行整理

座談會意見彙整表，詳見表 48 所示：

表48 資通安全管理機制座談會意見彙整表

項次.	座談會意見	處理情形
100/5/10 針對第一類電信業者召開之資通安全管理機制座談會專家及業者所提意見		
1	個資法施行細則即將訂頒實施，一旦發生個資外洩，除了損害賠償之外，行政機關很快就會行使行政檢查權，業界應有策略性的作法以為因應	已於附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)內容三、要項說明（四）

項次.	座談會意見	處理情形
		個人資料保護項下,增訂個人資料保護(pp6~7)要求內容
2	重點應放在風險分析,除了ISO27005之外可能還不夠,可參考 BS25999,先做 BIA 鑑別出核心業務,核心業務需要哪些硬體、軟體來支援。再作風險分析,會比較完整	資通安全等級評估方法,如 BS25999 所述之營運衝擊分析,內容詳如附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)pp2~3
3	企業應從風險評鑑著手,首先鑑別出核心業務,接著識別出核心業務有哪些風險存在,可能會受到天災或人為損害影響,造成營運無法持續運作。識別出風險後,才能將企業的資源作有效的運用。識別的方法已非常普遍,重點在於能否落實執行	通訊傳播事業宜先實施資通安全等級評估(高階風險評鑑作法(High-Level Risk Assessment),評估資通安全等級,以定義資通安全範圍與邊界,確定資通安全需求水準,作為後續訂定風險處理優先順序之參考,詳見附件4通訊傳播事業資通安全管理作業手冊(修訂草案)pp2~4
5	風險分析、風險評鑑是很重要的輸入項,但在體系的實施或系統導入的執行面,以過往的經驗來說,關注的層面主要還是在管理系統,不管是從資料保護或個資法的角度來看,檢查的環節裡針對技術面的實施並未有很落實的描述,或者在檢測的部分並未有很清楚的標準被定義出來。建議可在本次的研究中把技術面的要求作比較實質的描述。以電信業來說,電信機房是	有關通訊傳播事業之增項控制措施,已增訂於附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄7、8

項次.	座談會意見	處理情形
	很重要的關鍵設備，套用 ISO27001 的規定，只會告訴我們實體設備應有門禁，但到底需要什麼樣的門禁？機房座落的位置應在何處？這些部分都是管理系統中未加以描述的。這些實體安全與邏輯安全若沒有把真正的強度加進來的話，執行時不會特別關注，在檢查的時候也看不到，但最有可能出問題的卻是在這個部分。以 SONY 事件為例，是技術上的失能，是系統本身安全機制強度不夠，發生的是系統性的崩潰。企業無法承受的是系統化的錯誤，系統化的錯誤大多來自於技術失能，但目前大部分的規範或標準，在技術上的描述都不夠深入、明確，讓業者只能自行摸索，這部分仍有改善的空間	
6	台灣推動 ISMS 的進程，目的事業主管機關扮演很重要的角色，若目的事業主管機關有所要求，業者自然會配合。以衛生署為例，去年度補助醫院導入 ISMS，許多醫院即陸續通過 ISMS 的認證。就執行面的有效性來看，第一類電信業者會考慮得比較周全，不像某些政府機關是為了通過而通過。政府機關目前的作法，建議先針對資訊系統做分類分級，篩選出重要的資訊系統，找出系統間的關聯，接著作風險評鑑，再進行風險處理	電信法增訂第 56 條：為確保電信事業系統設備、資料及網路之安全，保障民眾通信權益，電信事業應辦理下列事項： 一、建立資通安全管理機制 二、建立資通安全防護及偵測設施 三、建立資通安全聯防及資通安全事件之通報、處理、回報等應變措施 建議通訊傳播事業宜提早因應，建立企業風險文化，履行法定義務。已明確表達主管機

項次.	座談會意見	處理情形
		關的立場
7	企業或機關導入 ISMS 的動機多來自於主管機關的要求，若只有外部的力量，通常會做得心不甘情不願，多半選擇最小範圍導入，敷衍了事。若能演化為內部的力量，逐漸形成企業文化，將能發揮最大成效	研究報告3.3個案訪談中發現,當組織的營運領域契合資安領域時,將由組織內部產生趨動資安標準導入之動能，並經由「風險意識文化建置過程」，以重新建構組織成員對於資安的意識,使組織成員擁有正確的資安認知與行為。詳見期末報告 pp45~55
8	國內導入 ISMS 最常見的狀況：多侷限在 IT 單位，核心作業流程都未納入。組織內真正重要的核心業務是否被界定出來？還是只做自己想做的部分？為何大部分的機關或企業只選擇某一範圍執行導入，最主要的原因仍是預算考量與需投入的資源多寡，造成機關或企業卻步。建議仍應從全組織的觀點做整體資安的考量，才會較有成效	本次規劃依據執照核發之營業項目範圍內,調查通訊傳播事業營運所需之資產群組，若組織規模龐大者,得區分為不同之事業體或是部門,區分為以下三大類,分別進行資產群組之調查,以界定保護之範圍,詳見附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)p2
9	企業內部單位組織太多，初期計畫全面實施導入，無論是否為核心業務均導入 ISMS，但經評估後發現全公司導入是做不到的。採取的策略是：有上級主管機關或業務要求的優先執行導入，至少先符合法令的要求。近兩年 NCC 提出資安管理規範	執照核發之營業項目範圍內,調查通訊傳播事業營運所需之資產群組,若組織規模龐大者,得區分為不同之事業體或是部門,詳見附

項次.	座談會意見	處理情形
	後，業界也意識到導入 ISMS 為趨勢，除了外部的要求之外，內部也有自省，並不只是單純由於 NCC 的要求。由前端的訂單系統、帳務系統逐步實施。去年 NCC 加入 ISO27011 的要求之後，針對電信網路的部分也開始執行 ISMS 的導入。相關資源的獲得，來自總公司的要求、與其他同業的比較或主管的想法，或者接觸到某些活動(例如 CIIP)後，意識到有此需求。以政策角度，每年初會訂定相關指標，檢視業務執行是否達到水準	件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)p.2
10	資通安全管理要點納入 ISO27011 後，稽查表訂定要考慮到台灣的現況，全面移植國外的制度不見得適用。在個資議題開始發酵後，通過 ISO27000 系列的認證不代表個資的防護 OK，應如何確認個資防護符合規定？建議可參考 NIST SP800-122 這份文件，可提供個資安全維護作為策略性的明確作法，清楚列出個資保護的控制措施	有關增項稽核表，已全數加以清查，並區分為通訊及傳播事業，分別有適用之控制措施，詳見附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 7、8
11	導入 ISMS 並非因為主管機關的要求，而是意識到重要性而主動進行，分期逐步擴大範圍。尤其在社會期待與主管機關的壓力下，特別注重資通安全。衛生署編列預算補助署立醫院通過 ISMS，電信產業是否也能獲得主管機關的補助	目前主管機關尚無編列補助預算計畫，但未來可以從加強通訊傳播事業資通安全管理機制之教育訓練著手，建議 NCC 納入參考
12	如何證明 ISMS 的有效性量測，目前朝向由 CIA 的面向來考量，納入個資保護的所有流程，包含業務、IT 都納入，防止個資被竊取與不當使用。並且由防禦系統與偵測系統中獲得數據，避免人為統計干擾結果	ISO/IEC 27004 特別強調沒有一種安全控制措施之測量方法，可以完全保證安全，現有之度量技術恐無法完全達到預期之效果，但是一旦可以量測，通常可

項次.	座談會意見	處理情形
		以獲致具體之成效
13	外商投資的公司，總公司已有 ISO 相關辦法，但並未移植到台灣分公司，台灣分公司只有機房，網管中心或是客戶資料都存在總公司，NCC 要求台灣分公司進行 ISO 機制的認證、資安管理或安全機制，執行上會有困難。若 NCC 有所要求，希望待電信法修正通過後，取得法律授權，在有法源依據、明確法規、明確施行細則及罰則的情況下，並正式行文，外商總公司即會配合辦理。目前外商公司的態度則是觀望中	本手冊主要為提供產業規範,輔導目的事業逐漸落實資通安全管理機制 另電信法增訂第 56 條:為確保電信事業系統設備、資料及網路之安全,保障民眾通信權益,電信事業應辦理下列事項： 一、建立資通安全管理機制 二、建立資通安全防護及偵測設施 三、建立資通安全聯防及資通安全事件之通報、處理、回報等應變措施 建議通訊傳播事業宜提早因應,建立企業風險文化,履行法定義務
14	瓦斯公司僅因為瓦斯幹管中埋了光纖，被列為第一類電信業者，電纜出租用戶數很少，若主管機關持續要求全面導入 ISMS，在無法負荷的情況下，可能考慮放棄此業務	建議參考資通安全等級評估方法,進行影響構面評估後,再行決定
15	資通安全等級的自我評估，如何確認評估符合事實？因評估構面不夠廣、法令適用不夠完善，建議適度調整。	已參照行政院規定加以修訂,將影響構面提昇至六個,並區分為三級,應可滿足需求,詳見附件 4 通訊傳播事

項次.	座談會意見	處理情形
		業資通安全管理作業手冊(修訂草案)(二)資通安全等級評估 pp2~4
16	ISO27011 驗證的相關疑義，有必要形成共同見解，建議適時釐清，以符合產業的需求	已修訂於附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 7、8
17	業者所提報的自評資料，NCC 並未有適時的意見回饋，目前業者只能根據自我認知的作業方式，自行摸索。建議後續可透過座談方式，提供更多資訊，以利業者配合	轉請主管機關參考
18	主管機關訂定績效的量測指標時必須很小心，數據若不能利用系統自動化統計，人工計算需耗費太多工時，反而沒有績效。ISO27004、ISO27005 強調控制措施的有效性不是由單一的措施來看，是由安全目標的角度綜整出一個指標	納入規劃參考
19	建議 NCC 不需訂定可用率的指標，只需要求業者提供安全、可靠的服務，市場自然會淘汰無法達到的業者	納入規劃參考
20	針對 SCOPE，NCC 是否有明確範圍？基地台是否包括在內？另有關驗證天數，ISO27001 是根據 ISO27006 作驗證天數的換算，目前與 NCC、TAF 達的共識是將所有驗證天數的三分之一加驗 ISO27011，但小數點後是否進位？也是驗證公司關心的重點。建議比照 ISO27006，針對驗證的範圍，訂定人天，驗證公司才會有遵循的標準，業者也不會遇到諮詢不同顧問公司得到不同答案的窘況	有關資通安全管理範圍區分為關鍵業務、支援業務及行政業務，附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)已詳列(pp2~4)，有關驗證人天，宜依據實際之驗證範圍估算
21	NCC 要求執行 ISO27011 驗證時，稽核員的資格應有通訊產業的背景，特別是首次執	感謝指導

項次.	座談會意見	處理情形
	行時，NCC 均會參與，應不致於發生顧問公司不瞭解相關作法的情況	
22	ISO27004，根據完整的架構，訂出適當的目標，因此不同類型的產業會訂出不同的目標，應不會發生強制用單一目標要求所有產業適用的情況	控制措施有效性量測，宜根據企業所採用之防護機制加以設計，本研究僅提供範例供個別企業參考自定
100/5/10 針對第二類電信業者召開之資通安全管理機制座談會專家及業者所提意見		
23	對服務業來說，信賴度最重要。推動制度時，人才流動最令企業頭痛，制度建立過程中，若沒有透過國際標準以第三者的角度、以標準程序加以驗證，球員兼裁判，無法客觀地評估此機制是確實可行的。附加價值則是同仁因建立制度而產生信心，也因建立此機制而趨向專業化，透過此機制也可檢視員工是不是都做了對的事	經由「風險意識文化建置過程」，以重新建構組織成員對於資安的意識，使組織成員擁有正確的資安認知與行為，並在執行營運業務時，將正確的認知與行為帶入工作情境當中，此觀點與本研究相符
24	資安人人有責，而不只是技術部門的責任。導入 ISO 就像為企業作體檢，知道自己的強處與弱點之後，面對挑戰時，會比較清楚因應之道。不是為 ISO 而 ISO，而是為了要合理化整個過程，跨國經營時，與其他國家仍能有共通語言。ISMS 做好，會有許多附加價值，例如參加政府標案、拿行銷科技獎，這些都是必要條件	經由「風險意識文化建置過程」，以重新建構組織成員對於資安的意識，使組織成員擁有正確的資安認知與行為，並在執行營運業務時，將正確的認知與行為帶入工作情境當中，此觀點與本研究相符
25	我們看這些國際標準就像許多官樣文章，但在實務上，尤其是風險管理，BS25999 反而比較好。它是由企業衝擊分析再到風險分析，原來的目的是要建立一套 BCP 的	已納入附件 4 通訊傳播事業資通安全管理手冊(修訂草案)之規劃架構中，詳見(二)資

項次.	座談會意見	處理情形
	關聯。從業務流程中分析，才會比較清楚問題出在哪裡	通安全等級評估 pp2~4
26	不管要不要通過認證，安全機制有它的好處，從安全防護的角度來看，不外乎三個階段：嚇阻、阻擋、拖延，有系統化的結構，至少在嚇阻上會發揮很大的作用，如果能取得證書當然更好。對於 attacker 來講，不會故意去挑很難侵入的公司，柿子挑軟的吃，若有相關系統、流程，控管機制已經存在，無論對內或對外，都能發揮嚇阻作用。阻擋則是指確實引入了哪些安全機制，不管多好的機制都有被破解的風險，所使用的機制能否拖延入侵，爭取到足夠的時間建立補救措施。以電信業來說，目前常用的都是 ISO27000 系列，重點放在資訊安全，並未在製造流程上著墨；BS25999 則跳脫了 IT 的範疇，由組織的角度來看營運持續。建議本研究案應適度呈現其他相關的電信標準，例如美國的電信機房建設標準等，會更完備	有關詳細之電信標準宜請參閱 NCC 編定之法規命令及行政規則,如建築物電信設備及空間設置使用管理規則等
27	資訊安全不要悶著頭做，可以尋求很多的外部資源協助。目的事業主管機關對下級單位的行政檢查權是很重要的作為，其依據就是資通安全管理作業要點與手冊，業者應該認真研究這些文件並有充分的瞭解，畢竟官方標準仍是最必要遵循的	感謝指導
28	實務上常見：通過 ISO27001 認證卻依然出現資安問題，進一步檢討後，發現發生問題的全都是在驗證範圍之外，表示驗證範圍的劃定大有問題，並未納入核心業務與作業流程	建議依據執照核發之營業項目範圍內,調查通訊傳播事業營運所需之資產群組,若組織規模龐大者,得區分為不同之事業體或是部門,區分為三大類,分

項次.	座談會意見	處理情形
		別進行資產群組之調查，詳見附件 4 通訊傳播事業資通安全管理手冊(修訂草案)之規劃架構中，詳見(二)資通安全等級評估 pp2~4
29	task force 一定要有相關部門參與，發生風險異常時能否承擔責任，如果不行，有告知主管的義務	感謝指導
30	民法、刑法中早就對個資保護有相關規定，只是大家都不習慣，個資法的通過對於企業主管來說是很大的危機，但若做得好，危機就可以轉化成商機	感謝指導
31	客戶帳務資料是目前因應個資保護最大的問題，以往曾將大量資料開放給經銷商運用，發生過系統被入侵、資料被竊取的資安事件，之後則進行實體切割，以杜絕類似事件。第二類電信事業必須快速因應環境的變化，個資法通過後，為維持企業的持續運作，需要建置一套更完整的機制	附件 4 通訊傳播事業資通安全管理手冊(修訂草案)已納入委託人應對受託人為適當之監督內容，詳見 pp6~7
32	總公司已通過 ISO27001，但台灣分公司並未納入，未來希望透過政策推動，訂出明確的施行細則讓業者有所遵循	轉請主管機關參考
33	台灣分公司雖有機房，但客戶資料都存在國外的總部，主要客戶為企業用戶，哪些資料屬於個資保護範疇？	可參考「電腦處理個人資料保護法」附件中有關個人資料「識別類」的說明
34	個資不准移往境外的規定，是所有資料都不可以，還是只有敏感資料？	個人資料的國際傳輸規定應由主管機關訂定
35	經銷商與 OEM 所使用的電腦設備各有其架構，如何納入加以規範	附件 4 通訊傳播事業資通安全管理手冊(修

項次.	座談會意見	處理情形
		訂草案)已納入委託人應對受託人為適當之監督內容,詳見 pp6~8
36	客戶個資保存在集團內部另一部門，委託機關與受委託機關的責任如何釐清	附件 4 通訊傳播事業資通安全管理手冊(修訂草案)已納入委託人應對受託人為適當之監督內容,詳見 pp6~8
37	多媒體複合平台，介接各家廠商，讓他們提供服務，在介接過程中，自然會有大量申辦證件個資在其中流通，目前雖有相關資安防範機制，但萬一發生個資外洩情況，如何舉證釐清責任歸屬？	附件 4 通訊傳播事業資通安全管理手冊(修訂草案)已納入委託人應對受託人為適當之監督內容,詳見 pp6~8
38	組織內的資訊部門，可引進外部資源，經由資安顧問的協助，與高階主管溝通，爭取支持	感謝指導
39	資訊應用不能悖離安全的原則，若沒有安全支持，就會喪失使用者的信賴。資安不能等到事件發生才做，也不需等到主管機關明文規定才做，目前已是很好的時機點，企業應開始投入這方面的工作。獲益的不會只有企業，個人也會有收穫，進而形成良好的企業文化	感謝指導
100/5/12 針對傳播業者召開之資通安全管理機制座談會專家及業者所提意見		
40	傳播事業規模落差很大，CIA 中著重的是可用性，特別是線路的穩定性與內容的傳遞，關乎其營運能否持續，目前都已做得非常好，本研究計畫的重點應在於如何透過有效性量測加以檢驗	控制措施有效性量測,宜根據企業所採用之防護機制加以設計,本研究僅提供範例供個別企業參考自定
41	目前的資通安全管理作業要點與手冊若要適用於傳播業，恐怕會遇上難以解讀的困境，建議修訂時應將電信業與傳播業分	依據通訊傳播基本法定義通訊傳播:指以有線、無線、衛星或其他

項次.	座談會意見	處理情形
	流，訂定適合其產業特性的參考指南	電子傳輸設施傳送聲音、影像、文字或數據者。本質上是相同的。差別在於對於通信秘密之保護。已修訂於附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 7、8
42	NCC 打算引進國際標準與目前業者的成果做比對，是很好的概念，若發現有不足處再予以補強	感謝指導
43	有關風險評鑑的作法，目前高階風險評鑑作法的六個構面，是很適當的，假如發生資安事件，會有多少的財務損失，主管對於這樣的議題通常會很重視，後勤支援單位對企業營運是否有效果？ISO27004 有效性量測很重要，藉由這方面的評估提醒主管資安的重要性，若沒做好，對於營運產生影響，會產生更大損失。本研究計畫建議應協助業者將業務的需求（主管的需求）轉化為資安的需求。量測目標值與結果的具體化，是後續要加強的地方	已納入附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)中
44	建議後續修訂資通安全管理作業要點與手冊時，能將 ISO27011 檢查表內容中相關名詞解釋增訂進來，讓名詞的定義能有一致性	附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 7、8，內容已與主管機關之承辦長官逐條修正
45	有關範圍的部分，大家談到通信傳播業的匯流與分流，目前電信業已有 ISO27011，傳播業又要再訂一個標準，MOD 被歸在電信業，可是又有傳播業的色彩，是否也要適用？第二類電信業者經營 VOD，被歸為電信業，是否也要適用傳播業的規定？傳	建議依據執照核發之營業項目範圍內，調查通訊傳播事業營運所需之資產群組，若組織規模龐大者，得區分為不同之事業體或是部

項次.	座談會意見	處理情形
	播業者取得電信執照的，要如何適用？執行稽核時是一家公司去 2 次？還是一次去看 2 份報告	門，區分為三大類，分別進行資產群組之調查，選定導入範圍
46	有關量測指標，建議適當融入 ISO27000 系列，ISO27011 從客戶服務等級協定(SLA)開始，NCC 訂出很多的定型化契約，規範業者與客戶之間的關係，以往 ISO27001 的框架並無法落實這部分的管理，納入 ISO27011 後可加強服務的落實	詳細內容請參閱附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 7、8
47	ISO27001 對於事件與事故有清楚的定義，對傳播業者來說，強調的是服務，可納入 ISO20000 系列對事件的定義，包括客戶來電詢問，都會影響服務的品質，都可包含在 ISO20000 系列的事故。資訊安全管理系統中納入與可用性(Availability) 有關的部分，對於傳播業者會比較有幫助，因產業的特性，較少發生與機密性有關的事故，反而常遇到與服務(可用性)相關的事故	感謝指導
49	如果不以取得 ISO 認證為前提，主管機關要如何評估業者執行導入的有效性？解讀標準、條文、作業程序、表單種種工作搞得人仰馬翻，最後卻沒有幾個人回答得出公司的機密資料是什麼，程序與證據的有效性要如何做判斷？即使都能回答清楚，是否就能論定其為有效？或者只要在驗證時看起來該具備的都有就發證書，只要不出事大家都沒事，如此是否值得投入這麼多的資源？如果能夠加上一些標準，即使不作認證，仍然能夠評估其有效性，也比較能夠說服主管，資安工作是值得長期投資的	適用於通訊傳播事業安全等級之控制措施項目，請參閱附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 6、7、8、9
50	ISO27000 系列比較高階、比較抽象，執行層面的東西建議參考 BS25999 的營運衝擊	已納入參考

項次.	座談會意見	處理情形
	分析，可以判斷出業務流程，風險評估也會比較準確，因此，營運持續管理才是傳播業真正重要的議題	
51	傳播事業的經營狀況正在改變，經營方式在數位時代是會改變的，數位電視全面普及之後，收視率的調查業者是否還會存在？答案當然是否定的，數位電視與顧客之間的互動密切，能夠直接掌握顧客行為時，就能主導廣告預算的分配。為了因應數位時代的來臨，傳播業者要儘快做出風險評估，才能有所因應	感謝指導
52	業者導入控管機制多半從執行面著眼，是為了讓工作更輕鬆，控管機制一定會有數據，呈現在主管眼前就是績效，而非真正考慮到制度面。平時主要配合會計師簽證、查核時的要求，若主管機關有要求，業者自然會調整腳步來配合	感謝指導
53	頻道代理商代理境外頻道，主要的客戶就是各有線電視台，擁有的個資數量很少，受到個資法的影響也很小	感謝指導
54	參加電視台活動的抽獎明信片包含民眾大量個資，大部分都由協力廠商負責處理，因個資法明文規定委託機關與受委託機關都有責任，因此與協力廠商的合約內容要求必須明確，應訂定處理的流程，包括如何銷毀，且委託機關也需做到相關查核，萬一有外洩情事，才能舉證無故意或無過失。對於個資的合理運用，資訊單位屬於行政後勤支援單位，沒有能力單獨處理，一定要由業務單位主導，甚至應加入法務單位共同討論，個資隱私長應由業務單位擔任，IT 單位建議只擔任資訊安全長	感謝指導

項次.	座談會意見	處理情形
55	IT 部門在公司的位階較低，只是系統的維運單位，在內部無主導權，提出資安相關預算時，很難向主管說明會對公司的營運有何影響、不做會造成什麼損失，既然會減少營收，對主管的經營績效又沒有直接助益，除非高階主管有 IT 背景，否則多半不會支持	感謝指導
56	由營運持續的觀點來看，傳播業反而做得更好，目前 NCC 雖然是由資安的角度切入，但資安不應只限縮在資訊系統，更不是只有機密資料，可用性涵蓋在資安範圍內，如何協助主管重視，並取得足夠的資源，彰顯資訊單位的績效，是當務之急	感謝指導
100/8/12 針對第一類電信業者召開之資通安全管理機制座談會專家及業者所提意見		
57	安全管理手冊中有關通報的部分提到「事件」一詞，行政院國家資通安全會報已將「事件」改為「事故」	已更正
58	三個影響構面，「資料保護受到損害」、「影響業務運作」及「法規遵循」，附件 1 與附件 2 出現的是「違反法規遵循」，兩者是不是同一件事	已更正
59	簡報 p.21 有關結構方程模式修正，在規劃階段「法規遵循」的部分是 0.74，但在維持階段的「法律影響」落到 0.67，兩者的關聯性為何	代表法規遵循在不同階段影響程度之差異
60	簡報 p.69 定義安全等級分為 A 級與 B 級，由行政院國家資通安全會報的角度來看，機關應分為 A、B、C、D 四級，通訊傳播事業分為 A、B 兩級，會不會產生混淆的現象	已修訂資產安全等級為普、中、高三級，與行政院之規定一致，另彙整企業安全等級為 ABC 三級，適用於不同之防護基準

項次.	座談會意見	處理情形
61	本研究最主要的目的主要是導出管理要點要做的部分，但兩者的聯結看起來是薄弱的。資通訊從業廠商的資安認知水平到何程度，需要如何加強，這是一種研究方式。如果廠商要導入 ISMS，有哪些重要因素需要被找出來。資訊安全文化建構來自於資安治理，有強烈的連帶關係。步驟的實施過程，談得比較少。國家資通安全發展方案中並未將資安治理的評估表清楚的揭露，但希望從成熟度的角度去看組織資安治理的成熟度，再去推動資訊安全的行動方案。這兩部分我是建議可以再做一些思考。如果從這個角度來看，資訊與資訊系統分類分級，以及 ISMS 所要訴求的，在某種層次上是不一樣的。或許看起來管理要點是著重在 ISMS，所以會有從部門別、系統別、業務別的角度去切入，可是最後連帶的，不管用何種分類方式，最後還是要定義出組織內的資訊與資訊系統的分級。建議步驟的部分，不管用何種範圍定義別去導入，都不可忽略資訊與資訊系統分類分級以及資訊治理兩部分	已納入資通安全等級評估方法。詳見附件 4 通訊傳播事業資通安全管理手冊(修訂草案)pp2~4
62	目前有幾家業者已申請 ISO27011 稽核的驗證服務，年底會陸續完成。管理作業要點修正條文對照表 p.3 第 5 條提到：「通訊傳播事業申請『開放赴大陸投資業務項目』前，應將其資通安全管理之實施作業範圍報經 NCC 核准後，就核准之作業範圍申請驗證。」要提醒業者的是：在申請範圍前，以往在申請 ISO27011 時，申請方與驗證方就 ISO27006 與 ISO27011 相關的規定要求去作範圍的制定，這部分會有主管機關的意見要表達，主管機關會希望期程之內，	感謝指導

項次.	座談會意見	處理情形
	資源上或技術上沒有困難的情況下，逐步 scope expand 的計畫，會裡面會要求要包含到個資、核心業務等等	
63	簡報內有建議：針對 A 級組織，未來在進行 ISMS 建置或設計時，考慮採用 BCM 裡面的專業作業 BIA(營運衝擊分析)。目前在增項稽核查檢表裡面並未針對 BIA 細部要求查檢的項目，未來這部分若列在 A 級的建議要求之內，增項稽核查檢表裡面對應的控制措施也要發展出來，提供申請單位或驗證單位作參考	BIA(營運衝擊分析)之概念已融入於資通安全等級評估方法中，增項稽核查檢表僅針對通訊傳播事業分別訂定適用之控制措施
64	目前分為 A、B 級，手冊上的規定，A 級沒問題，基本上都會通過驗證，B 級自行導入會有困難，也不太可能申請驗證。以我接觸的經驗，尤其第二類電信，單位規模大概都在 50 人以下，甚至 20 人以下。在這種情況下，手冊上的定義是 B 級單位也要做內部稽核，查檢表是否同時有是否符合與不適用三種選項，NCC 是否可以同意其自行勾選不適用？假如不是的話，在執行上，對 B 級單位還是會有蠻大的困難。因為有很多項目，B 級單位不是沒有就是做不到。設計一個表讓業者自行勾選，這個表的意義不大。若是回到主計處的內部查檢表的話，是不能選擇「不適用」的，要嘛就是做得很好，要嘛就是做得不盡完善，可是並沒有「不適用」的選項。所以，是不是可以考慮在執行上，被歸到 B 級的單位，在能力上已無法自行建立 ISMS 體系，在你們的幫助之下，能夠有一個合適的查檢表，他們就做這些事就好，差別只是做得完善或不盡完善	企業安全等級已修訂為 ABC 三級，分別適用不同之防護基準，詳見附件 4 通訊傳播事業資通安全管理手冊(修訂草案)p4~6

項次.	座談會意見	處理情形
65	業界選擇認證時的有效性可以將資訊安全的精神落實在組織內部，如何將 NCC 的要求對應到各個業務單位能將業務鑑別出來，最後能落實到核心業務，將其分為 A、B 級。選擇認證範圍時，其核心業務是否有效，查檢表不一定鑑別得出來，NCC 站在主管機關的角度上，應有一些方式與能力判別每一個不同的業者各有其不同的核心業務，對應後續送審的驗證範圍可以有個跟核心業務的關聯	企業安全等級已修訂為 ABC 三級，分別適用不同之防護基準，詳見附件 4 通訊傳播事業資通安全管理手冊(修訂草案)pp4~6
66	基於輔導、指導的角色，中華電信非常感謝，簡報 p.79 提到行政檢查，以中華電信的意見，資安認知很重要，但資安文化或資安治理過程很長，希望 NCC 長官能讓業者有較多時間聚焦在核心業務或個資保護上，比較有多餘的力氣來做這些事，行政檢查的部分建議先刪除	轉請主管機關參考
67	p.47~48，管理要點第四點：「本會執行電信事業資通安全管理，認有必要時，得向電信事業索取文書、資料或物品，甚至設備」，業者覺得較困擾，除了企業本身，有時會牽涉到第三者，這點是業者比較關切的	轉請主管機關參考
68	p.49 有關客服中心的議題，審查原則第三點提到：「均限制不得移往大陸設置營運或於當地投資、合作」，政府希望業者走出去，但這樣的要求與政府的政策不是那麼一致。事實上可以要求業者將客戶資料存放在台灣，客服中心營運的地點則不一定要在台灣。國外客服最多的大概是印度，菲律賓這幾年也搶了不少生意，美國人更重視個資，但即使經過 911 事件，美國也沒有限制業者外移	轉請主管機關參考，列為通訊傳播事業個人資料管理辦法之國際傳輸規定之參考

項次.	座談會意見	處理情形
69	簡報 p.71 提到：資通設備安全審驗作業要點基礎型設備或進階型設備的要求，電信業者設備多向國外採購，基於支持國內產業的立場，中華電信也願意配合，相關的辦法是否能清楚說明，讓業者有所遵循	資通設備安全審驗作業要點目前著重於資訊處理設施,並未涵蓋電信設備,詳細內容請參閱「資通設備安全審驗作業要點（草案）」
70	p.72 資通安全等級為 A 級者，鼓勵通過 ISMS 第三方驗證，這部分是否呼應 p.68，是以核心業務或個資為主，還是全業務都包含？是否能再說明清楚	資通安全等級評定為「高」級者,除實施前述「資通安全管理內部稽核表」之全部控制措施外,另依據產業別,實施適用之「通訊事業增項稽核表」或「傳播事業增項稽核表」,並以通過資訊安全管理系統第三方驗證為目標,逐年改善最終及於全企業，詳見附件 4 通訊傳播事業資通安全管理手冊(修訂草案)pp4~6
71	涉及法規解釋與政府政策的部分，本研究案不宜提出建議。管理要點草案條文對照表第 5 條第 2 項：「涉及國人個人資料之事項或業務部門、業務功能及系統等，例如電信業者之用戶資料庫、客服系統／客服中心、帳務系統／帳務中心等，均限制不得移往大陸設置營運或於當地投資、合作。」這部分其實是經濟部投審會的審查原則，隨時會因為時空環境而變動，放在要點裡面，後續若不合時宜，還需要修正，建議不應放入第 5 條	感謝指導

項次.	座談會意見	處理情形
72	有關法律的強制性，赴大陸投資需通過 ISO27011 的增項驗證條款，現階段針對附件 6 增項稽核表內容的妥適性，NCC 應積極主動提出詳細說明與完善的解釋，讓業者在申請驗證時，有遵循的方向	有關增項稽核表之內容已加以修訂,詳細內容請參閱附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 7、8
100/8/12 針對第二類電信業者召開之資通安全管理機制座談會專家及業者所提意見		
73	管理手冊修正草案 p.3(5)設計 ISMS。編號誤植，應該是(6)	已更正
74	管理手冊修正草案 p.6，通訊傳播事業只要經過外部稽核單位驗證通過 ISO27001，即可免除交付證明文件，立意即在鼓勵業者通過公正第三方的稽核。但其實要求業者提供的資料還是蠻多的，依本管理手冊規定仍需提交附件七、附件八等文件，建議簡化相關程序，直接以驗證報告替代，增加業者接受外部稽核之誘因，並可同時減少 NCC 在行政檢查上的負擔	納入規劃參考
75	附件八資通安全管理矯正／預防措施單之設計，應考量發生 3、4 級資安事故時需填入的欄位。例如：「檢查項目內容」似乎僅針對內外稽檢查出的項目，另外缺少矯正預防單負責單位、承辦人員欄位，亦缺少覆核欄位	已更正,詳細內容請參閱附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 10~14
76	建議可參考支付卡行業資料安全標準(PCI DSS)，適度加入要求較明確的管控項目	感謝指導
77	管理手冊修正草案 p.2，評估資訊安全等級提到三項評估準則，包括「資料保護受到損害」、「影響業務運作」及「法規遵循」等三個構面，「資料保護受到損害」這個構面描述的不是很清楚，是資料的機密性、完整性及可用性受到損害？還是資料保護	納入修訂參考

項次.	座談會意見	處理情形
	機制失效？建議應修正為「資料保護失效時造成損失」	
78	管理手冊修正草案 p.3，教育訓練包含「設計 ISMS」，後面實施、檢查沒有列出來，感覺就缺了什麼。教育訓練的內容，通常會針對不同職位的人員設計不同課程，可能要定義不同職位的人員要受什麼樣的資通安全訓練。如果沒辦法寫得很具體，建議只要寫執行教育訓練就好	納入修訂參考
79	管理手冊修正草案 p.3 提到「防護縱深」，A 級、B 級各列出一些需符合的項目，這些項目的妥適性到什麼程度，可以再作討論。ISMS 為人所詬病的就是沒有縱深，如果要談縱深，建議像美國 NIST SP800-60，把認證方式分類，再要求不同等級的單位應做到什麼樣的等級。但差異在哪裡，建議要清楚說明	納入修訂參考
80	管理手冊修正草案 p.4 推動方式，要推動 ISMS 第三方驗證，這是好事，但重點是範圍，例如僅是機房的維運，或是整個單位	感謝指導
81	附件 1-2 資料保護受到損害部分，後面的說明和前面的標題沒有對應到	已更正
82	增項稽核表建議要對應到前面的內部稽核表項目	詳見期末報告附件 6~9 通訊傳播事業安全控制措施修訂對照表
83	管理手冊修正草案 p.1，「基於保障資通安全及維護使用者權益原則，確保通訊傳播事業『資料』、系統、設備及網路安全..... 」，建議更改為『資訊』	依據電信法第 56 條增修條文內容，不予修訂
84	管理手冊修正草案 p.2，「需將通訊傳播事業之核心業務及支援個人資料蒐集、處理及利用之特定目的範圍內之所有資產納	已更正，詳細內容請參閱附件 4 通訊傳播事業資通安全管理作業

項次.	座談會意見	處理情形
	入...」，建議拿掉「特定目的範圍內」，即使超出特定目的範圍內，只要蒐集、處理及利用，還是必須被盤點進來。單純的蒐集、處理及利用，涵蓋面比較廣，且大部分的人也很難分辨是否在特定目的範圍內	手冊(修訂草案)p3
85	管理手冊修正草案 p.2 第(3)點，針對每個定義別依「資料保護受到損害」、「影響業務運作」及「法規遵循」之影響構面，分別評定影響構面之安全等級屬 A 級或 B 級，以確認「資訊安全需求」，建議改為「資訊通訊安全需求」或「資通安全的需求」	已更正，詳細內容請參閱附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)p3
86	管理手冊修正草案 p.3，「並定期進行內部稽核或外部驗證」，內稽每年被要求進行，此處的「或」易造成誤解。(p.4 資通安全等級為 A 級或 B 級者，稽核方式均為每年至少執行一次內部稽核。)	已更正，詳細內容請參閱附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)pp7~8(七)資通安全實施評鑑
87	管理手冊修正草案 p.3，「獲得管理階層的承諾，啟動 ISMS 專案」，此處之 ISMS 縮寫是第一次出現，於文件內並未定義且未有中文說明，且整本管理手冊談的都是資通安全，ISMS 為資訊安全管理系統與本手冊資通安全管理系統亦有差距	已更正
88	管理手冊修正草案 p.3，(5)選擇控制措施，其內容應包括下列項目: (A)資訊安全政策訂定。建議刪去「訂定」兩個字，因為該單元包括訂定與定期審查，原 CNS 27001 並無「訂定」兩個字。(F)通信與作業管理。建議修訂為「通訊」與作業管理(CNS 27001 原文)。	已更正
89	管理手冊修正草案 p.4，B 級單位可能包括無資料庫者，要求資料庫稽核設備可能過於嚴格，垃圾郵件對於 B 級或較小單位的	已更正

項次.	座談會意見	處理情形
	防禦意義不大	
90	管理手冊修正草案 p.4，通訊傳播事業應建立資通安全「事件」應變作業機制，p.3(I)資安「事故」管理，建議統一名詞	已全數更正為「事故」
91	管理手冊修正草案 p.4，資通安全等級為 A 級者，其「資訊」人員、業務人員及一般人員，每年至少須分別達到 12、6、3 小時之資通安全教育訓練。建議更改為「資通訊」人員。B 級亦同	已更正
92	管理手冊修正草案 p.4，「....計畫，並依據法定期限之要求，保存適當之「資訊」活動記錄。」建議修改為「資訊通訊」活動紀錄	已依據個資法施行細則，修訂為：採行適當安全維護措施，並保存適當之個人資料蒐集、處理及利用之活動稽核記錄，證明已盡管理之責任，詳細內容請參閱附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)pp6~7(五)個人資料保護
93	管理手冊修正草案 p.6，(3)附件五至附件十、各檢查項目之佐證資料、或經「本會認可」之資通安全管理機制驗證機構產出之稽核報告。本會認可驗證機構須被定義，是否同於 p.5 之「前項驗證機構須經『本會認可』之本國認證體系認證」	維持原內容
94	附錄 1-2，「系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關違反法律規定，遭致損害賠償或是『刑事處分』，並導致嚴重不良後果。」上面違反的是法律，下面違反的是法規命	已參照行政院國家資通安全會報之規定，修訂為系統運作、資料保護、資訊資產使用等，若未依循相關規範辦

項次.	座談會意見	處理情形
	令，此處會產生混淆之處，施行細則算法律還是法規？會不會造成損害賠償，此處區隔A、B級方式為刑事或行政處分，但刑事處罰的是行為人，行政罰處罰的是行政單位或自然人，以此區分似有不妥。因為B級的違反很可能還是會伴隨著刑事處罰	理，將導致機關從根本上違反法律，並導致嚴重不良後果，如：損害賠償、罰金或是刑責。詳細內容請參閱附件4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄1
95	附錄3-1，每年辦理社交工程演練及檢測企業網站安全弱點乙次。弱點掃描的部分建議為企業網路環境，僅檢查網站範圍太小	內容已依據主管機關意見刪除
96	附錄4-1，3.資通安全事件資料： 影響等級：『4』級：影響公共安全、社會秩序、人民生命財產 『3』級：業務無法運作，系統停頓 『2』級：系統效率降低，業務中斷 『1』級：業務短暫停頓，可立即修復 98年2月會報的通報辦法已修正，判定影響定級不會僅從營運中斷考量，建議此處的影響等級需考慮CIA三個構面，資料洩漏與完整性破壞都需要通報	已依據行政院國家資通安全會報規定修正，詳細內容請參閱附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄10
97	手冊中多處提到「安全等級」，為避免混淆，建議提到「資通安全等級」時，均以全稱表示	已更正
98	ISO27011增項稽核表實際稽核時問題非常多，至少30個以上，建議應另案討論	增項稽核表已與主管機關逐條討論，詳細內容請參閱附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄7、8
99	管理手冊修正草案 p.1，建議參照下列ISO/IEC 27000系列國際標準或國家標準之對應標準，惟所列6項標準均有CNS國家	國家標準已頒布者，會加以註記

項次.	座談會意見	處理情形
	標準，是否考量增列	
100	有 CNS 國家標準者，應以國家標準之中文翻譯為準；例如：p.1 第 1 項依 CNS27001 應為「資訊技術－安全技術－資訊安全管理系統－要求事項」，而非「資訊安全管理系統要求事項」；第 2 項依 CNS27002 應為「資訊技術－安全技術－資訊安全管理之作業規範」；第 3 項依 CNS27003 應為「資訊技術－安全技術－資訊安全管理系統實作指引」;第 4 項依 CNS27004 應為「資訊技術－安全技術－資訊安全管理－量測」；第 5 項依 CNS27005 應為「資訊技術－安全技術－資訊安全風險管理」；第 6 項依 CNS27011 應為「資訊技術－安全技術－資訊安全管理系統－植基於 CNS 27002 之電信組織資訊安全管理指導綱要」	維持原表示方法
101	管理手冊修正草案 p.2 出現「法規遵循」，附件 1-1 為「法律遵循」，附件 1-2 為「違反法規遵循」，其實講的是影響構面，是否考量其一致性	已更正
102	管理手冊修正草案 p.3，(5)選擇控制措施時，如何依資通安全等級選擇適切控制措施是有難度的，可考量讓此管理手冊與研考會所頒「安全控制措施參考指引」有相當程度上的連結。例如：若資通安全等級為 B 級者，選擇安全控制措施參考指引等級「普」之控制措施，若資通安全等級為 A 級者，選擇安全控制措施參考指引等級「中」或「高」之控制措施	已更正,詳細內容請參閱附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)之推動方式 pp5~6
103	管理手冊修正草案 p.3 之(1)防護縱深第 1 項 A 級同時有 IDS 與 IPS,因 IPS 已含 IDS 功能，且 IDS 為過時產品，有必要兩者都	依據「資通設備安全審驗作業要點（草案）」之項目訂定

項次.	座談會意見	處理情形
	寫嗎？A 級是否只須放 IPS 即可	
104	管理手冊修正草案 p.4 之(1)防護縱深第 2 項 B 級有入侵防禦系統，但附錄 3-1 並未列入，兩者不吻合	已更正
105	管理手冊修正草案 p.4 之(4)資安教育訓練時數要求，未要求主管應參加教育訓練，高階主管的支持是非常重要的，應考慮要求主管接受教育訓練	已修訂,詳細內容請參閱附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 5
106	附錄 1-2 有關以「業務別定義」與「以部門別定義」似乎重疊類似，均以業務為出發點；有關「以部門別定義」的描述應考量予以修正	已修訂為關鍵業務、支援業務及行政業務別
107	附錄 3 備註描述的社交工程與網站安全弱點檢測，管理手冊內文並未描述此項，建議在 p.4 考量加入(5)說明社交工程與網站安全弱點檢測	已依據主管機關意見刪除
108	附錄 8-1 缺少「稽核員」與「受稽者」簽名欄位，不利後續追蹤；亦可考量加入「稽核領隊」與「受稽者主管」簽名欄位	已更正,詳細內容請參閱附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 10~14
109	附錄 5 與附錄 6 均有檢查項目 1-1 與 1-2，填寫附錄 7 的檢查項目編號欄位時，如何分辨為附錄 5 或附錄 6 之檢查項目？是否考量於附錄 7 第一列加入填寫範例，備註欄位註明範例，提供填寫者參考	已更正,詳細內容請參閱附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 10~14
110	管理手冊修正草案 p.3，防護縱深的部分提到資通安全等級為 A、B 級者，應分別建置防火牆…等。電信業者提供的服務通常都是網路存取服務，若有額外服務都是視客戶的需求，設備或軟體的保護標的是指第二類電信本身內部的系統？還是提供給外	防護縱深著重於資訊處理設施,詳細內容請參閱附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 5

項次.	座談會意見	處理情形
	部的服務？這部分似乎沒有明確的定義	
111	管理手冊修正草案 p.4，推動方式的部分，A、B 級核心業務是由業者自行評定嗎？屆時會有單位負責審查所訂等級是否符合實際狀況嗎？p.6 第 2 點，如果有第三方驗證機構認可通過 ISO27001，即可免提報相關資料。是要 NCC 業管範圍內通過認證才可以免除？還是只要某個小範圍資訊系統通過即可？希望也能明確說明	由企業依據執照核發之營業項目範圍內，調查通訊傳播事業營運所需之資產群組，若組織規模龐大者，得區分為不同之事業體或是部門，區分為關鍵、支援及行政三大類，分別進行資產群組之調查，選定導入範圍
112	商業司針對無店面零售業者推動 DP-mark 的管理制度，未來業者若通過相關管理制度，是否即可符合 NCC 管理辦法的要求？是否考慮統一來推行	個資法對於目的事業之管轄授權給目的事業主管機關，故商業司之規定，並不適用於通訊傳播事業
113	有關驗證範圍，手冊中並未提到內稽的範圍有多大，若企業未通過外稽，必須要通過全公司的內稽；若已通過部分範圍的外稽，例如資訊機房，只需要做資訊機房的內稽。這是管理手冊裡的漏洞，總之，還是鼓勵大家通過外稽	由企業依據執照核發之營業項目範圍內，調查通訊傳播事業營運所需之資產群組，若組織規模龐大者，得區分為不同之事業體或是部門，區分為關鍵、支援及行政三大類，分別進行資產群組之調查，選定導入範圍
100/8/15 針對傳播業者召開之資通安全管理機制座談會專家及業者所提意見		
114	資安問題是國安層級的問題，不只是企業營運面或一般用戶權益保障的問題。政府持續運作案的推動，主要內容分為幾部分，包括關鍵基礎設施防護、政府核心業	感謝指導

項次.	座談會意見	處理情形
	務的持續運作、首長人身安全的保障維護及危機的處理等。這幾項元素中，幾乎超過一半，或多或少都與資訊安全有關。因為資訊就是政府持續運作的神經中樞，如果資安沒辦法確保，不要談什麼政府持續運作，更不要談關鍵基礎設施是否能受到保護。因為有政府持續運作案的推動，發現資安問題有必要拉高到國安會層級來處理。也因為如此，才會開始用國家安全的角度來看待資安議題	
115	從國安的角度來看資安議題，會考慮到實體安全的部分，倘若遇到天災人禍，普通的保全人力根本無法維持重要設施的實體安全，目前列管清單上的關鍵基礎設施都與軍警簽有聯合支援協定，一旦有事，設施的安全將由軍警接管。除此之外，是否也有其他未列入的重要設施，其防護等級也必須提高。廣播電台與電視業者在危機時刻都扮演重要角色，有必要提高實體安全的防護等級	感謝指導
116	要求民間業者建置備用系統，似乎是浪費投資的事，但是假設主要系統在危機時已無法使用，備用系統確有必要。因此，備用系統的建置應列入資通安全實體防護面的議題加以考量	感謝指導
117	遇到災難時，政府可能需要民間通訊傳播業者的支援，例如遇到地震或水災等緊急狀況時，負責救災的官員需要有優先通訊權，需要有通盤的考量與相關規定	依據電信法第 25 條 電信事業對下列通信應予優先處理： 一、於發生天災、事變或其他緊急情況或有發生之虞時，為預防災害、進行救助或維持秩序之通信

項次.	座談會意見	處理情形
		二、對於陸、海、空各種交通工具之遇險求救及飛航氣象等交通安全之緊急通信 三、為維護國家安全或公共利益，有緊急進行必要之其他通信
118	實體安全、備用系統及變時支援三項議題，需要有更明確的規範，讓業者有所遵循	轉請主管機關參考
119	核心系統是由業者的觀點來看，還是主管機關的觀點？目前電信業者通過認證的大多是帳務系統，但這是主管機關關注的重點嗎？主管機關是否重視業者在維運過程中的資訊？尤其是傳播業，這些資訊真的會影響到業務的持續運作嗎？真正會影響到業務持續運作的可能是設備的實體安全，有些資安事件發生的時候，資訊的漏失並不是主管機關想要控管的重點	由企業依據執照核發之營業項目範圍內，調查通訊傳播事業營運所需之資產群組，若組織規模龐大者，得區分為不同之事業體或是部門，區分為關鍵、支援及行政三大類，分別進行資產群組之調查，選定導入範圍
120	個案訪談後找到 22 項關鍵的控管措施，大部分與資訊安全有關，是否真正是傳播業想要做或能夠做的，做了之後是否真的對於提升資通安全的保護水平有幫助？我個人的看法是幫助並不會太大。這時就會產生困擾，到底主管機關在管理資通安全業者的時候，希望他們能做到什麼樣的水準？主管機關的期許為何？這就回到當初的目標，若是從關鍵設施的角度來看，以德國的經驗來看，大部分都不是由業者來做，而是由政府(資訊安全局)來做，政府在第一時間已經做出評比，列出重要設施清單，動用國安資源進行保護，甚至業者也	有關關鍵基礎建設之保護，建議依據行政院國土安全辦公室之相關研究或規定辦理

項次.	座談會意見	處理情形
	不能隨意啟動這些機制。這部分是有一個關鍵基礎設施的專責小組負責。這部分業者能做的並不多，大部分是由政府來執行	
121	若要將這些安控措施都訂進來，以 NCC 的管轄範圍，通訊業與傳播業在本質上就有差異，運用同一套資訊安全管理規範，是否能達到當初 NCC 期望的目的，這部分建議再思考	依據通訊傳播基本法定義通訊傳播:指以有線、無線、衛星或其他電子傳輸設施傳送聲音、影像、文字或數據者。本質上是相同的。差別在於對於通信秘密之保護。已修訂於附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 7、8
122	主管機關在進行資通安全的確保時，要同時考量關鍵基礎設施的保護與業界的資通安全水準提升。關鍵基礎設施的保護既有國際標準，也有國際慣例，主管機關要做並不困難。一旦主管機關發動了，鑑別出業者的設施屬於關鍵基礎設施後，要對業者提供什麼樣的資源？業者為了營運的需求，投資了這些設備，為了國安層級的需求，就要業者如何如何，對業者來說根本不可能做到。所以，政府必須要有配套的措施。若不屬於關鍵基礎設施，則適用一般的資通安全規範，政府制定的角度是從維持社會穩定、民生秩序，這就不是國安層級的問題，就是一般的業者都要做到的，如果沒做好，民眾沒有得到適當的服務，會向主管機關抗議，主管機關就會產生壓力，所以主管機關必須對業者有所要求	有關關鍵基礎建設之保護,建議依據行政院國土安全辦公室之相關研究或規定辦理

項次.	座談會意見	處理情形
123	政府組織再造，會產生新的資通安全權責單位，這是一個很好的時機，對 NCC 來說，只要多出一分力量，就可以把這些不同的單位連結起來，可以把這些事情做得更完美	感謝指導
124	未必要修改電信法才能對業者有所要求，舉例來說，金融單位的資安問題也層出不窮，主管機關只要公布某某銀行發生資安問題，業者自然會產生壓力去進行改善。今天我們討論的是一個認證的過程，認證過程所需的要件滿足了，就發給認證，在這些要件裡面，就可以把剛才考慮到的那些事情放進要件裡面，這部分是主管機關可以做的	感謝指導
125	通訊業與傳播業的本質有所差異，當時之所以要保護通訊事業的資通安全，主要是因為其擁有大量的民眾個資與通聯紀錄等。另外也包含了通訊系統的可用性，所以我們對他們的要求都有一些相關的要件，比如說可能參照了一些國際標準，還有最近新增的到大陸投資需通過 ISO27011 的要求。仔細去看 ISO27011 的要求，原則上還是立基於前述的兩點，首先要確保通聯紀錄只有被授權的人才能存取，其次是如果通訊事業發生任何中斷的情況，業者必須在一定時間內回復到正常可用狀態。這些都是針對通訊事業所作的一些基本的要求。可是反過來看，就傳播事業來講，是不是跟通訊事業有同樣的需求存在？在看作業要點與管理手冊時，尤其是管理手冊，其實都有提到內稽的部分，要求通訊傳播事業每年要去檢視評估的計畫等級，要填寫 ISO27011 的增項稽核表，某種程度	依據通訊傳播基本法定義通訊傳播:指以有線、無線、衛星或其他電子傳輸設施傳送聲音、影像、文字或數據者。本質上是相同的。差別在於對於通信秘密之保護。已修訂於附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 7、8

項次.	座談會意見	處理情形
	對傳播業者來說，個資數量與可用性都不是那麼的高，但若要求通訊傳播業者都要拉成同一個水平，其實某些業務並沒有那麼重要，業者可能會覺得不是那麼必要，對一般民眾來說，也不是那麼必要。在這麼多業務當中，找出關鍵業務是需要被保護的，對傳播業者來說，也許只有 10%，剩下的 90%是否也要遵循與通訊一樣嚴格的標準？第一、第二類電信業者在導入 ISMS 時都會遇到一些困難，更何況是傳播業者，要投入的人力成本與資源投入都是難以控制的	
126	資通安全管理作業要點修正，初期鎖定的目標是通訊業，引用的標準是 ISO27011，修正之後變成作業要點實施，成為後續驗證的需要。目前預計分為 A、B 兩級，A 級鼓勵通過第三方驗證。要點修正條文對照表 p.3 第 5 條，「電信事業申請赴大陸地區投資，應於系統審驗前，向本會認可之資通安全管理機制驗證機構，就核准之作業範圍申請驗證，並取得驗證合格證明。」，這一點是很多業者關切的。比較可惜的是當初在研擬相關作業要點與增項稽核表時，是引用 ISO27011，核心業務的定義都是以電信業者的角度來思考，所以第 5 條提到客戶個資的資料庫、客服系統、帳務系統都會偏向電信業者。所以很多業者都會擔心核心業務要如何認定，要點中的敘述好像跟實際的業務有所差距，範圍如何界定？其實是要報 NCC 審核的，所以要點第 5 條「資通安全管理之實施作業範圍報經本會核准後」，才能實施後續的認驗證。資訊安全管理系統傾向要有內部機制去評	由企業依據執照核發之營業項目範圍內，調查通訊傳播事業營運所需之資產群組，若組織規模龐大者，得區分為不同之事業體或是部門，區分為關鍵、支援及行政三大類，分別進行資產群組之調查，選定導入範圍

項次.	座談會意見	處理情形
	量出所謂的核心業務，但依目前的作業辦法，是要由 NCC 來加以認定。未來業者如果有需要，特別是針對認證範圍要做個釐清。未來如何將個資保護的議題融入 ISMS，也是業者需要思考的	
127	管理手冊 p.4，倒數第二段，「資通安全管理實施計畫範圍內，若涉及個人資料保護者，應依據『通訊傳播事業個人資料管理辦法』之規定，訂定個人資料檔案安全維護計畫，並依據法定期限之要求，保存適當之資訊活動記錄。」是否強調實施範圍需涵蓋個人資料保護？與範圍內涉及個人資料保護，強度是不同的。目前業者選擇 ISO27001 的認證範圍多偏向機房管理，因業者覺得機房是公司內部目前較能掌握的部分。個資法施行細則雖尚未公布，後續仍是需考量的重點	已修訂，詳細內容請參閱附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)(五)個人資料保護 pp6~7
128	管理手冊 p.6，ISO 27011 相關條款較適用第一類電信業者，有時候連第二類電信都不見得適用，更何況現在連傳播業者都要適用，在增項稽核表的填寫時，應該要多作考量，哪些部分是可以預先刪除掉的，也可以事先考量，畢竟 ISO 27011 是針對第一類電信的整個範圍，如果範圍還未涵蓋到所有基礎設施，而只涵蓋到部分機房時，也不見得完全適用	依據通訊傳播基本法定義通訊傳播：指以有線、無線、衛星或其他電子傳輸設施傳送聲音、影像、文字或數據者。本質上是相同的。差別在於對於通信秘密之保護及機線設施之多寡。已修訂於附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 7、8
129	簡報 p.63，ISO27005 已於 2011 年改版，建議改採 2011 年版	ISO/IEC 27005：2011 之內容，僅名詞定義修正，主要架構並未修正，故維持原內容

項次.	座談會意見	處理情形
130	以國際標準來說，通常要求的是大原則，主管機關在訂定相關的規範時，若有不同的要求，應訂定相關量測的指標，ISO27001是有提到一些量測的項目，但並未針對特定的行業，如果我們對通訊業者有特定的要求，應提供量測的數據，若未量測，很難有效具體改善	ISO/IEC 27004 提供發展與使用安全控制措施與測量方法之指引，用以評估 ISMS 實施 ISO/IEC 27001 所描述控制措施之有效性，包含政策、資訊風險管理、控制目標、流程及程序等之評估，協助鑑別哪些控制措施需要改變或是強化，但同時也特別強調沒有一種安全控制措施之測量方法，可以完全保證安全
131	傳播業者多為單向傳播，傳送的只有節目內容，與資訊的關聯性不高，擁有民眾的個人資料並不多，資安方面可能只有有線電視業者會較相關	由企業依據執照核發之營業項目範圍內，調查通訊傳播事業營運所需之資產群組，若組織規模龐大者，得區分為不同之事業體或是部門，區分為關鍵、支援及行政三大類，分別進行資產群組之調查，選定導入範圍
132	雖然是同一個主管機關 NCC，傳播業者與電信業者本質上就有差別。即使是辦活動，也多是委外，並未擁有大量民眾個資，但管理手冊裡的相關規定這麼多，傳播業者擔心不能做到管理手冊所要求的各項要求。且管理手冊只是將原來的「電信事業」改為「通訊傳播事業」，細則並沒有修改，很擔心實施上會不會有困難，應考慮產業	依據通訊傳播基本法定義通訊傳播：指以有線、無線、衛星或其他電子傳輸設施傳送聲音、影像、文字或數據者。本質上是相同的。差別在於對於通信秘密之保護及機線設施

項次.	座談會意見	處理情形
	別的差異，可能需要再與 NCC 溝通	之多寡。已修訂於附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 7、8
133	目前公司內部推動資安，主要是針對員工個人與對外的網站，除此之外，設備邁向數位化，採購防火牆、加強縱深等等這些是有的，但傳播業這一塊與電信業的落差還是蠻大的，這種情況下，電視公司只能就內部已有的規劃持續去做，管理手冊裡面規範的這麼多，但並不是業者會遇到的問題，業者會有不知從何著手的困擾	依據通訊傳播基本法定義通訊傳播:指以有線、無線、衛星或其他電子傳輸設施傳送聲音、影像、文字或數據者。本質上是相同的。差別在於對於通信秘密之保護及機線設施之多寡。已修訂於附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 7、8
134	光是內部稽核表就令業者相當頭痛，不知如何做到全面稽核。業者雖然擁有數位設備與少量的民眾個資，但其營運管理非常的單純，若管理手冊要實施，光為了應付內部稽核，可能就不是企業的 IT 部門應付得了的事情。我們也贊同資通安全是非常重要的事，但請 NCC 也要考量業者營運上的困難。是否有什麼樣的模式可以協助傳播事業做好營運事業體的內部稽核，而不是套一個那麼大的圈圈，感覺上不是那麼容易做到的事情	由企業依據執照核發之營業項目範圍內，調查通訊傳播事業營運所需之資產群組，若組織規模龐大者，得區分為不同之事業體或是部門，區分為關鍵、支援及行政三大類，分別進行資產群組之調查，選定導入範圍
135	不能僅是將「電信事業」改為「通訊傳播事業」，否則修正後的管理手冊要施行，會有窒礙難行之處。赴大陸投資需要額外通過的相關認證，是否有必要，值得再商榷	依據通訊傳播基本法定義通訊傳播:指以有線、無線、衛星或其他電子傳輸設施傳送聲音、影像、文字或數據者。本質上是相同的。

項次.	座談會意見	處理情形
		差別在於對於通信秘密之保護及機線設施之多寡。已修訂於附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 7、8
136	開放赴大陸投資業務項目，僅限第二類電信業者的一般業務，並未針對傳播事業。ISO27011 偏重第一類電信，把對第一類電信的要求放在第二類電信的一般業務，是否恰當，值得再討論	依據通訊傳播基本法定義通訊傳播:指以有線、無線、衛星或其他電子傳輸設施傳送聲音、影像、文字或數據者。本質上是相同的。差別在於對於通信秘密之保護。已修訂於附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 7、8
137	通訊與資訊一定有其相關之處，才會同時由 NCC 所業管。資訊安全不僅指資訊被竊取，也包括資訊的承載、資訊是否被完整與及時的傳送。傳播業雖然未擁有大量民眾個資，但做為重要的資訊承載者，不應妄自菲薄，應將觀念、格局放大一點。舉個最極端的例子來說，軍事上的入侵或政變，控制了資訊就控制了國家的命脈。至於傳播業者是否要跟第一類電信業者負同樣的責任與義務，細節上則可以再討論	依據通訊傳播基本法定義通訊傳播:指以有線、無線、衛星或其他電子傳輸設施傳送聲音、影像、文字或數據者。本質上是相同的。差別在於對於通信秘密之保護。已修訂於附件 4 通訊傳播事業資通安全管理作業手冊(修訂草案)附錄 7、8

資料來源：本計畫自行整理

7. 參考文獻

[1]Allen, D.K. and Fifield, N., “Re-engineering change in higher education”, Information Research, Vol. 4:3. 1999.

[2]Bartlett, F. (1932), “Remembering: A Study in Experimental and Social Psychology”, London: Cambridge University Press.

[3]Bartunek, J., “Changing Interpretive Schemes and Organizational Restructuring: The Example of a Religious Order”, Administrative Science Quarterly, Vol.29, pp. 355-372. 1984.

[4]Bell, J., Doing Your Research Project, Buckingham: Open University Press. 2005.

[5]Berger, P.L. and Luckmann, T., (1967), “The Social Construction of Reality”, New York: Anchor Books.

[6]Blumberg, B., Cooper, D.R. & Schindler, P.S., Business Research Methods, Maidenhead: McGraw-Hill. 2005.

[7]Bougon, M., Weick, K., and Binkhorst, D., “Cognition in Organizations: An Analysis of the Utrecht Jazz Orchestra”, Administrative Science Quarterly, Vol. 22, pp. 606-639. 1977.

[8]Broderick J. S., “ISMS, security standards and security regulations”, Information Security Technical Report, Vol.11:1, pp. 26-31. 2006.

[9]Calder, B. and Schurr, P. “Attitudinal Processes in Organizations”, Research in Organizational Behavior, Vol. 3, pp. 283-302. 1981.

[10]Chang, S. E. and Ho, C. B., “Organizational factors to the effectiveness of implementing information security management”, Industrial Management & Data Systems, Vol. 106:3, pp.345-361. 2006.

[11]Chang, S. E. and Lin, C. S., “Exploring Organizational Culture for Information Security Management”, Industrial Management & Data Systems, Vol. 107:3, pp. 438-458. 2007.

[12]Chang, Shuchih Ernest and Lin, Chin-Shien, “Exploring organizational culture for information security management”, Industrial Management & Data Systems, Vol.107:3, pp.438-458, 2007.

[13]Cooper, R.B., “Information technology development creativity: a case study of attempted radical change”, MIS Quarterly, Vol. 24:2, pp.245-276, 2000

[14]Cooper, R.B., “The inertial impact of culture on IT implementation”, Information Management, Vol.27:1, pp.17-31, 1994.

[15]Daft, R.L. and Weick, K.E., “Towards a Model of Organizations as Interpretive Systems”, Academy of Management Review, Vol. 9, pp. 284-295. 1984.

[16]Douglas, M., (1985) “Measuring Culture: A Paradigm for the Analysis of Social Organization”, Columbia University Press, New York, NY.

[17]Dutton, J.E. and Jackson, S.E., “Categorizing Strategic Issues: Links to Organizational Actions”, Academy of Management Review, Vol. 12, pp. 76-90. 1987.

[18]Eden, C.,“On the Nature of Cognitive Maps”, Journal of Management Studies, Vol. 29:3, pp. 261-265. 1992.

[19]Freeman, Edward H., “Holistic Information Security: ISO 27001 and Due Care”, Information Systems Security, Vol. 16:5, pp. 291-294. 2007.

[20]Fung, M., K. Fung., “To what extent are labor-saving technologies improving efficiency in the use of human resources? Evidence from the banking industry”, Prod. Oper. Manag, Vol. 17:1, pp. 75-92. 2008.

[21]Ghernouti-Hélie, S., Tashi, I. and Simms, D. (2010, February), “A multi-stage methodology for ensuring appropriate security culture and governance”, ARES 2010, Krakow, Poland.

[22]Gioia, D.A., (1986), “Symbols, Scripts, and Sensemaking: Creating

Meaning in the Organizational Experience", In H.R. Sims Jr. and D.A. Gioia (Eds.) The Thinking Organization. San Fancisco CA: Jossey-Bass, 49-74.

[23]Glaser,B. & Strauss,A., The Discovery of GroundedTheorytrategies for Qualitative Research, Chicago: Aldine. 1967.

[24]Gray, B., Bougon, M., and Donnellon, A., "Organizaions as Constructions and Destructions of Meaning", Journal of Management, Vol. 11, pp. 83-95. 1985.

[25]Hagberg, R. and Heifetz, J. (1997), "Corporate Culture: Telling the CEO the Baby is Ugly", Hagberg Consulting Group, San Mateo, CA.

[26]Hristova, N., O'Hare, G.M.P., (2004), "wireless advertising adapted to the user location, device and emotions.", Thirty-Seventh Hawaii International Conference on System Sciences (HICSS-37), IEEE Computer Society Press.

[27] Internation Register of ISMS Certificates http://www.iso27001certificates.com/

[28]ISO/IEC 17799 – Information technology – Code of Practice for Information Security Management, Second edition, ISO, 2005.

[29]ISO/IEC 27001 – Information technology – Information security management systems – Requirements, First edition, ISO, 2000.

[30]ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements

[31] ISO/IEC 27002:2007 Information technology — Security techniques — Code of practice for information security management

[32] ISO/IEC 27003:2010 Information technology — Security techniques — Information security management system implementation guidance

[33] ISO/IEC 27004:2009 Information technology — Security techniques —

Information security management — Measurement

[34] ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk management

[35] ISO/IEC 27011:2008 Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

[36]ISO/IEC, ISO/IEC38500:2008, Corporate governance of information technology, 2008.

[37]Jotsov, V.S. and Sgurev, V.S. (2010, July), "Self-learning strategies in multiagent environments", 2010 IEEE International Conference on Intelligent Systems, London, UK.

[38]Kiesler, S. and Sproull, L., "Managerial Response to Changing Environments: Perspectives on Problem Sensing from Social Cognition", Administrative Science Quarterly, Vol. 27, pp. 548-570. 1982.

[39]Koolwaaij, J., Tarlano, A., Luther, M., Morhs, B., Battestini, A., Vaidya, R., (2006), "ContextWatcher – Sharing context information in everyday life.", IASTED International Conference on Web Technologies, Applications, and Services (WTAS2006), Calgary, Canada.

[40]Liao, S. S., He, J. W. and Tang, T. H., "A framework for context information management", JIS, Vol. 30:6, pp. 528-539. 2004.

[41]Martilla, J. A. and James, J. C., Importance-performance analysis, Journal of Marketing, Vol. 41:1, pp. 77-79. 1985.

[42]McGee, A. R., Bastry, F. A., Chandrashekhar, U., Vasireddy, S. R. and Flynn, L. A., "Using the Bell Labs Security Framework to Enhance the ISO 17799/27001 Information Security Management System", Bell Labs Technical Journal, Vol. 12:3, pp. 39-54. 2007.

[43]Ministry of Economics, Trade and Industry (METI), Guidance to

Introducing Information Security Governance, 1st July, 2009(in Japanese)

[44]Moch, M. and Bartunek, J., (1990), “Creating Alternative Realities at Work: The Quality of Work Life Experiment at FoodCom”, New York: Harper Business.

[45]Neisser, U., (1976), “Cognition and Reality: Principles and Implications of Cognitive Psychology”, San Francisco, CA: W.H. Freeman and Co.

[46]Ogiela, M.R. and Ogiela, U. (2010, April), “Information security management based on grammar threshold schemes”, NOMS 2010, Osaka, Japan.

[47]Ohki, E., (2009), “Framework of Information Security Governance”, Japan Society of Security Management 23rd Annual conference, Japan.

[48]Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T. and Kagaya, T. (2009, November), “Information Security Governance Framework”, WISG ’09, Chicago, USA.

[49]Orlikowski, Wanda J. and Gash, Debra C., “Technological Frames: Making Sense of Information Technology in Organizations”, ACM Transactions on Information Systems, 1993.

[50]Pivka, Marjan & Mulej, Matjazcirc, “Requisitely Holistic ISO 9000 Audit Leads To Continuous Innovation/Improvement”, Cybernetics & Systems, Vol. 35:4, pp. 363-378. 2004.

[51]Porac, J.F. and Thomas, H., “Taxonomic Mental Models in Competitor Definition”, Academy of Management Review, Vol. 15:2, pp. 224-240. 1990.

[52]Saint-Germain, R., “Information Security Management Best Practices Based on ISO/IEC 17799”, Information Management Journal, Vol. 39:4, pp. 60-66. 2005.

[53]Smircich, L. and Stubbart, C., “Strategic Management in an Enacted

World", Academy of Management Review, Vol. 10:4, pp. 724-736. 1985.

[54]Starbuck, W.H., (1989), "Why Organizations Run into Crises ... and Sometimes Survive Them", In K. Laudon and J.A. Turner (Eds.) Information Technology and Management Strategy Englewood Cliffs NJ: Prentice Hall, 11-33.

[55]Tsohou, A., Karyda, M. and Kokolakis, S., "Formulating Information Systems Risk Management Strategies Through Cultural Theory", Information Management & Computer Security, Vol. 14:3, pp. 198-217. 2006.

[56]Van Niekerk, J.F. and Von Solms, R., "Information security culture: A management perspective", Computers and Security, Vol. 29:4, pp. 476-486. 2010.

[57]Weick, K.E., (1979a), "The Social Psychology of Organizing Reading", MA: Addison-Wesley.

[58]Weick, K.E., "Cognitive Processes in Organizations", Research in Organizational Behavior, Vol. 1, pp. 41-74. 1979b.

[59]Weiser, M., "The computer for the 21st century", Scientific American, Vol. 265, pp. 94-104. 1991.

[60]Yin, Robert K, Applications of case study research-2nd ed. ,2003

[61]CNS 14929-3 資訊技術－資訊技術安全管理指導綱要 －第 3 部：資訊技術安全管理之技術

[62]中華民國 97 年 1 月 9 日總統華總一義字第 09700002321 號令修正國家通訊傳播委員會組織法

[63]中華民國 99 年 05 月 26 日華總一義字第 09900125121 號令修訂個人資料保護法

[64]行政院研考會，民 98 年，政府機關落實資通安全之行為模式研究

[65]行政院研考會，民 98 年，資訊系統風險評鑑參考指引

[66]行政院國家資通安全會報，民 98 年修訂，政府機關資訊安全責任等級分級作業施行計畫

[67]行政院國家資通安全會報，民 99 年，資訊系統分類分級與鑑別機制參考手冊

[68]李金泉，1993，SPSS/PC+實務與應用統計分析，松崗電腦圖書資料股份有限公司，台北。

[69]國家通訊傳播委員會公告取得 ISO/IEC 27001 證明之電信事業名單 http://www.ncc.gov.tw/chinese/content.aspx?site_content_sn=2251&is_history=0

[70]國家通訊傳播委員會公告電信傳播事業業者名單 http://www.ncc.gov.tw/chinese/gradation.aspx?site_content_sn=1357&is_history=0

[71]陳育砥,以組織生態學與社會交換理論探討組織導入標準,碩士論文,2010

8. 附件

8.1.附件 1 資訊安全管理系統研究問卷

8.2.附件 2 資訊安全測量構面範例

8.3.附件 3 通訊傳播事業資通安全管理要點修正條文對照表(英文版)

8.4.附件 4 通訊傳播事業資通安全管理手冊修訂建議草案

8.4.1. 附錄 1 通訊傳播事業資通安全等級自我評估彙整表

8.4.2. 附錄 2 通訊傳播事業資通安全等級自我評估說明表

8.4.3. 附錄 3 通訊傳播事業資通安全管理詳細風險評鑑表

8.4.4. 附錄 4 通訊傳播事業資通安全管理機制實施計畫參考範本

8.4.5. 附錄 5 資通安全管理實施計畫應執行工作事項表

8.4.6. 附錄 6 通訊傳播事業資通安全管理內部稽核表(修訂對照)

8.4.7. 附錄 7 通訊事業增項稽核表

8.4.8. 附錄 8 傳播事業增項稽核表

8.4.9. 附錄 9 個人資料保護安全控制措施

8.4.10. 附錄 10 國家通訊傳播委員會資通安全事故通報單

8.4.11. 附錄 11 資通安全管理矯正／預防措施一覽表

8.4.12. 附錄 12 資通安全管理矯正／預防措施單

8.4.13. 附錄 13 內部稽核表檢查項目勾選不適用之說明

8.4.14. 附錄 14 增項稽核表檢查項目勾選不適用之說明

8.5.附件 5 通訊傳播事業資通安全管理手冊修訂建議草案(英文版)

8.6.附件 6 通訊傳播事業資通安全管理內部稽核修訂對照表

8.7.附件 7 通訊事業增項稽核修訂對照表

8.8.附件 8 傳播事業增項稽核修訂對照表

8.9.附件 9 通訊傳播事業個資保護控制措施內部稽核修訂對照表

8.10.附件 10 第 1 場次資通安全管理機制座談會會議紀錄

8.11.附件 11 第 2 場次資通安全管理機制座談會會議紀錄

8.12.附件 12 第 3 場次資通安全管理機制座談會會議紀錄

8.13.附件 13 第 4 場次資通安全管理機制座談會會議紀錄

8.14.附件 14 第 5 場次資通安全管理機制座談會會議紀錄

8.15.附件 15 第 6 場次資通安全管理機制座談會會議紀錄

8.16.附件 16 資通安全管理機制成果發表會會議記錄

8.17.附件 17 ISO/IEC 27011 控制措施對照表

附件1　資訊安全管理系統研究問卷

問卷編號：

敬愛的企業主管 您好：

國家通訊傳播委員會(以下簡稱NCC)有鑑於通訊、傳播事業擁有大量消費者個人資料，已成為不法集團窺伺與竊取之目標，然國內多數業者之資訊安全實施範圍尚不夠完整，為建構政府及民間完整資安防護網，擬配合增訂相關法規條文，賦予導入資通安全管理機制之法源。為瞭解「**產業資訊安全與個人資料保護現況**」，本研究擬進行以下問卷調查，**所蒐集之資料僅供**資訊安全管理系統研究計畫(以下稱本計畫)**之用，您的寶貴意見對於本計畫具有關鍵之影響，研究之成果將會提供NCC作為修訂「通訊傳播事業資通安全管理作業要點」建議草案及「通訊傳播事業資通安全管理手冊」建議版本之參考**。

本問卷內容不會蒐集您所屬企業的營業機密與您個人的隱私問題，且該資料之識別資訊會加以妥慎處理，使其揭露方式無從識別特定企業及當事人，請您安心！在此對您的熱心協助，致上萬分謝意！

請您協助於5月20日前完成填答，並將紙本郵寄給中華軟協鍾如郁小姐收；您也可透過電子郵件(yedda@mail.cisanet.org.tw)或傳真(FAX：02-2557-9007)方式回覆，謝謝。

委託機關：國家通訊傳播委員會

執行機關：中華民國資訊軟體協會
聯絡人：鍾如郁資深專員
聯絡地址：台北市大同區承德路二段239號6樓
聯絡電話：(02)2553-3988分機629
電子信箱： yedda@mail.cisanet.org.tw

問卷填寫說明

(1) 本問卷需要您提供：貴公司目前資訊安全管理的現況，請就您瞭解的內容，作為回答以下問題的依據。
(2) 本問卷採用逐項列舉的評量尺度(填答範例如下表)，請以1到5分為標準，數字愈大代表認知**重要程度/實際實施程度**愈高，請您依據實際情況，在”☐”**勾選**(☒)出一個最適合的敘述。

請依下列敘述，選出貴公司所認知的重要程度與實際的實施程度。(請二者都填)	認知重要程度 非常不重要 / 稍微不重要 / 普通 / 稍重要 / 非常重要	實際實施程度 完全沒實施 / 僅少部份實施 / 已部份實施 / 大部份實施 / 完全落實
貴公司的資安政策：		
1. 有高層的支持。…….….....	☐ ☐ ☒ ☐ ☐	☐ ☐ ☒ ☐ ☐
2. 有將資安政策文件化。.....…….....	☐ ☐ ☐ ☒ ☐	☐ ☒ ☐ ☐ ☐

本問卷需要由業管　貴公司**內部稽核或資訊安全的管理階層協助**填答。若您未參與上述業務，請將本問卷轉交給適當之主管填答。感謝您!

壹、**企業基本資料：(請勾選)**

1.貴公司所屬產業類別：

□第一類電信產業 □第二類電信產業 □傳播產業

2.貴公司營業項目：**(請勾選貴公司核准的營業項目，可重覆勾選)**

第一類電信事業核准營業項目

□固定通信網路業務
□行動通信網路業務
□衛星固定通信業務
□其他＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿(請勾選後填寫)

第二類電信事業核准營業項目

□語音單純轉售服務
□非E．164 網路電話服務
□E．164 網路電話服務
□批發轉售服務
□公司內部網路通信服務
□頻寬轉售服務
□語音會議服務
□網際網路接取服務
□存轉網路服務
□存取網路服務
□視訊會議服務
□數據交換通信服務
□付費語音資訊服務
□行動轉售服務
□行動轉售及加值服務
□其他＿＿＿＿＿＿
(請勾選後填寫)

傳播事業

□無線廣播電臺
□無線電視電臺
□社區共同天線業者
□衛星廣播電視事業(直播衛星廣播電視服務經營者)
□衛星廣播電視事業(衛星廣播電視節目供應者)
□有線電視系統經營者
□有線電視播送系統
□其他＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿(請勾選後填寫)

3.貴公司員工人數：□一百人以下 □一百人至五百人 □五百人至一千人

□一千人至五千人 □五千人至一萬人 □一萬人以上

4.貴公司資本額（新台幣）：

□一億以下 □一億至十億 □十億至五十億 □五十億至一百億

□一百億至一百五十億 □一百五十億至二百億 □二百億以上

5.貴公司擁有個人資料的數量：

□無客戶個人資料 □一千萬筆以上

□五千筆以下 □五千至五萬筆 □五萬至五十萬筆

□五十萬至一百萬筆 □一百萬至五百萬筆 □五百萬至一千萬筆

6.貴公司是否已通過 CNS/ISO/IEC 27001 驗證　　□是　□否

7.貴公司通過 CNS/ISO/IEC 27001 驗證之範圍(前一題填答"是"者，請回答本題)

□依據實體環境區分（例如：主機房）

□依據部門/單位區分（例如：資訊中心）

□依據業務流程區分（例如：客戶服務）

□依據資訊系統區分（例如：帳務管理系統）

□依據資訊流區分（例如：涉及個人資料之資訊系統及部門/單位均納入）

貳、**企業資訊環境：(請勾選)**

請依下列敘述，選出貴公司所認知的重要程度。	認知重要程度				
	非常不重要	稍微不重要	普通	稍微重要	非常重要
營運業務所需之**資訊化**程度。	□	□	□	□	□
對上述**資訊系統之依賴**程度。	□	□	□	□	□
擁有資訊**設備與員工**的比例。	□	□	□	□	□
對**委外**作業**安全**之重視程度。	□	□	□	□	□
對於資訊安全**資源投入**比例。	□	□	□	□	□
以**系統化**的方法，實施資安管理程度。	□	□	□	□	□
對於企業營運過程之**風險**進行**評鑑**作業之程度。	□	□	□	□	□
營運安全包含人員、實體、系統及**營運持續**等重視之程度。	□	□	□	□	□
對於員工之安全**認知訓練**程度。	□	□	□	□	□
對於營運安全維護，訂定明確之**權責區分**與作業程序之程度。	□	□	□	□	□
對於客戶**個人資料**之保護程度。	□	□	□	□	□
安全概念已融入貴公司**組織文化**之程度。	□	□	□	□	□
法律對於貴公司落實資訊安全意願的影響程度。	□	□	□	□	□
主管機關的政策對於貴公司**資源投入**資訊安全的影響程度。	□	□	□	□	□
資料**保護受到損害**之重視程度。	□	□	□	□	□
對於安全**影響業務運作**之重視程度。	□	□	□	□	□
對於安全相關**法律規程之遵循**程度。	□	□	□	□	□
安全造成**人員傷亡**之重視程度。	□	□	□	□	□
安全損害**組織信譽**之重視程度。	□	□	□	□	□

參、問卷

請依下列敘述，選出貴公司所認知的重要程度與實際的實施程度。(請二者都填)	認知重要程度					實際實施程度				
	非常不重要	稍微不重要	普通	稍微重要	非常重要	完全沒有實施	僅少部份實施	已部份實施	大部份已實施	完全落實實施
貴公司資安相關的管理活動： 1. 有**管理階層主動的支持**與領導。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司在與外部團體進行活動時： 1. 在與**第三方的協議**中，會涵蓋所有資安要求及與需要實作的安全控制措施。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司的組織**資產**： 1. 有指定的部門或專人負責維護與管理。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司組織資產所採取的**分類**法： 1. 依據**分類**結果實施**機密等級**的標示與保護措施。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司對於**聘僱前**的員工、承包商及第三方使用者： 1. **聘僱契約**有陳述他們對組織資安的責任。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司對於**聘僱間**的員工、承包商及第三方使用者： 1. 有定期接受與職務相關的資安**認知訓練**。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司對於**終止聘僱**員工、承包商及第三方使用者： 1. 有要求歸還所擁有的組織資產，並確實地將存取**權限移除**。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司對於**實體安全**： 1. 有**門禁管控**及保護辦公室、房間及設備之保全設施。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司對於**設備安全**的保護： 1. 保護**不受**停電或其他公用設施失效而**中斷運作**之措施。..... 2. 有措施保護**組織外部**所擁有的設備。..... 3. 在**汰換設備前**有檢核是否儲存任何敏感資料。..... 4. **未經授權**不得將設備、資訊及軟體**帶出**。.....	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐
貴公司對於**資訊設備**與系統： 1. 操作時職務與**權限**有加以區隔。..... 2. **開發、測試及運作**有加以區隔。.....	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐
貴公司對於**委外廠商**： 1. 有定期監審及稽核他們提供的服務與報告。..... 2. 委外所造成的變更有進行管理與重新評鑑風險。.....	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐
貴公司對於系統的**規劃與驗收**： 1. 有對未來系統容量的要求**預作規劃**。..... 2. 有建立明確的**驗收準則**。.....	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐
貴公司對於**程式碼**： 1. 有防範惡意程式碼的**控制措施**與辦法。..... 2. 有防止未經授權程式碼**執行**的控制措施與辦法。.....	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐

請依下列敘述，選出貴公司所認知的重要程度與實際的實施程度。(請二者都填)	認知重要程度					實際實施程度				
	非常不重要	稍微不重要	普通	稍微重要	非常重要	完全沒有實施	僅少部份實施	已部份實施	大部份已實施	完全落實實施
貴公司對於**備份**政策：										
1. 有**定期**的執行備份。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 有測試在系統失效後能**馬上復原**。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
對於貴公司的**網路服務**與安全：										
1. 有**管控**網路系統與應用程式。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 有**確保**網路服務提供者以安全的方式提供**服務**。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司對於**儲存媒體**的管理：										
1. 有適當的程序，管理**可攜式**的媒體。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 有正式的**汰換程序**，以防止敏感資訊的洩露。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司對於**資訊交換**的安全：										
1. 與**組織外**的團體(單位)建立保護協議。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 對於**工作場域間**傳送的資訊加以保護。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司對於**電子商務**的安全：										
1. 保護在公眾**網路上傳輸**而涉及電子商務的資訊，使不受未經授權的揭露與修改。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 保護涉及**線上交易**的資訊，以防止不完整傳輸或未經授權的揭露或複製。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司對於資安的**監控**：										
1. 有相關的**稽核日誌**，以記錄異常。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 有**記錄**系統管理者與操作者的**活動**。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司對於**使用者**的**管理**：										
1. 有正式的**註冊**與註銷註冊程序。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 有正式的管理程序控制**通行碼**(Password)的配發。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司**要求使用者**：										
1. 要求使用者遵照良好安全實務去**選擇與使用通行碼**(Password)。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 對紙本媒體與可移除式儲存媒體之**桌面淨空**，及資訊處理設施的**螢幕淨空**。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司對於網路**服務**的**存取**：										
1. 使用者要經過特定**授權**才可以使用。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 有對不同使用**群組**的網路加以**區隔**。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司對於**作業系統**的**存取控制**：										
1. 由保全**登入程序**控制作業系統的存取。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 有唯一及可辨識的**使用者ID**。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
對於貴公司**資訊與應用系統**的存取控制：										
1. 有明確的**政策限制**使用者與支援人員。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 敏感性系統有**隔離**的電腦作業**環境**。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

請依下列敘述，選出貴公司所認知的重要程度與實際的實施程度。(請二者都填)

	認知重要程度					實際實施程度				
	非常不重要	稍微不重要	普通	稍微重要	非常重要	完全沒有實施	僅少部份實施	已部份實施	大部份實施	完全落實實施
對於貴公司**行動**運算與**通信**設備的資安：										
1. 宜採取適當的安全措施，以防範使用行動計算(**筆記型電腦**)與通信設施(**行動上網**)的風險。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 備妥適切的安全安排與控制措施，才可授權遠距工作的活動。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司對於新資訊系統或現有資訊系統的**營運提升**：										
1. 有特別詳述對資安**控制措施的要求**。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
對於貴公司的**應用系統**：										
1. 有**確認輸入**的資料，以確保正確且適切。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 資訊/資料的**輸出**之確認。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
對於貴公司的**密碼**控制措施：										
1. 發展與實施正式的**政策**。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 有適當的**金鑰管理**。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
對於貴公司的系統與程式碼的**控制**：										
1. 有對**測試資料**進行保護。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 有**程式源碼**存取的限制。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司對於作業系統與應用程式的**變更**：										
1. 對於**軟體套件**變更的限制。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 有監督**委外**的開發。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司對於控制資訊系統的技術**脆弱性**：										
取得**及時**的資訊並進行**評估**，以採取適當的措施。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
所有員工、承包商及第三方使用者的**資安事件通報**：										
1. 有適切的**通報管道**。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 會**通報**可疑的資安**弱點**。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
對於貴公司**回應**資安事故與改進：										
1. 有建立管理的**責任**與**程序**。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 會從資安事故中**學習**，並收集證據符合審判證明的規則。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
貴公司對於維持整體組織營運**持續運作**的管理過程：										
1. 能**及時恢復**中斷的營運到要求的等級。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 有**定期**的**測試**與**更新**計畫。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
對於要求貴公司相關的**法律**、**法令**、**法規**與**契約**：										
1. 有實施適當的程序，以**遵循**智慧財產權的**要求**。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. 有**確保個人資料**的保護與隱私。.....	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

四、貴公司期望主管機關給予之協助：_____

_____

_____

_____

五、您是否希望得到本研究的結果? □是 □否

收 件 人:_____職　　稱:_____

電子郵件:_____ 服務機構:_____

聯絡地址:_____

<問卷到此結束，感謝您熱心協助!>

附件 2　　資訊安全測量構面範例

ISO/IEC 27004:2009 附錄 A 提供一個資訊安全測量構面的樣板，樣板包含所有在 7.5 定義，在 5.4 所描述的元件，組織可根據本身的需求進行樣板修改。

B.1　ISMS 訓練

B.1.1　ISMS 完訓人員

B.1.2　資訊安全訓練

B.1.3　資訊安全認知訓練之符合性

B.2　密碼原則

B.2.1　密碼品質 – 手動的

B.2.2　密碼品質 – 自動的

B.3　ISMS 審查流程

B.4　ISMS 持續改善資訊安全事故管理

B.4.1　有效性

B.4.2　矯正措施的實施

B.5　管理承諾

B.6　對惡意程式碼的保護

B.7　實體環境控制措施

B.8　紀錄檔的審查

B.9　定期維護管理

B.10　第三方安全協議

相關流程與控制措施	相關測量構面範例	測量構面範例名稱
4.2.2 h)	B.4.1	資訊安全事故管理有效性
5.2.2 d)	B.1.1	ISMS 完訓人員
8.2	B.4.2	矯正措施的實施
A.6.1.8	B.3	ISMS 審查流程

相關流程與控制措施	相關測量構面範例	測量構面範例名稱
A.6.1.1 和 A.6.1.2	B.5	管理承諾
A.6.2.3	B.10	第三方安全協議
A.8.2 和 A.8.2.2	B.1.2	資訊安全訓練
A.8.2 和 A.8.2.2	B.1.3	資訊安全認知之符合性
A.9.1.2	B.7	實體環境控制措施
A.9.2.4	B.9	定期維護管理
A.10.4.1	B.6	對惡意程式碼的保護
A.10.10.1 和 A.10.10.2	B.8	紀錄檔的審查
A.11.3.1	B.2.1	密碼品質 – 手動的
A.11.3.1	B.2.2	密碼品質 – 自動化

B.1 ISMS 訓練

B.1.1 ISMS 訓練人員

測量構面辨識	
測量構面名稱	ISMS 完訓人員
事故識別碼	特定組織
測量構面目的	建立組織資訊安全原則的控制措施遵守
控制措施/流程目標	5.2.2[27001:2005]訓練、認知與能力
控制措施(1)/流程(1)	5.2.2.d[27001:2005]控制措施/流程下的測量 組織應確保被賦與 ISMS 責任的所有人員應有能力執行任務，包含維持教育紀錄、培訓、技能、經驗及資歷
控制措施(2)/流程(2)	如果適用(已規劃或已實施)，如果允許可進一步將控制措施/流程群組化，包含在相同度量範圍之內
測量與屬性的目標	
測量目標	員工資料庫

屬性	訓練紀錄
基本度量值等級 (1)	
基本度量值	員工已經接受 ISMS 每年訓練計畫的訓練人數 員工已經接受 ISMS 訓練的人數
測量方法	ISMS 訓練的紀錄/註冊的計數(欄位填寫為"已取得訓練")
測量方法類型	數值
等級類型	比率
測量單元	員工
延伸測量規格	
延伸測量	ISMS 訓練人員的百分比值
測量功能	接受 ISMS 訓練的員工人數/必須接受 ISMS 訓練的員工人數
指標等級	
指標	使用色碼做顏色標識，長條圖描繪幾個報告期間對於門檻界線(紅色、黃色、綠色：在分析模型詳加定義)的遵守，用於圖表的報告期間的次數是由組織自行定義
分析模型	0 – 60%: 紅色；60 – 90%: 黃色；90 – 100%: 綠色 黃色等級，如果每季增加未達 10%，將被自動評估為紅色
決策標準等級	
決策標準	紅色 – 干預是必需的,必須進行因果關係的分析來找到不遵守和表現不佳的原因 黃色 – 此指標應密切關注，免於下降到紅色值 綠色 – 無須任何行動
測量結果	
指標詮釋	特定組織
報表格式	根據決策標準繪製不同顏色的長條圖。測量方法與可能進行的管理行動之簡短摘要，應附加於長條圖上

股東	
測量委託人	負責 ISMS 的經理人
測量審查人	負責 ISMS 的經理人
資訊擁有者	負責訓練的經理人 – 人力資源
資訊蒐集者	負責訓練管理 – 人力資源部門
資訊溝通者	負責 ISMS 的經理人
頻率/期間	
資料蒐集頻率	每月，每月的第一個工作日
資料分析頻率	每季
產出測量結果報表的頻率	每季
測量版本	一年一次審查
測量期間	一年一次

B.1.2 資訊安全訓練

測量構面辨識	
測量構面名稱	資訊安全訓練
事故識別碼	特定組織
測量構面目的	評量年度資訊安全認知訓練要求的遵守
控制措施/流程目標	A.8.2 在職期間 目標：確保所有員工、承包商以及第三方使用者都瞭解資訊安全威脅與其關切事項、以及他們的職責和責任，並配備支援組織安全政策的過程中，減少人為錯誤的風險
控制措施(1)/流程(1)	A.8.2.2. [27001:2005] 資訊安全認知、教育、與訓練 有關他們的工作職能，所有組織的員工、相關承包商及第三方使用者等，應當接受適當的認知培訓和定期更新組織政策和程序
測量與屬性的目標	
測量目標	員工資料庫
屬性	訓練紀錄
基本度量值等級 (1)	
基本度量值	員工已經接受年度資訊安全認知訓練的人數 員工需要接受年度資訊安全認知訓練的人數
測量方法	年度資訊安全認知訓練的記錄/註冊的計數(欄位為”已取得訓練”)
測量方法類型	數值
等級類型	比率
測量單元	員工
延伸測量規格	
延伸測量	人員接受年度資訊安全認知訓練的百分比

測量功能	接受年度資訊安全認知訓練的員工數 需要接受年度資訊安全認知訓練的員工數
指標等級	
指標	使用色碼做顏色標識，長條圖描繪幾個報告期間對於門檻界線(紅色、黃色、綠色：在分析模型詳加定義)的遵守，用於圖表的報告期間的次數是由組織自行定義
分析模型	0 – 60%: 紅色；60 – 90%: 黃色；90 – 100%: 綠色。 黃色等級，如果每季增加未達 10%，將被自動評估為紅色
決策標準等級	
決策標準	紅色 – 干預是必需的,必須進行因果關係的分析來找出不遵守和表現不佳的原因 黃色 – 此指標應密切關注，免於下降到紅色值 綠色 – 無須任何行動
測量結果	
指標詮釋	特定組織
報表格式	根據決策標準繪製不同顏色的長條圖。測量方法與可能進行的管理行動之簡短摘要，應附加於長條圖上
股東	
測量委託人	負責 ISMS 的經理人；安全管理；訓練管理
測量審查人	安全經理人
資訊擁有者	資訊安全主管與負責訓練的經理人
資訊蒐集者	負責訓練管理 – 人力資源部門
資訊溝通者	負責 ISMS 的經理人
頻率/期間	
資料蒐集頻率	每月，每月的第一個工作日
資料分析頻率	每季
產出測量結果	每季

報表的頻率	
測量版本	一年一次審查
測量期間	一年一次

B.1.3 資訊安全認知之符合

測量構面辨識	
測量構面名稱	資訊安全認知原則之符合
事故識別碼	特定組織
測量構面目的	評估所有相關人員遵守組織的安全原則的狀況
控制措施/流程目標	在職期間 確保所有員工、承包商及第三方使用者都瞭解資訊安全威脅與其關切事項、以及他們的職責和責任，並配備支援組織安全政策的過程中，減少人為錯誤的風險
控制措施(1)/流程(1)	有關他們的工作職能，所有組織的員工、相關承包商及第三方使用者等，應當得到適當的認知培訓和定期更新組織政策和程序 (實施）所有有關的人員必須接受 ISMS 資訊安全認知培訓，方能獲得資訊系統授權資格
控制措施(2)/流程(2)	管理應要求員工、承包商及第三方使用者，按照組織內既定的政策和程序應用安全 (實施）所有相關 ISMS 人員在被授予資訊系統使用權限以前，應必須簽署協議
測量與屬性的目標	
測量目標	1.1. 資訊安全認知訓練計畫/時程安排 1.2. 已經完成訓練或是在訓練過程中的人員 2.1. 計畫簽署使用者協議/時程安排 2.2. 已經簽署協議的人員
屬性	1.1. 確定計畫的人員 1.2. 人員狀態方面的培訓 2.1. 確定簽署計畫的人員 2.2. 人員狀態方面的協議簽署

基本度量值等級 (1)	
基本度量值	1.1. 截至目前的計畫人員數 1.2. 簽署的人員數 2.1. 截至目前簽署計畫的人員數 2.2. 截至目前已簽署的人員數
測量方法	1.1. 計算截至目前已經簽署或完成訓練的人員數 1.2. 詢問負責人已經完成訓練與簽署的的人員百分比 2.1. 計算至此日已經簽署或完成訓練的人員數 2.2. 計算已經簽署協議的人員數
測量方法類型	1.1. 客觀的 1.2. 主觀的 2.1. 客觀的 2.2. 客觀的
等級	1.1. 從零到無窮大的整數 1.2. 從零到一百的整數 2.1. 從零到無窮大的整數 2.2. 從零到無窮大的整數
等級類型	1.1. 序數 1.2. 比率 2.1. 序數 2.2. 序數
測量單元	1.1. 人員 1.2. 百分率 2.1. 人員 2.2. 人員
延伸測量規格	
延伸測量	1. 截至目前的進展 2. 截至目前簽屬的進展

測量功能	1. 狀態表示為比例組合 2. 趨勢
指標等級	
指標	a) 狀態表示為組合的比例 b) 趨勢
分析模型	a) 以[截至目前計畫人員數乘以 100]除以[截至目前的進展]和截至目前簽署的進展 b) 與先前的狀態進行比對
決策標準等級	
決策標準	a) 結果比率應該相對地落在 0.9 到 1.1 之間以及 0.99 到 1.01 之間，表示控制措施目標與沒有行動的達成率。 b) 趨勢應該要向上或是呈現穩定的狀態
測量結果	
指標詮釋	指標的詮釋 a) 如以下所述: -遵守組織安全認知原則的組織標準滿意比例應落在 0.9 <=1st 比率 <=1.1 與 0.99 <=2nd 比率 <=1.01 ，對應到標準字體。 -遵守組織安全認知原則的組織標準滿意度欠佳比例應落在 1st 比率 < 0.9 或 1st 比率 >1.1，與 0.99 <= 2nd 比率 <=1.01，對應斜體字。 -遵守組織安全認知原則的組織不符合的比率 2nd 比率<0.99 或 2nd 比率>1.1，對應粗體字。 指標的詮釋 b) 如以下所述: -趨勢線向上顯示員工服從原則有更好的現象，趨勢線向下則表明素質下降，趨勢變化的程度能提供實施控制措施的有效性。圖形兩個方向的變化指出，控制措施實施上需要仔細檢查來確定原因，如果趨勢是負向的，那可能需要管理層的干涉，而正向趨勢則應該被檢驗來鑑定潛在的做法。
報表格式	標準字體：滿到標準滿意程度 斜體字：達到未標準滿意程度 粗體字：未達到標準
股東	

測量委託人	負責 ISMS 的經理人；安全管理；訓練管理
測量審查人	安全經理人
資訊擁有者	資訊安全主管；訓練經理人
資訊蒐集者	訓練管理 – 人力資源部門
資訊溝通者	負責 ISMS 的經理人
頻率/期間	
資料蒐集頻率	每月，每月的第一個工作日
資料分析頻率	每季
產出測量結果報表的頻率	每季
測量版本	一年一次審查
測量期間	一年一次

B.2 密碼原則

B.2.1 密碼品質 – 手動的

測量構面辨識	
測量構面名稱	密碼品質
事故識別碼	特定組織
測量構面目的	評估使用者登入組織資訊系統所使用的密碼品質
控制措施/流程目標	防止使用者選擇使用不安全的密碼
控制措施(1)/流程(1)	使用者應該被要求遵守良好的密碼選擇和使用的安全實務實施： 所有使用者對每個系統應選擇安全性較強的密碼，包含： 1)密碼長度高於 8 2)不是任何一個人容易猜測或者利用個人相關資訊而取得，例如姓名、電話、生日等 3)不要包含字典用字 4)可自由使用連續相同的全數字或全字母字元 對組織的資訊系統，所有使用者的帳號和密碼必須被員工系統所控管，密碼強度可藉由密碼破解軟體進行檢測
測量與屬性的目標	
測量目標	使用者密碼資料庫
屬性	個人密碼
基本度量值等級 (1)	
基本度量值	1. 以註冊密碼的數量 2. 密碼字元數是能夠滿足組織密碼品質原則
測量方法	1. 計算使用者密碼資料庫的密碼字元數 2. 要求每位使用者能使用滿足組織密碼原則的字元數
測量方法類型	1. 客觀的 2. 主觀的

等級	1. 從零到無窮大的整數 2. 從零到無窮大的整數
等級類型	1.1. 序數 1.2. 比率 2.1. 序數 2.2. 序數
測量單元	1.1. 人員 1.2. 百分率 2.1. 人員 2.2. 人員
延伸測量規格	
延伸測量	遵守著組織密碼品質原則的密碼的字元總數
測量功能	遵守著組織密碼品質原則的密碼字元數之總和
指標等級	
指標	a) 滿足組織密碼品質原則的密碼比率 b) 根據密碼品質原則遵守的狀態趨勢
分析模型	a) 以[註冊密碼的數量]除以[遵守著組織密碼品質原則的密碼字元數之總和] b) 比較前者比率
決策標準等級	
決策標準	如果產生的結果比率是 0.9 以上，代表控制措施目標的達成，則沒有行動需要額外進行。如果產生的結果比率落在 0.8 與 0.9 之間，則控制措施目標沒有達成，但是正面趨勢指出需要改善。如果產生的結果比率落在 0.8 以下，則須立即採取行動。
測量結果	
指標詮釋	指標的定義 1 應如同以下所述：

	• 組織標準須符合組織密碼策略的滿意比例> 0.9 • 組織標準須符合組織密碼策略的欠佳比例在[0.8 <= 的比率<= 0.9] • 組織標準符合組織密碼原則不符合的比例<0.8 指標的定義 b)應如同以下所述： • 趨勢線向上顯示員工服從原則有更好的現象，趨勢線向下則表明素質下降。趨勢變化的程度可以提供洞察實施控制措施的有效性 • 負向趨勢須要更進一步的控制措施像是共識或技術手法去強迫選擇一組強大的密碼或是定期性的更改密碼 • 正向趨勢應該被檢驗從目前的比例中去估計必要條件去符合密碼規範 其效果的標準沒有得到滿足，是妥協密碼的風險增加，可能導致未經授權的系統訪問，標準規範的效果不符合，讓密碼的風險增加，可能導致未經授權的軟體侵入。衍生的潛在因素包含安全知識的缺乏，技術實施的不足,和實施在全資訊系統上時間的不足
報表格式	趨勢線描繪了密碼的數量，與組織的密碼品質原則一致，與以前報告期間的趨勢線進行重疊呈現趨勢線
股東	
測量委託人	負責 ISMS 的經理人；安全經理人
測量審查人	安全管理
資訊擁有者	系統管理員
資訊蒐集者	安全人員
資訊溝通者	安全人員
頻率/期間	
資料蒐集頻率	每年

資料分析頻率	每年
產出測量結果報表的頻率	每年
測量版本	每一年審查與更新
測量期間	一年一次

B.2.2 密碼品質 – 自動的

測量構面辨識	
測量構面名稱	密碼品質
事故識別碼	特定組織
測量構面目的	評估使用者登入組織資訊系統所使用的密碼品質
控制措施/流程目標	防止使用者選擇使用不安全的密碼
控制措施(1)/流程(1)	使用者應該被要求遵守良好的密碼選擇和使用的安全實務
測量與屬性的目標	
測量目標	員工系統帳戶資料庫
屬性	儲存於員工系統帳戶紀錄的個別密碼
基本度量值等級 (1)	
基本度量值	1. 密碼總數 2. 未被破解的密碼總數
測量方法	1. 查詢員工帳戶資料 2. 在員工系統帳戶紀錄使用混合攻擊的密碼駭客
測量方法類型	1. 客觀的 2. 客觀的
等級	1. 從零到無窮大的整數 2. 從零到無窮大的整數
等級類型	1. 次序 2. 次序
測量單元	1. 密碼 2. 密碼
延伸測量規格	
延伸測量	無

測量功能	無
指標等級	
指標	1) 能在四小時內破解的密碼比率 2) 比率值為 1 的趨勢
分析模型	a) 以[密碼總數]除以[破解的密碼總數] b) 比較前者比率
決策標準等級	
決策標準	如果產生的結果比率是 0.9 以上，代表控制措施目標的達成，則沒有行動需要額外進行。如果產生的結果比率落在 0.8 與 0.9 之間，則控制措施目標沒有達成，但是正面趨勢指出需要改善。如果產生的結果比率落在 0.8 以下，則須立即採取行動。
測量結果	
指標詮釋	指標 1 的詮釋如以下所述： • 組織標準須符合組織密碼策略的滿意比例> 0.9 • 組織標準須符合組織密碼策略的欠佳比例在[0.8 < 1 比率< 0.9] • 組織標準符合組織密碼政策不符合的比例<0.8 指標的定義 b)應如同以下所述： • 趨勢線向上顯示員工服從原則有更好的現象.趨勢線向下則表明素質下降。趨勢變化的程度可以提供洞察實施控制措施的有效性 • 負向趨勢須要更進一步的控制措施像是共識或技術手法去強迫選擇一組強大的密碼或是定期性的更改密碼 • 正向趨勢應該被檢驗從目前的比例中去估計必要條件去符合密碼規範 其效果的標準沒有得到滿足，是妥協密碼的風險增加，可能導致未經授權的系統訪問，標準規範的效果不符合，讓

	密碼的風險增加，可能導致未經授權的軟體侵入。衍生的潛在因素包含安全知識的缺乏,技術實施的不足，和實施在全資訊系統上時間的不足
報表格式	趨勢線描繪所有紀錄測試的密碼破解，與以前報告期間的趨勢線進行重疊呈現趨勢線
股東	
測量委託人	負責 ISMS 的經理人。安全管理人
測量審查人	安全管理
資訊擁有者	系統管理員
資訊蒐集者	保安人員
資訊溝通者	保安人員
頻率/期間	
資料蒐集頻率	每周
資料分析頻率	每周
產出測量結果報表的頻率	每周
測量版本	每一年審查與更新
測量期間	適用於每三年一次

B.3 ISMS 審查流程

測量構面辨識	
測量構面名稱	ISMS 審查流程
事故識別碼	特定組織
測量構面目的	評估資訊安全的獨立審查完成程度
控制措施/流程目標	管理組織內的資訊安全
控制措施(1)/流程(1)	A.6.1.8 組織管理資訊安全與實施的方法 (例如：資訊安全的控制措施目標、控制措施、原則、流程、程序) 在計畫的時間間隔內，或者當安全導入的重大改變時應該被獨立審查。 (實施)組織管理資訊安全方法與其導入應該被第三方資訊安全顧問進行檢視審查
測量與屬性的目標	
測量目標	1. 第三方審查的報告 2. 第三方審查的計畫
屬性	1. 由第三方審查報告 2. 由第三方審查計畫
基本度量值等級 (1)	
基本度量值	1. 由第三方審查次數 2. 計畫由第三方審查的總次數
測量方法	1. 經由第三方定期審查報告的次數 2. 計畫由第三方定期審查報告的總次數
測量方法類型	1. 客觀的 2. 客觀的
等級	1. 從零到無窮大的整數 2. 從零到無窮大的整數

等級類型	1. Ordinal 次序 2. Ordinal 次序
測量單元	1. 審查 2. 審查
延伸測量規格	
延伸測量	無
測量功能	無
指標等級	
指標	完成獨立審查的進度比率
分析模型	以「經由第三方定期審查報告的次數」除以「計畫由第三方定期審查報告的總次數」求得的值
決策標準等級	
決策標準	指標值應或在 0.8 到 1.1 之間,表示控制措施目標與沒有行動的達成率。而且如果無法滿足主要情況，其值應該超過 0.6。
測量結果	
指標詮釋	指標的定義應如同以下所述: 組織內資訊安全管理的組織標準透過第三方審查應符合 0.8<=比例<=1.1 組織規範符合組織的欠佳比例在[0.6<=比例<0.8 或 1 比例>1.1，監控是必須去卻飽式當的程序是被執行的 組織規範不符合[0<=比例<0.6]，必須立即介入以確保適當的程序是被執行的 如果第二季的季末，其指標是未滿足，資深管理應該被通知與要求來支援 其效果的標準沒有得到滿足，則是沒有效率的管理審核流程，衍生的潛在因素包含低預算、不正確的計畫、以及缺

	少重要人員與管理承諾
報表格式	長條圖描繪經過一段報告產出時間與決策標準所定義的門檻界線之遵守
股東	
測量委託人	負責 ISMS 的經理人。品質系統管理人
測量審查人	負責 ISMS 的經理人
資訊擁有者	負責 ISMS 的經理人
資訊蒐集者	內部審計。品質管理人
資訊溝通者	內部審計。品質管理人。負責 ISMS 的經理人
頻率/期間	
資料蒐集頻率	每季
資料分析頻率	每季
產出測量結果報表的頻率	每季
測量版本	每兩年審查與更新
測量期間	適用於每兩年一次

B.4 ISMS 持續改善

B.4.1 資訊安全事故管理效能

測量構面辨識	
測量構面名稱	資訊安全事故管理效能
事故識別碼	特定組織
測量構面目的	評估資訊安全事故管理的效能
控制措施/流程目標	使之能夠迅速安全事故偵測與回應安全事故
控制措施(1)/流程(1)	4.2.2 h [27001:2005]
測量與屬性的目標	
測量目標	ISMS
屬性	個別事故
基本度量值等級 (1)	
基本度量值	預定人數上限
測量方法	資訊安全事故報告產出的日期的事故計次
測量方法類型	客觀的
等級	數值
等級類型	比率
測量單元	員工
延伸測量規格	
延伸測量	事故超出門檻界線
測量功能	門檻界線內的總事故數之比較
指標等級	
指標	折線圖所描繪連續水平線說明門檻數字對事故總數超過幾個報告期間

分析模型	紅色：當事故總數超過門檻界線（超過線）；黃色：當事故總數的 10%以內的門檻界線；綠色：當事故總數低於門檻界線的 10%以上或更多
決策標準等級	
決策標準	紅色 – 干預是必需的，必須進行因果關係的分析來找出不遵守和表現不佳的原因 黃色 – 此指標應密切關注，免於下降到紅色值 綠色 – 無須任何行動
測量結果	
指標詮釋	兩次報告循環若觀察到紅色值，事故管理程序的審查應該修成現有程序或者是確認額外的程序。如果在兩次報告循環中未觀察出趨勢，則須採取修正行動方案，適時提出 ISMS 範圍的延伸
報表格式	折線圖
股東	
測量委託人	ISMS 管理委員會 負責 ISMS 的經理人 安全管理 事故管理
測量審查人	負責 ISMS 的經理人
資訊擁有者	負責 ISMS 的經理人
資訊蒐集者	事故管理經理人
資訊溝通者	ISMS 管理委員會
頻率/期間	
資料蒐集頻率	每月
資料分析頻率	每月
產出測量結果	每月

報表的頻率	
測量版本	每六個月
測量期間	每月

附件 3 通訊傳播事業資訊通訊安全管理作業要點修正條文對照表(英文版)

Comparison of Revisions to the Notes on Information and Communication Security for Communication and Broadcasting Businesses

Revised rules	Current rules	Description
1. This guideline is created according to Section 3-8 of the National Communications Commission Organization Act to support the National Communication Commission's (NCC) efforts in enforcing information and communication security (ICS) to communication and broadcasting businesses.	1. This guideline is created according to Section 3-8 of the National Communications Commission Organization Act to support the National Communication Commission's (NCC) efforts in enforcing information and communication security (ICS) to telecommunication businesses.	To accommodate Section 3 of the National Communications Commission Organization Act, the governed industries were revised to: communication and broadcasting businesses. Revision to the current rules.
2. In order to enforce ICS in the communication and broadcasting industries, it is necessary to compile this Information and Communication Security Manual for Communication and Broadcasting Industries. The goals of this manual are to ensure communication security and to protect users' rights. Its contents must address the following details: (1) ICS standards. (2) Evaluating ICS levels. (3) The ICS policy. (4) ICS training. (5) ICS reports and responses. (6) Assessment on the implementation of ICS. Industry participants, experts, or any relevant institutions shall be engaged in the creation of this manual, and may be reviewed and revised depending on the implementation progress.	2. In order to enforce ICS in the telecommunication industry, it is necessary to compile this Information and Communication Security Manual for Telecommunication Industry. The goals of this manual are to ensure communication security and to protect users' rights. Its contents must address the following details: (1) ICS standards. (2) Evaluating ICS levels. (3) The ICS policy. (4) ICS training. (5) ICS reports and responses. (6) Assessment on the implementation of ICS. Industry participants, experts, or any relevant institutions shall be engaged in the creation of this manual, and may be reviewed and revised depending on the implementation progress. Once this manual has been	To accommodate Section 3 of the National Communications Commission Organization Act, the governed industries were revised to: communication and broadcasting businesses. Revision to the current rules.

Revised rules	Current rules	Description
Once this manual has been created or revised, it is subject to proper approval procedures and shall be announced on NCC's website.	created or revised, it is subject to proper approval procedures and shall be announced on NCC's website.	
3. To ensure proper data maintenance and normal system/equipment functioning in communication and broadcasting businesses, NCC shall comply with the requirements set forth in this manual and gather ICS information relating to communication and broadcasting businesses on a regular basis, thereby providing assistance, recommendations, or other appropriate guidance to communication and broadcasting businesses.	3. To ensure proper data maintenance and normal system/equipment functioning in telecommunication businesses, NCC shall comply with the requirements set forth in this manual and gather ICS information relating to telecommunication businesses on a regular basis, thereby providing assistance, recommendation, or other appropriate guidance to telecommunication businesses.	To accommodate Section 3 of the National Communications Commission Organization Act, the governed industries were revised to: communication and broadcasting businesses. Revision to the current rules.
4. Communication and broadcasting businesses based on the contents of this manual should be set "Information Security Management Implementation Plan", the template will be provided by the NCC.		added
5. NCC may request for any relevant information from, or seek opinions in the presence of, communication and broadcasting businesses when exercising ICS management over the communication and broadcasting industries. NCC will notify the communication and broadcasting business in writing or other appropriate methods before	4. NCC may request for any documents, data, or objects, or seek opinions in the presence of, or conduct site inspections at the premises of, telecommunication businesses as deemed necessary when exercising ICS management over the telecommunication industry. Before conducting the abovementioned site inspection, NCC must notify through writing	To accommodate Section 3 of the National Communications Commission Organization Act, the governed industries were revised to: communication and broadcasting businesses. 2. According to Section 4 of the Telecommunications Act: the assets and equipment owned by a telecommunication business can not be inspected, confiscated, or seized except required by law.

Revised rules	Current rules	Description
seeking opinions in the presence of eligible representatives described above. All opinions expressed must be documented, detailing the time, place, and other necessary details with the signature, seal, or finger print of the representative.	or other appropriate methods for the availability of relevant users or representatives on site. All findings of the site inspection must be documented, detailing the time, place, and other necessary details with the signature, seal, or fingerprint of the site representative. For any documents, data, or objects obtained in (1) above which the provider has requested for their return after the investigation, NCC must exercise care to ensure the integrity of all items obtained; items that do not need to be returned must be kept or handled in the appropriate manner. NCC must maintain the integrity of the inspected site and objects throughout the site inspection described in (1) above.	Deleted the list of documents and objects to be obtained, and details to be inspected on site. 3. According to Section 55 of the Telecommunication Act: NCC may request any relevant information from, or seek opinions in the presence of, telecommunication businesses, users of dedicated telecommunication services, or radio stations and their users as deemed necessary to supervise and govern the telecommunication industry. 4. Revision to the current rules.
6. To apply for investments in Mainland China, it is mandatory for communication and broadcasting businesses to present the scope of their ICS management and seek approval from NCC before approaching a NCC-recognized ICS system certifier for certification over their permitted business activities. After which, the applicants must obtain certification on ISO/IEC27001 compliance, and all additional audit focuses thereof listed in the Information and Communication Security	5. To apply for investments in the telecommunication industry in Mainland China, it is mandatory for telecommunication businesses to present the scope of their ICS management and seek approval from NCC before approaching a NCC-recognized ICS system certifier for certification over their permitted business activities. After which, the applicants must obtain certification on ISO/IEC27001 compliance, and all additional audit focuses thereof listed in the Information and Communication Security	To accommodate Section 3 of the National Communications Commission Organization Act, the governed industries were revised to: communication and broadcasting businesses. The revision was based on "Prohibited Business Activities for Investors and Service Providers under Technological Co-operation Arrangements in Mainland China": The following is a list of principles for reviewing investments in the telecommunication industry

Revised rules	Current rules	Description
Manual for Communication and Broadcasting Industries. Any processes, departments, business functions, and systems involving the use of personal data, such as the databases, customer service systems/centers, accounts systems/centers incorporated by telecommunication businesses, cannot be relocated or established in Mainland China, either through means of investment or business co-operation. To apply for the the joint operation of telecommunication businesses in Mainland China, as permitted under Section 70-1-2 or Section 72-1 of the Regulations for Administration Fixed Network Telecommunications Businesses, it is mandatory for telecommunication businesses to approach a NCC-recognized ICS system certifier for certification over their permitted business activities before the system inspection. After which, the applicants must obtain certification on ISO/IEC27001 compliance, and all additional audit focuses thereof listed in the Information and Communication Security Manual for Telecommunication and Broadcasting Industries.	Manual for Telecommunication Industry. To apply for the the joint operation of telecommunication businesses in Mainland China, as permitted under Section 70-1-2 or Section 72-1 of the Regulations for Administration Fixed Network Telecommunications Businesses, it is mandatory for telecommunication businesses to approach a NCC-recognized ICS system certifier for certification over their permitted business activities before the system inspection. After which, the applicants must obtain certification on ISO/IEC27001 compliance, and all additional audit focuses thereof listed in the Information and Communication Security Manual for Telecommunication and Broadcasting Industries.	(general activities of Type II telecommunication business): (1) Currently, investments in the general activities of Type II telecommunication business in Mainland China are only applicable to the so-called "message storage/forwarding, message services, online data processing, Internet data centers, and Internet connection services". (2) All Taiwanese businesses investing in Mainland China must present proof of ISO 27011 certification, which governs the implementation of ISMS by telecommunication businesses. (3) Any processes, departments, business functions, and systems involving the use of citizens' personal data, such as user databases, customer service systems/centers, accounts systems/centers incorporated by telecommunication businesses, cannot be relocated or established in Mainland China, either through means of investment or business co-operation. (4) All Taiwanese businesses investing in Mainland China are prohibited from offering exclusive technologies, patents, copyrights, or other technology-related properties in place of cash capital.
7. NCC shall publish on its website a list of NCC-recognized	6. NCC shall publish on its website a list of NCC-recognized	

Revised rules	Current rules	Description
ICS system certifiers.	ICS system certifiers.	
8. NCC shall publish on its website a list of ICS-certified communication and broadcasting businesses on a regular basis.	7. NCC shall publish on its website a list of ICS-certified telecommunication businesses on a regular basis.	To accommodate Section 3 of the National Communications Commission Organization Act, the governed industries were revised to: communication and broadcasting businesses. Revision to the current rules.

通訊傳播事業資通安全管理手冊
(修訂建議草案)

國家通訊傳播委員會

中華民國 100 年 11 月　日

目　　次

一、依據.....附件 3-1
二、目的.....附件 3-1
三、要項說明.....附件 3-2
（一）資通安全管理標準.....附件 3-2
（二）資通安全等級評估.....附件 3-2
（三）資通安全管理機制.....附件 3-4
（四）資通安全認知訓練.....附件 3-6
（五）個人資料保護.....附件 3-6
（六）資通安全應變通報.....附件 3-7
（七）資通安全實施評鑑.....附件 3-7
（八）年度提報資料要求.....附件 3-8
四、附錄.....附件 3-10
附錄 1　通訊傳播事業資通安全等級自我評估彙整表 .....附錄 1-1
附錄 2　通訊傳播事業資通安全等級自我評估說明表 .....附錄 2-1
附錄 3　通訊傳播事業資通安全管理詳細風險評鑑表 .....附錄 3-1
附錄 4　通訊傳播事業資通安全管理機制實施計畫參考範本 .....附錄 4-1
附錄 5　資通安全管理實施計畫應執行工作事項表 .....附錄 5-1
附錄 6　通訊傳播事業資通安全管理內部稽核表(修訂對照).....附錄 6-1
附錄 7　通訊事業增項稽核表 .....附錄 7-1
附錄 8　傳播事業增項稽核表 .....附錄 8-1
附錄 9　個人資料保護安全控制措施 .....附錄 9-1
附錄 10　國家通訊傳播委員會資通安全事故通報單 .....附錄 10-1
附錄 11　資通安全管理矯正／預防措施一覽表.....附錄 11-1
附錄 12　資通安全管理矯正／預防措施單 .....附錄 12-1
附錄 13　內部稽核表檢查項目勾選不適用之說明 .....附錄 13-1
附錄 14　增項稽核表檢查項目勾選不適用之說明 .....附錄 14-1

通訊傳播事業資通安全管理手冊

一、依據

本手冊依通訊傳播事業[1]資訊通訊安全管理作業要點第二點之規定訂定之，主要為提供產業規範，輔導目的事業逐漸落實資通安全管理機制。

另電信法增訂第五十六條：為確保電信事業系統設備、資料及網路之安全，保障民眾通信權益，電信事業應辦理下列事項：

一、建立資通安全管理機制。

二、建立資通安全防護及偵測設施。

三、建立資通安全聯防及資通安全事件之通報、處理、回報等應變措施。

建議通訊傳播事業宜提早因應，建立企業風險文化，履行法定義務。

二、目的

基於保障資通安全[2]及維護使用者權益原則，確保通訊傳播[3]系統設備、資料及網路安全，本手冊包含下列要項：

（一）資通安全管理標準。

（二）資通安全等級評估。

（三）資通安全管理機制及教育訓練。

（四）資通安全應變通報。

（五）資通安全實施評鑑。

（六）年度提報資料要求。

[1] 通訊傳播事業：指經營通訊傳播業務者

[2] 資訊通訊安全簡稱資通安全或資安。

[3] 通訊傳播：指以有線、無線、衛星或其他電子傳輸設施傳送聲音、影像、文字或數據者

三、要項說明

（一）資通安全管理標準

通訊傳播事業實施資通安全管理，建議參照下列 CNS 國家標準或是 ISO/IEC 27000 系列國際標準，建立目的事業之資通安全管理機制：

1、資訊安全管理系統要求事項：CNS/ISO/IEC 27001

2、資訊安全管理作業規範：CNS/ISO/IEC 27002

3、資訊安全管理系統實施指引：ISO/IEC 27003

4、資訊安全管理測量方法： ISO/IEC 27004

5、資訊安全管理風險管理：CNS/ISO/IEC 27005

6、電信事業資訊安全管理實作指引：ISO/IEC 27011

（二）資通安全等級評估

1、通訊傳播事業宜依據下列步驟，實施高階風險評鑑作法(High-Level Risk Assessment)，評估資通安全等級，以定義資通安全範圍與邊界，確定資通安全需求水準，作為後續訂定風險處理優先順序之參考：

（1）依據執照核發之營業項目範圍內，調查通訊傳播事業營運所需之資產群組，若組織規模龐大者，得區分為不同之事業體或是部門，區分為以下三大類，分別進行資產群組之調查：

- 關鍵業務：包含下列項目：

  電信事業之電信設備、電信機線設備、微波電台、管線基礎設施及電信終端設備等。

  有線廣播電視事業之頭端、信號處理設備、分配線網路、分配中心、光纖投落點及訂戶終端設備等。

  無線廣播(電視)事業之電臺、轉播站、節目中繼電臺、纜

線、信號處理設備等。

衛星廣播電視事業之地球電臺、衛星機構、衛星轉頻器等。

- 支援業務：指廣播電視節目供應業務、第二類電信轉售服務業務及支援通訊傳播事業營運所需之資訊處理設施，但非屬關鍵業務者，例如：客戶服務、帳務、會計系統，或是涉及客戶個人資料蒐集、處理及利用者。
- 行政業務：指通訊傳播事業內部輔助單位之業務項目，例如：人事、行政、總務等。

（2）依據每一資產群組失效後之「衝擊影響程度」，評估資產安全等級，決定資通安全管理機制改善之優先順序，並每年定期更新。

（3）填寫「通訊傳播事業資通系統安全等級自我評估彙整表」（詳見附錄 1）及「通訊傳播事業資通安全等級自我評估說明表」（詳見附錄 2）。

2、評估資通安全等級步驟如下：

（1）需將支援通訊傳播事業營運所需之「關鍵業務」、「支援業務」及「行政業務」等資產群組全部納入，決定資產安全等級，逐步建立資訊安全管理機制。

（2）針對每個資產群組依「影響業務運作」、「資料保護受到損害」、及「法律規章之遵循」等之影響構面，分別評定各影響構面之資產安全等級，區分為普、中、高三級。

（3）資產群組失效之衝擊影響程度，依據各影響構面，採用最高原則方式處理，當有任一影響構面之衝擊影響程度為「高」者，則該資產群組之資產安全等級應評估為「高」；如全部影響構面之衝擊影響程度均為「普」者，該資產群組之資產安全等級則評估為「普」。

（4）最後將所有經評定資產群組之資產安全等級彙整，取其最高者，

作為評定企業安全等級之依據，區分為 A、B、C 三級，如最高之資產群組資通安全等級為「高級」者，其企業安全等級為「A」級；如最高之資產群組資通安全等級為「中級」者，其企業安全等級為「B」級；如最高之資產群組資通安全等級為「普級」者，其企業安全等級為「C」級。

（三）資通安全管理機制

1、通訊傳播事業之資產群組，其資產安全等級經評定為「高」級者，得視需要參考 CNS/ISO/IEC 27005 標準，進一步實施詳細風險評鑑(Detailed Risk Assessment)(詳見附錄 3)或是自行定義其風險管理作法，以決定風險處理策略。

2、通訊傳播事業應依自我評估之資通安全等級，訂定資通安全管理實施計畫，並每年定期進行內部稽核乙次（資通安全管理實施計畫範本，詳見附錄 4）：

3、通訊傳播事業應依照「資通安全管理實施計畫應執行工作事項表」（附錄 5）之企業安全等級，規劃資通安全管理實施計畫，每年應執行下列工作事項：

（1）防護縱深

- 企業安全等級為「A」級者，防護縱深至少應建置包括防火牆、入侵偵測系統（Intrusion Detection System，IDS）、入侵防禦系統（Intrusion Prevention System，IPS）、防毒軟體、垃圾郵件過濾、網頁過濾管控設備、網路安全監控等設備，其安全等級至少應符合「資通設備安全審驗作業要點（草案）」進階型設備之要求。
- 企業安全等級為「B」級者，防護縱深至少應包括防火牆、IDS、IPS、防毒軟體、垃圾郵件過濾等設備，其安全等級至少應符合「資通設備安全審驗作業要點（草案）」基礎型設備之要求。

- 企業安全等級為「C」級者，防護縱深至少應包括防火牆、IDS、IPS、防毒軟體、垃圾郵件過濾等設備。

（2）推動方式

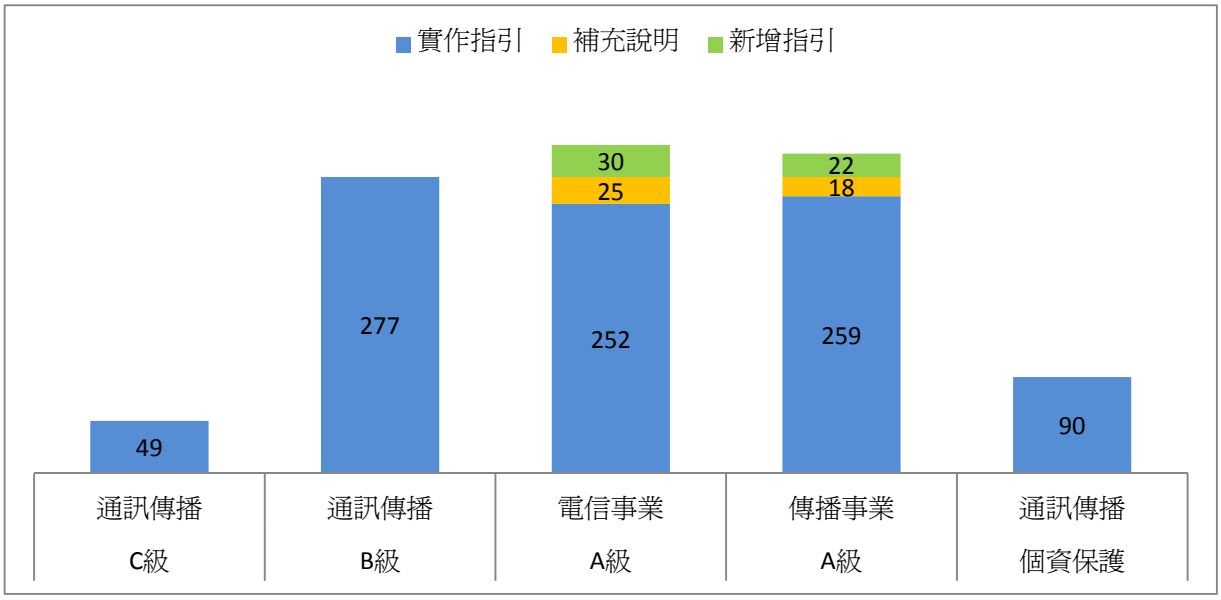


圖 1 通訊傳播事業資通安全等級適用之安全防護基準

通訊傳播事業應成立資安推動小組，建立資通安全管理機制，將企業安全等級區分為「A」、「B」、「C」三級，以選擇適用之安全基準，詳見圖 1 所示。

- 企業安全等級評定為「C」級者，應實施「資通安全管理內部稽核表」(詳見附錄 6)之最小限安全需求項目。
- 企業安全等級評定為「B」級者，應實施「資通安全管理內部稽核表」之全部控制措施。
- 企業安全等級評定為「A」級者，除實施前述「資通安全管理內部稽核表」之全部控制措施外，另依據產業別，實施適用之「通訊事業增項稽核表」(詳見附錄 7)或「傳播事業增項稽核表」(詳見附錄 8)，並以通過資訊安全管理系統第三方驗證為目標，逐年改善最終及於全企業。
- 適用於個人資料檔案保護之資安控制措施，詳見附錄 9 所示。

（3）稽核方式

- 每年至少執行一次內部稽核。
- 已通過資訊安全管理系統驗證之資產群組，應定期維持更新及辦理稽核工作。

（四）資通安全認知訓練

為建立通訊傳播事業員工正確資通安全認知、提升安全防護水準，應推動內部資通安全教育訓練，並依照附錄 5，規劃每年應辦理之資通安全教育訓練及宣導時數如下：

主管、資通訊人員、業務人員及一般人員，每年至少須分別達到 3、12、6、3 小時之資通安全認知訓練。

（五）個人資料保護

1、資通安全管理實施計畫範圍內，若涉及個人資料蒐集、處理及利用者，應依據個人資料保護法之規定，訂定「個人資料檔案安全維護計畫」及「業務終止後個人資料處理方法」，採行適當安全維護措施，並保存適當之個人資料蒐集、處理及利用之活動稽核記錄，證明已盡管理之責任。

2、上開所稱適當安全維護措施或安全維護事項或適當之安全措施，係指通訊傳播事業為防止個人資料被竊取、竄改、損毀、滅失或洩漏，採取技術上與組織上之必要措施。包括下列事項：

(1) 成立管理組織，配置相當資源。

(2) 界定個人資料之範圍。

(3) 個人資料之風險評估及管理機制。

(4) 事故之預防、通報及應變機制。

(5) 個人資料蒐集、處理及利用之內部管理程序。

(6) 資料安全管理及人員管理。

(7) 認知宣導及教育訓練。

(8) 設備安全管理。

(9) 資料安全稽核機制。

(10)必要之使用紀錄、軌跡資料及證據之保存。

(11)個人資料安全維護之整體持續改善。

(12)其他安全維護事項，如業務終止後個人資料處理方法等。

前述之必要措施，以所須支出之費用，與所欲達成之個人資料保護目的，符合適當比例者為限。

3、受通訊傳播事業委託蒐集、處理或利用個人資料者，於個資法適用範圍內，視同委託機關。委託人應對受託人為適當之監督，包含下列事項，定期確認受託人執行之狀況，並將確認結果記錄之：

(1) 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。

(2) 受託人應採取之適當安全維護措施。

(3) 有複委託者，其約定之受託人。

(4) 受託人或其受僱人違反個人資料保護法規或委託契約條款時，應向委託人通知之事項及採行之補救措施。

(5) 委託人對受託人保留指示之事項。

(6) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。

（六）資通安全應變通報

通訊傳播事業應建立資通安全事故應變作業機制，當發生資通安全事故時，應立即填具「國家通訊傳播委員會資通安全事故通報單」(附錄 10)向本會通報，並採取應變措施。

（七）資通安全實施評鑑

1、內部稽核

通訊傳播事業每年應自我評估資產群組安全等級，選擇適用之安全控制措施，至少執行一次內部稽核，並將稽核結果依規定填寫於本手冊

之相關附錄：

通訊傳播事業依附錄 6、7、8 執行內部稽核時，須填具附錄如下：

（1）檢查項目勾選「是」者，須檢附相關佐證資料。

（2）檢查項目勾選「否」者，須填具「資通安全管理矯正／預防措施一覽表」（附錄 11）及「資通安全管理矯正／預防措施單」（附錄 12）。

（3）檢查項目勾選「不適用」者，須填具「內部稽核表檢查項目勾選不適用之說明」（附錄 13）。「增項稽核表檢查項目勾選不適用之說明」（附錄 14）

2、外部驗證

通訊傳播事業鼓勵向辦理資通安全管理系統驗證之機構申請外部驗證，其申請驗證範圍應符合資通安全管理系統 CNS/ISO/IEC 27001 標準及本手冊附錄 7、8 之規定。

前項驗證機構須經本會認可之本國認證體系認證核可，經驗證合格之通訊傳播事業，本會將於網站上公布。

3、行政檢查

通訊傳播事業如發生附錄 10 之資通安全事故影響等級為 3 級或 4 級者，依其自我評估之資通安全等級，須於 1 週內備妥下列相關資料，以供本會行政檢查之用。

（1）重大資安事故應變措施之處理說明。

（2）資通安全管理實施計畫。

（3）附錄 11 至附錄 13、各檢查項目之佐證資料、或經本會認可之資通安全管理機制驗證機構產出之稽核報告。

（八）年度提報資料要求

1、各通訊傳播事業應於每年 9 月底前，依其自我評估之資通安全等級，提報下列資料至本會：

（1）附錄 1、附錄 2、附錄 6、附錄 7 及附錄 8，擁有個資檔案者，需提報附錄 9。

（2）依要項說明三（六）執行內部稽核，勾選檢查項目「否」者，須提報附錄 11 及附錄 12。

（3）依要項說明三（六）執行內部稽核，勾選檢查項目「不適用」者，須提報附錄 13 及附錄 14。

2、通訊傳播事業經本會認可之資通安全管理機制驗證機構進行外部驗證，並取得 CNS/ISO/IEC 27001 證明者，僅須提報附錄 1、附錄 2、附錄 7(或附錄 8)及附錄 14，擁有個資檔案者另需提報附錄 9，得免提報附錄 6 及附錄 13，惟須檢附該驗證證書及驗證報告等相關資料影本。

3、通訊傳播事業經本會認可之資通安全管理機制驗證機構進行外部驗證，並取得 ISO/IEC 27001 標準及附錄 7(或附錄 8)ISO/IEC 27011 增項稽核表驗證合格證明者，僅須提報附錄 1 及附錄 2，擁有個資檔案者另需提報附錄 9，得免提報附錄 6 至附錄 14，惟須檢附該驗證證書及驗證報告等相關資料影本。各項提報資料，詳見下表所示。

年度提報資料統計表

區分	內部稽核	外部驗證 CNS/ISO/IEC 27001	外部驗證 ISO/IEC 27011 增項
附錄 1. 通訊、傳播事業資通安全等級自我評估彙整表	**V**	**V**	**V**
附錄 2.通訊、傳播事業資通安全等級自我評估說明表	**V**	**V**	**V**
附錄 6.資通安全管理內部稽核表	**V**		
附錄 7.通訊事業增項稽核表	**⊙**	**⊙**	

區分	內部稽核	外部驗證 CNS/ISO/IEC 27001	外部驗證 ISO/IEC 27011 增項
附錄 8.傳播事業增項稽核表	⊙	⊙	
附錄 9.個人資料檔案保護之安全控制措施	⊙	⊙	⊙
附錄 11.資通安全管理矯正／預防措施一覽表	⊙		
附錄 12.資通安全管理矯正／預防措施單	⊙		
附錄 13.內部稽核表檢查項目勾選不適用之說明	⊙		
附錄 14.增項稽核表檢查項目勾選不適用之說明	⊙	⊙	
備註：V 必須提報項目　⊙視需要提報項目			

四、附錄

附錄 1　通訊傳播事業資通安全等級自我評估彙整表

附錄 2　通訊傳播事業資通安全等級自我評估說明表

附錄 3　通訊傳播事業資通安全管理詳細風險評鑑表

附錄 4　通訊傳播事業資通安全管理機制實施計畫參考範本

附錄 5　資通安全管理實施計畫應執行工作事項表

附錄 6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

附錄 7　通訊事業增項稽核表

附錄 8　傳播事業增項稽核表

附錄 9　個人資料保護安全控制措施

附錄 10　國家通訊傳播委員會資通安全事故通報單

附錄 11　資通安全管理矯正／預防措施一覽表

附錄 12　資通安全管理矯正／預防措施單

附錄 13　內部稽核表檢查項目勾選不適用之說明

附錄 14　增項稽核表檢查項目勾選不適用之說明

附錄 1　通訊傳播事業資通安全等級自我評估彙整表

公司名稱			
單位主管		評估日期：	
評估人員		評估日期：	
聯絡窗口	電話：	傳真：	行動：
	Email：		

資產群組	業務類別	影響構面／影響等級（註二）			資產安全等級
		影響業務運作	資料保護受到損害	法律規章之遵循	
	□關鍵業務	□高	□高	□高	□高
	□支援業務	□中	□中	□中	□中
	□行政業務	□普	□普	□普	□普
	□關鍵業務	□高	□高	□高	□高
	□支援業務	□中	□中	□中	□中
	□行政業務	□普	□普	□普	□普
	□關鍵業務	□高	□高	□高	□高
	□支援業務	□中	□中	□中	□中
	□行政業務	□普	□普	□普	□普

企業安全等級：　□A 級　□B 級　□C 級

（本表可視需要自行延伸）

附錄 1 之填表說明

註一：評估資通安全管理作業範圍之業務類別

業務類別	說明
關鍵業務	電信事業之電信機線設備、微波電台、管線基礎設施及電信終端設備等。 有線廣播電視事業之頭端、信號處理設備、分配線網路、分配中心、光纖投落點及訂戶終端設備等。 無線廣播(電視)事業之電臺、轉播站、節目中繼電臺、纜線、信號處理設備等。 衛星廣播電視事業之地球電臺、衛星機構、衛星轉頻器等。
支援義務	支援業務：指廣播電視節目供應業務、第二類電信轉售服務業務及支援通訊傳播事業營運所需之資訊處理設施，但非屬關鍵業務者，例如：客戶服務、帳務、會計系統，或是涉及客戶個人資料蒐集、處理及利用者。
行政業務	行政業務：指通訊傳播事業內部輔助單位之業務項目，例如：人事、行政、總務等

註二：影響構面／資產安全等級

安全等級 影響構面	普 （等級 1）	中 （等級 2）	高 （等級 3）
1. 影響業務運作	● 系統可容忍之中斷時間較長（如：超過 4 小時或是 8 小時以上以上） ● 系統故障對社會秩序、民生體系運作不致造成影響或僅有輕微影響	● 系統可容忍之中斷時間短（如：1 小時或是 4 小時以內） ● 系統故障對社會秩序、民生體系運作將造成嚴重影響 ● 系統故障將造成關鍵業務執行效能嚴重降低	● 系統可容忍之中斷時間非常短（如：1 分鐘或是 10 分鐘以內） ● 系統故障對社會秩序、民生體系運作將造成非常嚴重影響，甚至危及國家安全 ● 系統故障將造成關鍵業務執行效能非常嚴重降低，甚至業務停頓
2. 資料保護受到損害	● 一般性資料 ● 資料若外洩或遭竄	● 敏感性資料 ● 資料若外洩或遭竄	● 機密性資料 ● 資料若外洩或遭竄

安全等級 影響構面	普 （等級 1）	中 （等級 2）	高 （等級 3）
	改，不致影響個人權益或僅導致個人權益輕微受損	改，將導致個人權益嚴重受損之資料	改，將導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損
3. 法律規章之遵循	系統運作、資料保護、資訊資產使用等，若未遵循相關規範辦理，不會導致機關違反法規命令。	系統運作、資料保護、資訊資產使用等，若未遵循相關規範辦理，將導致機關違反法規命令，並伴隨輕微後果，如：行政處分或罰鍰等	系統運作、資料保護、資訊資產使用等，若未依循相關規範辦理，將導致機關從根本上違反法律，並導致嚴重不良後果，如：損害賠償、罰金或是刑責

附件 4

附錄 2　通訊傳播事業資通安全等級自我評估說明表

公司名稱				
單位主管		評估日期：		
評估人員		評估日期：		
聯絡窗口	電話：	傳真：	行動：	
	Email：		頁次：第　頁/共　頁	

資產群組	業務類別	影響構面	資產安全等級 普、中、高		原　因　說　明
	□關鍵業務 □支援業務 □行政業務	影響業務運作	前一年度		
			本年度		
		資料保護受到損害	前一年度		
			本年度		
		法律規章之遵循	前一年度		
			本年度		
			本年度		
（本表可視需要自行延伸）	□關鍵業務 □支援業務 □行政業務	影響業務運作	前一年度		
			本年度		
		資料保護受到損害	前一年度		
			本年度		
		法律規章之遵循	前一年度		
			本年度		
企業安全等級	□ A 級　□ B 級　□ C 級				

附件 4

附錄3 通訊傳播事業資通安全管理詳細風險評鑑表

NO.	部門	保管人	說明	資訊資產	資產類別	數量	機密性	完整性	可用性	資訊資產價值	威脅	脆弱性	風險估計			
													威脅等級	脆弱等級	風險值	風險等級
					資訊紀錄		中	中	中	6	未授權存取資料	網路存取規劃不當。	2	3	36	中

<公司全銜>資通安全管理實施計畫

文件編號： ISMS-1-001

版　　次： 1.0

文件日期： 100 年 11 月 1 日

機密等級： 限　閱

公司 LOGO

文件制/修訂紀錄

制(修)訂版次	制(修)訂日期	制(修)訂說明	作者	備註
V1.0	1001101	初版發行	資通安全管理推動小組	

目　　錄

壹、　資通安全政策 1

一、　資通安全目標 1
二、　目標的執行 1

貳、　法規命令之要求 3

一、　電信法 3
二、　個人資料保護法 3

參、　資通安全管理組織 3

肆、　資通安全管理範圍 4

一、　資通安全等級評估 5
二、　評估資通安全等級步驟 7

伍、　資通安全管理機制 7

一、　一般要求 7
二、　風險評鑑作法 8
三、　執行工作事項 8
四、　推動方式 9
五、　稽核方式 11
六、　資通安全認知訓練 11
七、　資通安全應變通報 11
八、　資通安全實施評鑑 11
九、　年度提報資料要求 12

陸、　資通安全文件管理 13

一、　一階文件 14
二、　二階文件 14
三、　三階文件 14
四、　四階文件 15
五、　資通安全文件之核定 15

柒、　附件 15

壹、 資通安全政策

本公司以「客戶為尊、服務第一、積極創新、持續成長」為具體目標，持續推出資、通訊市場整合型服務，亦致力於發展相關行動應用商品，更積極強化優質門市服務品質，為消費者打造無所不在的行動生活。

從「人性」出發，以「客戶」為服務核心，持續強化核心能力，並透過結盟、合作，積極開發行動商務、網路應用，以及寬頻影音多媒體等新穎服務，擴大電信網路與資訊科技整合運用效果，使本公司之服務成為社會大眾的生活好幫手，以及廣大企業的經營好伙伴。

為強化資訊安全管理、確保資通訊資產的機密性、完整性與可用性、強化全體同仁對資訊安全之認知，依據主管機關頒定之「通訊傳播事業資通安全管理作業手冊」(以下簡稱「資安管理手冊」)及相關國家、國際資安標準規範，特制定本「資通安全管理實施計畫」，其政策目標如下：

一、 資通安全目標

（一）提昇企業經營競爭力

（二）降低資通安全之風險

（三）改善資通安全管理效率

二、 目標的執行

(一) 推動資通安全是管理問題，必須由高層主管支持與參與，各單位主管應督導部屬，協助達成本公司資通安全目標。

（二）全體同仁應充分了解資通安全管理制度的重要性，建立使命感，積極推動。

（三）確保資通訊資產的機密性、完整性及可用性，防止敏感性資料與客戶個人資料不當揭露。

（四）各項資通安全防護及管理規定，應符合主管機關法規命令及相關資通安全政策之要求。

（五）提供資安相關教育訓練，建立資訊安全認知，培養資訊安全管理技能。

（六）依據執照核發之營業項目範圍，得區分為不同之事業體或是部門，調查營運所需之資產群組，依據主管機關資通安全等級評估方法，進行衝擊分析與風險評鑑，以選定適當之導入範圍。

（七）導入範圍內之資通訊資產應予適當保護，採行合宜之安全控制措施，並定期演練前項備援回復作業。

(八) 所有資訊安全事故或可疑之安全弱點，應即時依程序通報反映，並予以適當調查及處理。

（九）發現資安議題應即時研商對策，謀求改善機制，健全資訊安全管理制度。

(十) 透過稽核程序，找出資安問題，提出改善建議，降低資安風險。

(十一) 違反本政策與資訊安全相關規範，依法令或本公司懲戒規定辦理

(十二) 提供委外廠商及第三方團體必要之資通安全技術協助。

(十三) 須考量時間與資源，列出優先順序，逐步推展最終及於全公司，並申請通過外部驗證，驗證範圍應符合資通安全管理系統 CNS/ISO/IEC 27001 標準及主管機關之規定。

(十四) 本政策應每年定期評估檢討，以反映政府法令、技術發展及業務需求等，以落實資通安全作業。

(十五) 本政策須經資通安全管理推動小組審議通過，奉董事長核定後實施，修正時亦同。

貳、 法規命令之要求

以下法規命令之要求，公司全體同仁宜提早因應，以建立企業風險文化，履行法定義務：

一、 電信法

第五十六條增修條文　為確保電信事業系統設備、資料及網路之安全，保障民眾通信權益，電信事業應辦理下列事項：

（一）建立資通安全管理機制。

（二）建立資通安全防護及偵測設施。

（三）建立資通安全聯防及資通安全事件之通報、處理、回報等應變措施。

二、 個人資料保護法

第二十七條　非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

參、 資通安全管理組織

本公司由負責稽核業務之主管擔任資訊安全長，納編各部門之副主管成立資通安全管理推定小組，組織架構詳見圖 1所示，負責推動以下工作：

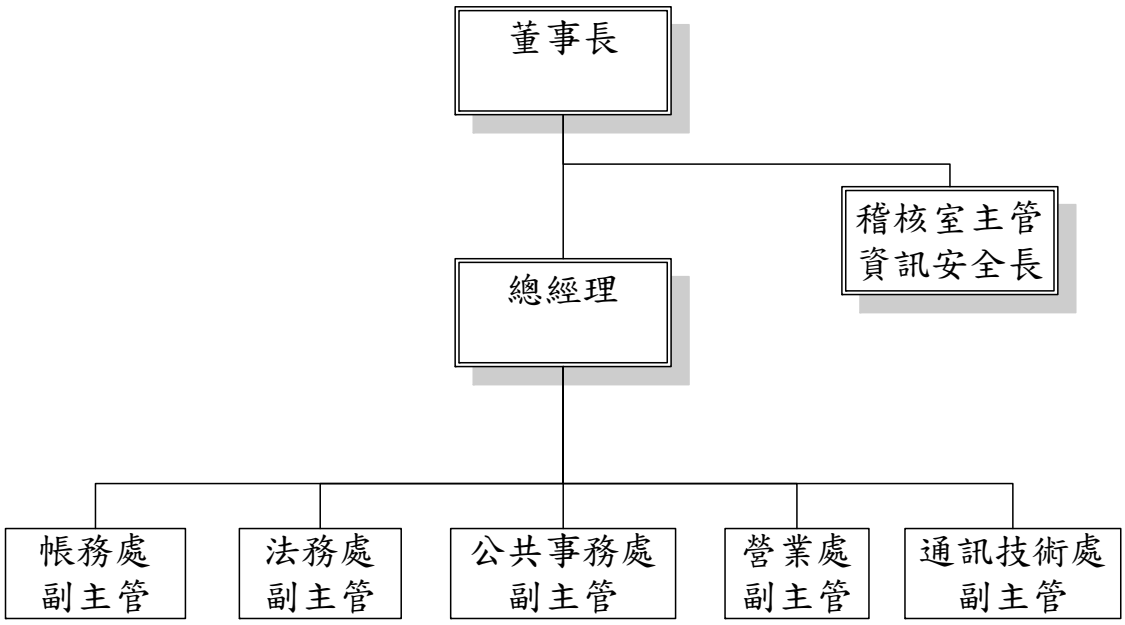


圖1　本公司資通安全推動小組組織架構圖

(1) 關於資訊安全政策訂定研議事項。

(2) 關於資訊安全組織權責分工協調事項。

(3) 關於資訊資產安全管理研議事項。

(4) 關於人員管理及資訊安全教育訓練研議事項。

(5) 關於實體與環境安全管理研議事項。

(6) 關於通信與作業管理研議事項。

(7) 關於存取控制管理研議事項。

(8) 關於系統獲取、開發及維護安全管理研議事項。

(9) 關於資訊安全事故管理研議事項。

(10) 關於營運持續管理計畫研議事項。

(11) 關於法規遵循之研議事項。

(12) 其他資訊安全管理事項研議事項。

(13) 辦理並執行資訊安全管理系統相關事務。

肆、 資通安全管理範圍

依據本公司執照核發之營業項目範圍內，調查營運所需之資產群組，進行資

通安全等級評估。

一、 資通安全等級評估

區分為以下三大類業務項目，若規模龐大者，得區分為不同之事業體或部門，分別進行資產群組之調查。

(一) 關鍵業務

1. 第一類電信

指本公司第一類電信執照核定範圍內之電信機線設備、微波電台、管線基礎設施及電信終端設備等，包含以下業務：

- 固定通信網路業務
- 行動通信網路業務
- 衛星通信網路業務

2. 第二類電信

指本公司第二類電信執照核定範圍內之電信機線設備及電信終端設備等，包含以下業務：

- 數據交換通信服務
- 網際網路接取服務
- 非Ｅ·１６４ 網路電話服務
- Ｅ·１６４ 網路電話服務
- 公司內部網路通信服務
- 語音會議服務
- 存取網路服務
- 視訊會議服務

3. 傳播事業

指本公司傳播執照核定範圍之頭端、信號處理設備、分配線網路、分配中心、光纖投落點及訂戶終端設備、電臺、轉播站、節目中

繼電臺、纜線、信號處理設備、地球電臺、衛星機構、衛星轉頻器等，包含以下業務：

- 有線廣播電視
- 廣播電視
- 衛星廣播電視

(二) 支援業務

1. 第二類電信轉售業務

指本公司第二類電信執照核定範圍內之轉售服務業務及支援營運所需之資訊處理設施，包含以下業務項目：

- 語音單純轉售服務
- 批發轉售服務
- 頻寬轉售服務
- 存轉網路服務
- 付費語音資訊服務
- 行動轉售服務
- 行動轉售及加值服務

2. 廣播電視節目供應業務

指本公司廣播電視節目供應業務之資訊處理設施，包含：客戶服務、帳務、會計系統，及所有相關客戶個人資料蒐集、處理及利用之系統。

(三) 行政業務

指本公司內部輔助單位之業務項目，例如：人事、行政、總務等部門。

依據每一資產群組失效後之「衝擊影響程度」，評估資通安全等級，決定資通安全管理機制改善之優先順序，並每年定期更新。

評估後須填寫「資通系統安全等級自我評估彙整表」(詳見資安管理手冊

附錄 1）及「資通安全等級自我評估說明表」（詳見資安管理手冊附錄 2）。

二、 評估資通安全等級步驟

(一) 需將支援營運所需之「關鍵業務」、「支援業務」及「行政業務」等資產群組全部納入，區分優先順序，逐步建立資訊安全管理機制。

(二) 針對每個資產群組依「影響業務運作」、「資料保護受到損害」、及「法律規章之遵循」等之影響構面，分別評定各影響構面之資產安全等級，區分為普、中、高三級。

(三) 資產群組失效之衝擊影響程度，依據各影響構面，採用最高原則方式處理，當有任一影響構面之衝擊影響程度為「高」級者，則該資產群組之資通安全等級應評估為「高」級；如全部影響構面之衝擊影響程度均為「普」級者，該資產群組之資通安全等級則評估為「普」級。

(四) 最後將所有經評定資產群組之資產安全等級彙整，取其最高者，作為評定本企業安全等級之依據，區分為 A、B、C 三級，如最高之資產群組資通安全等級為「高級」者，其企業安全等級為「A」級；如最高之資產群組資通安全等級為「中級」者，其企業安全等級為「B」級；如最高之資產群組資通安全等級為「普級」者，其企業安全等級為「C」級。

伍、 資通安全管理機制

一、 一般要求

本公司依據整體營運活動與所面臨的風險，建立、實作、運作、監視、

審查、維持與改進資通安全，資通安全管理機制採用之 PDCA(Plan, Do, Check, Act)過程模型，詳見圖 2所示，並依據主管機關頒布之「通訊傳播事業資通安全管理作業手冊」之規定，建立本公司之資通安全管理機制。

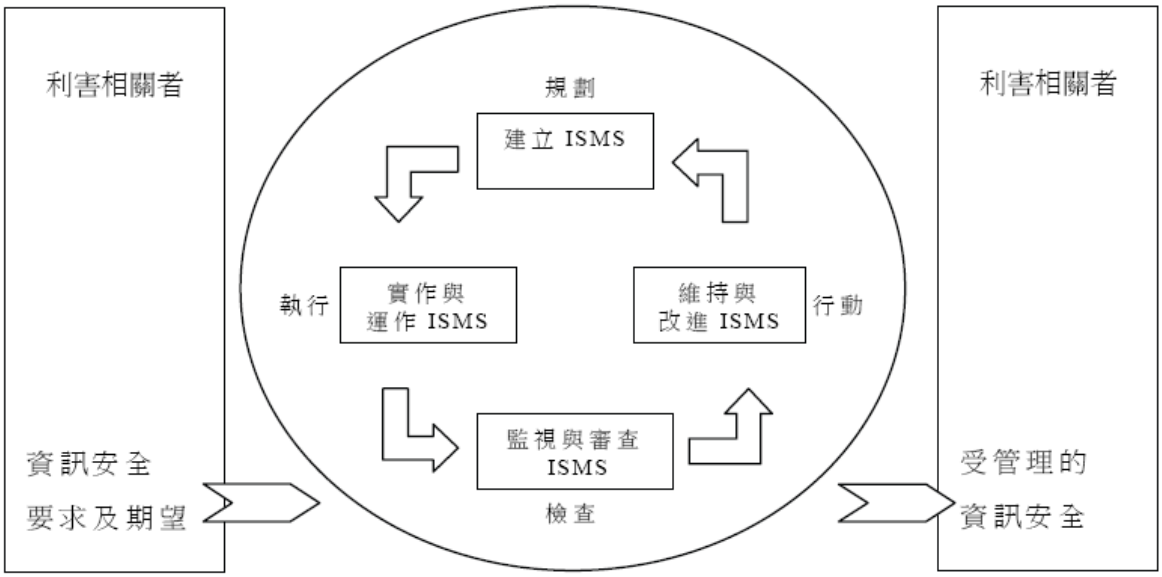


圖2　資通安全管理機制採用之 PDCA 過程模型

二、 風險評鑑作法

前項資產群組其安全等級經初步評定為「高」級者，得視需要參考 CNS/ISO/IEC 27005 標準，進一步實施詳細風險評鑑(Detailed Risk Assessment)，以決定風險處理策略（詳見資安管理手冊附錄 3）。

三、 執行工作事項

前項資產群組其安全等級經本公司核定後，應依據核定之資通安全等級，完成以下工作事項，詳見表 1所示：

表1　資通安全管理實施計畫應執行工作事項表

作業名稱 / 內容 / 等級	資訊處理設施防護縱深	推動方式	稽核方式	資安教育訓練時數（主管、資通訊人員、業務人員、一般人員）	個資保護
A 級	防火牆、IPS、IDS、防毒軟體、垃圾郵件過濾、網頁過濾管控設備、網路安全監控等設備，其安全等級至少應符合「資通設備安全審驗作業要點（草案）」進階型設備之要求。	以通過資訊安全管理系統第三方驗證為目標	每年至少執行一次內部稽核	每年至少達到（3、12、6、3）小時	涉及個人資料保護者應依據個資法施行細則，訂定個人資料檔案安全維護計畫，採取適當安全維護措施。
B 級	防火牆、IDS、IPS、防毒軟體、垃圾郵件過濾等設備，其安全等級至少應符合「資通設備安全審驗作業要點（草案）」基礎型設備之要求。	自行規劃並成立資通安全管理推動小組	每年至少執行一次內部稽核	每年至少達到（3、12、6、3）小時	
C 級	防火牆、IDS、IPS、防毒軟體、垃圾郵件過濾等設備	加強資通安全宣導	每年至少執行一次內部稽核	每年至少達到（3、12、6、3）小時	

四、 推動方式

前項企業安全等級經本公司核定後，應區分為「A」、「B」、「C」三級，選擇適用之安全基準，建立資通安全管理機制。詳見圖 3所示。

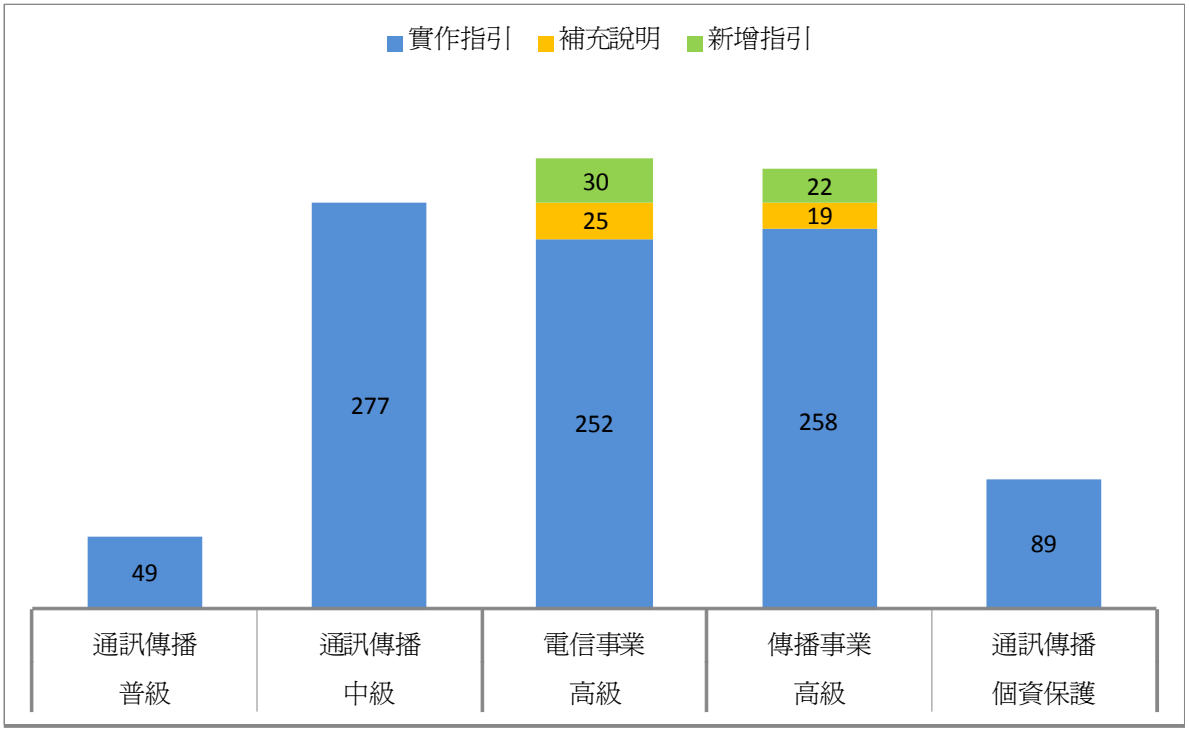


圖3　通訊傳播事業資通安全等級適用之安全防護基準

(一)　企業安全等級評定為「C」級者，應實施「資通安全管理內部稽核表」(詳見資安管理手冊附錄 6)之最小限安全需求項目。

(二)　企業安全等級評定為「B」級者，應實施「資通安全管理內部稽核表」之全部控制措施。

(三)　企業安全等級評定為「A」級者，除實施前述「資通安全管理內部稽核表」之全部控制措施外，另依據業務別，實施適用之「通訊事業增項稽核表」(詳見資安管理手冊附錄 7)或「傳播事業增項稽核表」(詳見資安管理手冊附錄 8)，並以通過資訊安全管理系統第三方驗證為目標，逐年改善最終及於全公司。

(四)　業務內容涉及個人資料保護者，應依據個資法之規定，另擬定個人資料檔案安全維護計畫，並參考適用於個人資料檔案保護之資安控

制措施(詳見資安管理手冊附錄 9)。

五、 稽核方式

(一) 每年至少執行一次內部稽核。

(二) 已通過資訊安全管理系統驗證之資產群組，應定期維持更新，免另辦理內部稽核作業。

六、 資通安全認知訓練

為建立通訊傳播事業員工正確資通安全認知、提升安全防護水準，應推動內部資通安全教育訓練，規劃每年應辦理之資通安全教育訓練及宣導時數如下：

主管、資通訊人員、業務人員及一般人員，每年至少須分別達到 3、12、6、3 小時之資通安全認知訓練。

七、 資通安全應變通報

應建立資通安全事故應變作業機制，當發生資通安全事故時，應立即填具「國家通訊傳播委員會資通安全事故通報單」（詳見資安管理手冊附錄 10）向主管機關通報，並採取應變措施。

八、 資通安全實施評鑑

(一) 內部稽核

本公司每年應於 8 月底前至少執行一次內部稽核，並將稽核結果依規定填寫以下記錄：

附件 6、7、8 執行內部稽核時，須填具附件如下：

（1）檢查項目勾選「是」者，須檢附相關佐證資料。

（2）檢查項目勾選「否」者，須填具「資通安全管理矯正／預防措施一覽表」（資安管理手冊附錄 11）及「資通安全管理矯正／預防措施單」（資安管理手冊附錄 12）。

（3）檢查項目勾選「不適用」者，須填具「內部稽核表檢查項目勾選不適用之說明」（資安管理手冊附錄 13）。「增項稽核表檢查項目勾選不適用之說明」（資安管理手冊附錄 14）

(二) 行政檢查

本公司萬一發生資通安全事故影響等級為 3 級或 4 級者，須於三天內備妥下列相關資料，以供主管機關行政檢查之用。

（1）重大資安事故應變措施之處理說明。

（2）資通安全管理實施計畫及執行成果

（3）資安管理手冊附錄 11 至附錄 13、各檢查項目之佐證資料、或經主管機關認可之資通安全管理機制驗證機構產出之稽核報告。

九、 年度提報資料要求

(一) 各通訊傳播事業應於每年 9 月底前，依其自我評估之資通安全等級，提報下列資料至本會：

（1）附錄 1、附錄 2、附錄 6、附錄 7 及附錄 8，擁有個資檔案者，需提報附錄 9。

（2）依要項說明三（六）執行內部稽核，勾選檢查項目「否」者，須提報附錄 11 及附錄 12。

（3）依要項說明三（六）執行內部稽核，勾選檢查項目「不適用」者，須提報附錄 13 及附錄 14。

(二) 通訊傳播事業經本會認可之資通安全管理機制驗證機構進行外部驗

證，並取得 CNS/ISO/IEC 27001 證明者，僅須提報附錄 1、附錄 2、附錄 7(或附錄 8)及附錄 14，擁有個資檔案者另需提報附錄 9，得免提報附錄 6 及附錄 13，惟須檢附該驗證證書及驗證報告等相關資料影本。

(三) 通訊傳播事業經本會認可之資通安全管理機制驗證機構進行外部驗證，並取得 ISO/IEC 27001 標準及附錄 7(或附錄 8)ISO/IEC 27011 增項稽核表驗證合格證明者，僅須提報附錄 1 及附錄 2，擁有個資檔案者另需提報附錄 9，得免提報附錄 6 至附錄 14，惟須檢附該驗證證書及驗證報告等相關資料影本。各項提報資料，詳見下表所示。

年度提報資料統計表

區分	內部稽核	外部驗證 CNS/ISO/IEC 27001	外部驗證 ISO/IEC 27011 增項
附錄 1. 通訊、傳播事業資通安全等級自我評估彙整表	V	V	V
附錄 2.通訊、傳播事業資通安全等級自我評估說明表	V	V	V
附錄 6.資通安全管理內部稽核表	V		
附錄 7.通訊事業增項稽核表	⊙	⊙	
附錄 8.傳播事業增項稽核表	⊙	⊙	
附錄 9.個人資料檔案保護之安全控制措施	⊙	⊙	⊙
附錄 11.資通安全管理矯正／預防措施一覽表	⊙		
附錄 12.資通安全管理矯正／預防措施單	⊙		
附錄 13.內部稽核表檢查項目勾選不適用之說明	⊙		
附錄 14.增項稽核表檢查項目勾選不適用之說明	⊙	⊙	
備註：V 必須提報項目 ⊙視需要提報項目			

陸、 資通安全文件管理

本公司資通安全文件，係為管制資訊安全各項管理性及支援性作業而建立之必要程序，文件架構，詳見圖 4所示，各階文件應加以文件化，並注意適時更新，讓有需要的使用者均可隨時取得。

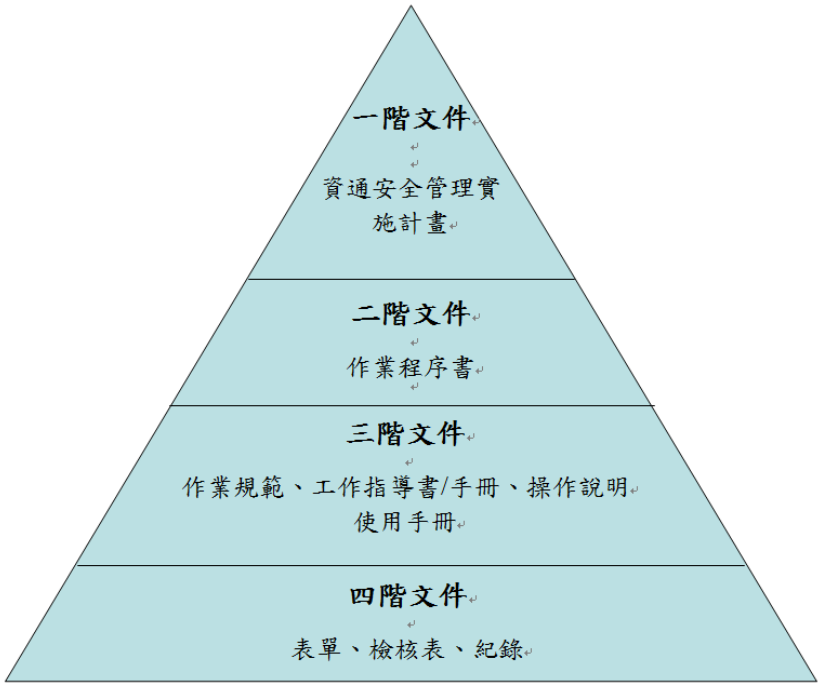


圖4　資通安全管理文件位階

一、 一階文件

本公司資通安全管理實施計畫，提供本公司資訊安全管理系統一個整體性的描述，說明本公司資通安全實施之範圍、資通安全政策、相關程序、並描述本公司各項流程間之交互關係。所有與資通安全相關之人員，均應熟悉本政策文件之政策及執行目標，並將其運用為各種程序、方法及工作規範之指導原則。

二、 二階文件

應依據內部稽核表之內容，規劃及發展資訊安全相關之各項活動與服務所需之組織運作流程。

三、 三階文件

為確保本公司各項資訊安全規劃、維運及支援作業(Operation Support)工作於必要時能有適當之指引，針對流程中之關鍵技術或作業另訂說明文件，

如作業指導書(或手冊)、作業規範、操作說明(或使用手冊)等，以作為相關作業執行時之指導。

四、 四階文件

為利於落實本公司各項作業，並達到制度化與一致化之目的，對於資通安全之各項要求，於流程執行過程中提供細部之表單、大綱、及查核表等，以利相關人員依照規定之表單及資料執行各項作業，並記錄作業執行結果。此類表單，可以採用電子媒體方式處理，但仍必須保留該表單必要之資料。

五、 資通安全文件之核定

(一) 資通安全一階文件由資通安全管理推動小組研擬，經資訊安全長核定後實施，修正時亦同。

(二) 資通安全第二、三、四階文件，由資通安全管理推動小組授權各分組研提，並由分組召集人審查核定後實施。

柒、 附件

請參閱資通安全管理手冊之附錄

附錄 5 資通安全管理實施計畫應執行工作事項表

作業名稱 內容 等級	資訊處理設施防護縱深	推動方式	稽核方式	資安教育訓練時數（主管、資通訊人員、業務人員、一般人員）	個資保護
A 級	防火牆、IPS、IDS、防毒軟體、垃圾郵件過濾、網頁過濾管控設備、網路安全監控等設備，其安全等級至少應符合「資通設備安全審驗作業要點（草案）」進階型設備之要求。	以通過資訊安全管理系統第三方驗證為目標	每年至少執行一次內部稽核	每年至少達到（3、12、6、3）小時	涉及個人資料保護者應依據個資法施行細則，訂定個人資料檔案安全維護計畫，採取適當安全維護措施。
B 級	防火牆、IDS、IPS、防毒軟體、垃圾郵件過濾等設備，其安全等級至少應符合「資通設備安全審驗作業要點（草案）」基礎型設備之要求。	自行規劃並成立資通安全管理推動小組	每年至少執行一次內部稽核	每年至少達到（3、12、6、3）小時	
C 級	防火牆、IDS、IPS、防毒軟體、垃圾郵件過濾等設備	加強資通安全宣導	每年至少執行一次內部稽核	每年至少達到（3、12、6、3）小時	

附件 4

附錄 6 通訊傳播事業資通安全管理內部稽核表

公司名稱			
資通安全等級	□B 級 □C 級		
單位主管		稽核日期：	
稽核人員		稽核日期：	
聯絡窗口	電話：	傳真：	行動：
	Email：		

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
1.資訊安全政策						
1.1 是否依據相關法律、法規及營運要求，訂定組織資訊安全政策？	◎	◎				
1.2 是否考量組織之整體業務活動及其相關風險，訂定資訊安全政策？	◎	◎				
1.3 是否識別違反資訊安全政策之後果及訂定處理程序？	◎	◎				
1.4 是否由管理階層核准資訊安全政策文件，正式發布且轉知所有員工與各相關外部團體？	◎	◎				
1.5 資訊安全政策文件是否包括資訊安全之定義、整體目標、範圍、實施內容、執行組織、權責分工、員工責任、事故通報處理流程？	◎	◎				
1.6 是否依據資訊安全政策，訂定原則、標準及對組織特別重要之法規要求說明文件及資料（如法律、法規命令、行政規則、契約、安全教育、訓練、認知、營運持續管理、作業程序、資訊安全控管文件、使用者應遵守的安全規則）？	◎	◎				

附錄 6 通訊傳播事業資通安全管理內部稽核表

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
1.7 資訊安全政策是否就一般和特定責任之權責（包括通報資訊安全事故）加以定義？。	◎	◎				
1.8 是否對支援資訊安全政策的文件建立補述文件？例如：針對特定資訊系統的更詳盡安全政策和程序，或使用者宜遵守的安全規則。	◎	◎				
1.9 資訊安全政策是否由具有發展、審查及評估等核准權限之管理者，依規劃期間或有重大變更時，作必要之審查及調整？	◎	◎				
1.10 是否妥善維護資訊安全管理政策之審查紀錄與訂定管理審查程序，包括審查時程及週期?	◎	◎				
1.11 是否定期對組織人員及資訊設備進行安全評估，以確定其遵守資訊安全政策及相關規定？	◎	◎				
1.12 是否指定專人或專責部門進行資訊安全政策的維護及檢討？	◎	◎				
2.資訊安全之組織						
2.1 管理階層是否在組織內藉由清楚的指示、明確的指派及確認資訊安全責任，主動地展現承諾以支持安全？	◎	◎	◎			
2.2 是否指派擁有權責之管理階層或成立跨部門組織負責推動、協調及監督資訊安全管理事項？	◎	◎				
2.3 是否指定專人或專責部門，負責辦理下列資訊安全管理工作事項(1)資安政策、計畫、措施之研議，(2)風險評鑑、資訊分類、系統安全控管措施，(3)資料及資訊系統之使用管理及保護，(4)資安認知訓練及資安稽核？	◎	◎				

附錄 6 通訊傳播事業資通安全管理內部稽核表

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
2.4 資訊安全責任的配置是否依據資訊安全政策，並明確地識別需保護之個別資產與執行特定安全作業過程的責任，並加以文件化？	◎	◎				
2.5 是否依據員工之職務內容，訂定員工資訊安全作業程序、權責規範或授權層級並予以文件化？（含經管使用設備及作業須知）	◎	◎				
2.6 是否訂定各項資訊處理設施之用途及使用授權，及其安全之作業程序？	◎	◎				
2.7 是否識別並定期審查組織對於資訊保護之機密性或保密協議之要求？	◎	◎				
2.8 是否訂定當發生資安事故時，如何及時與主管機關聯繫並通報之適當程序或規定？	◎	◎				
2.9 是否訂定與各特殊利益團體、專家安全論壇及專業協會維持適當聯繫？	◎	◎				
2.10 獨立審查組織對資訊安全管理之作法與其實作（例如：各項資訊安全的控制目標、控制措施、政策、過程及程序），是否定期召開管理審查會議？當資安作業環境發生重大變更時，亦依上述作法與實作，召開管理審查會議？	◎	◎				
2.11 因營運需要開放給外部團體（含其他機關、往來業者、維護廠商、委外承包商、聘僱人員及一般民眾）使用之資訊，是否執行風險評鑑與實作安全控制措施？並於契約或規定中包含雙方權利、義務、資料保護、資訊保密、服務標的水準、智慧財產權、事故發生處理與違約處理等條款？	◎	◎				
2.12 是否對不開放外部團體存取的資	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
訊進行必要的控制措施？						
2.13 因營運需要開放給外部組織或人員存取之資訊，其存取權限是否定期審查？	◎	◎				
2.14 因營運需要開放給外部團體（含其他機關、往來業者、維護廠商、委外承包商、聘僱人員及一般民眾等）使用之資訊，於開放使用之前，是否闡明所有已識別之安全要求？	◎	◎				
2.15 委外契約中有關安全需求內容，是否包含法律要求（如個人資料保護法）、雙方有關人員權責、安全控管措施、作業程序、事故通報程序、服務水準、對委外廠商稽核權等資訊安全責任與事宜，並得依實際需要適時修改安全控管措施及作業程序等？	◎	◎	◎			
3.資產管理						
3.1 是否明確識別所有資產，並製作與維持所有重要資產的清冊？	◎	◎				
3.2 是否有明確之定義，如何分辨何種資產是重要資產，再依據該定義作資產盤點，並建立與維護重要資產清冊？	◎	◎				
3.3 現有之重要資產清冊是否包含災難回復所需之資訊，如：資產型態/格式/位置/備份資訊/使用版本/業務價值？	◎	◎				
3.4 資產清冊是否定期審查，確保資產處於適切狀態？	◎	◎				
3.5 是否識別所有資訊資產之擁有者，並指派其依適切控制措施維護資訊資產之責任？	◎	◎				
3.6 是否識別及實作所有與資訊處理設施相關（含電子郵件、網路使用及行動	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
設備等）之使用規則，並加以文件化？						
3.7 是否依據資訊對於組織的價值、法律要求、敏感性及重要性加以分類？	◎	◎				
3.8 是否依據組織採用的分類法，訂定適當之資訊標示與處理程序？	◎	◎	◎			
3.9 是否對於機密性資訊、敏感性之手稿資訊、影印公文之廢紙及已過保存期限之公文，於棄置前予以銷毀？	◎	◎	◎			
4.人力資源安全						
4.1 是否依照組織的資訊安全政策，訂定正式文件，規範所有員工、承包商或第三方使用者之安全角色與責任？	◎	◎	◎			
	◎	◎	◎			
4.2 是否明確定義所有聘僱之應徵者、承包商及第三方使用者背景查證檢核之限制與程序，確保符合隱私權、個人資料保護及/或聘僱勞工保護相關法令之要求？	◎	◎				
4.3 被賦予機敏資訊存取權的所有員工、承包商及第三方使用者，是否在被允許存取資訊處理設施之前，簽署適當之機密性或保密協議？	◎	◎				
4.4 管理階層是否有要求員工、承包商及第三方使用者，依照組織已訂定的政策與程序執行安全事宜？	◎	◎				
4.5 對所有員工、承包者及第三方使用者工作職務有關之安全程序及資訊處理設施，是否提供正確使用之認知、教育與訓練？	◎	◎				
4.6 是否訂定員工違反組織安全政策與程序之懲處規定？	◎	◎				
4.7 是否在與員工、承包商或第三方使用者所訂之契約內規定，在聘僱終止	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
後，與職務有關之責任仍然是有效的？						
4.8 所有員工、承包商及第三方使用者離職或聘雇終止時，是否依規定繳回其任職期間保管之資訊資產？（包含所有的軟體、公司文件、設備、行動裝置、信用卡、存取卡、軟體、手冊及儲存於電子媒體的資訊等所有其他組織資產）	◎	◎				
4.9 所有員工、承包商及第三方使用者之聘僱、契約或協議終止時，或因變更而調整時，是否對資訊及資訊處理設施之存取權限迅速予以移除？	◎	◎				
5.實體及環境安全						
5.1 是否適當使用安全邊界（如圍牆、入口閘門或人員駐守的接待櫃檯等屏障），保護含有資訊與資訊處理設施的區域？	◎	◎				
5.2 組織管理之資訊處理設施（如通訊服務設施），在實體上是否與第三方管理（如：客戶代管設備）之資訊處理設施區隔？	◎	◎				
5.3 具有關鍵或敏感的資訊處理設施之安全區域，是否對於授權進出人員作必要之限制及監督其活動？	◎	◎				
5.4 安全區域之進出權限是否定期審查並更新，並於必要時廢止？	◎	◎				
5.5 辦公處所是否實施必要之保護措施？	◎	◎	◎			
5.6 是否檢查及評估重要資通訊設備設置地點，鄰近場所之任何安全威脅，如火災、灰塵、水災、震動、化學效應、電力供應、電磁幅射、民間暴動及其他天然或人為災害等可能對設備之危害？	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
5.7 是否設計並實施適當的控制措施，以保護敏感資訊處理設施之地點及內部人員通訊錄？	◎	◎				
5.8 是否嚴禁在電腦機房內使用未經核准之電器或其他物品？	◎	◎				
5.9 備援設備及備份媒體存放位置，是否與主要場地保持安全距離？	◎	◎				
5.10 安全區域是否與易燃物或危險物料保持安全距離，並不宜儲存大量的物資？	◎	◎				
5.11 是否設計並實施適當之控制措施，監督安全區域內之工作，並確保其需知原則？	◎	◎				
5.12 是否訂定未經授權前，禁止拍照、錄影、錄音和其他記錄性設備之規定，如行動裝置上的照相機？	◎	◎				
5.13 無人使用之安全區域是否上鎖並定期檢查？	◎	◎				
5.14 對於收發、裝卸區及其他未經授權人員可進入之作業場所，是否有適當之進出控制措施，並應與資訊處理設施隔離，以避免未經授權的存取？	◎	◎				
5.15 是否明確訂定資通訊設備之控制措施（包括場外使用之設備，及財產之攜出），以降低資料未經授權存取、遺失及損壞之風險？	◎	◎				
5.16 處理敏感資料的資通訊設備或資訊處理設施是否予特別保護並評估其有效性？	◎	◎				
5.17 是否採取適當控制措施，降低潛在實體威脅，如：竊盜、火災、爆裂物、煙害、水災（或水源供應停止）、閃電、	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
溫度、濕度、灰塵、振動、化學效應、電力供應干擾、通信干擾、電磁輻射及蓄意破壞等？						
5.18 電腦作業區（含機房）是否落實執行禁止抽煙及飲食？	◎	◎				
5.19 是否具備環境監控機制，掌握資通訊設備及資訊處理設施之溫度及溼度狀況？	◎	◎				
5.20 是否對於支援性公共設施，如電源供應、水源供應、污水處理、暖氣/通風及空調，設計適當之保護措施，並施行之，確保不受公共設施失效所導致之中斷？	◎	◎	◎			
5.21 備援電源是否定期檢查並測試，確保能在斷電期間正常運作？	◎	◎				
5.22 電信機線設備（telecommunications lines）、網路佈纜（network cabling）及電源纜線，是否設計適當之安全保護措施，並施行之？	◎	◎				
5.23 通信纜線（communications cables）及電源纜線是否接地並隔離，防止互相干擾？	◎	◎				
5.24 設備是否定期且正確的維護保養，確保其可用性及完整性？	◎	◎				
5.25 各項設備是否依據供應商建議的間隔與保養手冊，定期檢查並維護？	◎	◎				
5.26 設備之維護與修理，是否由授權之維護人員執行？	◎	◎				
5.27 是否妥適保存所有可疑、實際之系統錯誤資訊，及所有預防性、矯正性之維護紀錄？	◎	◎				
5.28 設備送場外維修，對於儲存在設備	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
內資訊是否訂有安全保護措施？						
5.29 攜出場所外之設備和媒體，是否訂有安全保護措施？	◎	◎	◎			
5.30 行動裝置（設備）是否訂有嚴謹保護措施（如使用授權管理、設通行碼、檔案加密、專人看管）？	◎	◎	◎			
5.31 設備汰除前，是否將機密性、敏感性資料及有版權的軟體予以移除或實施安全覆寫？	◎	◎	◎			
5.32 含有敏感性資訊之設備汰除後，是否根據風險評鑑決定實體銷毀與否？	◎	◎	◎			
5.33 資訊資產如須攜出場外使用，是否經事前授權，並於攜出場外與歸還時，進行安全查核及紀錄？	◎	◎	◎			
6.通訊及作業管理						
6.1 資訊處理設施與資通訊設備相關之各項作業程序及活動是否文件化、並適當維護？如電腦開機與關機程序、備份、設備維護、資訊的處理與處理、異常情況之處理、緊急聯絡資訊、重新啟動及復原程序、稽核存底與日誌資訊之維護、電腦機房與郵件處理管理，以及生命財產安全（safey）等。	◎	◎				
6.2 資訊處理設施與資通訊設備之變更，是否有正式核准之程序，並向相關人員通報變更細節？	◎	◎				
6.3 資訊處理設施與資通訊設備之變更，是否詳實紀錄，並重新進行風險評鑑？	◎	◎				
6.4 資訊處理設施與資通訊設備之變更，是否備有後撤(fallback)程序，包括不成功的變更、意外事故的中止及復原	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
之程序與責任？						
6.5 對於安全要求較高的業務，是否區隔其職務與責任領域？	◎	◎				
6.6 業務資訊資產之使用、資料建檔、系統操作、網路管理、行政管理、系統發展維護、變更管理、安全管理等工作，是否授權由不同的人員執行？	◎	◎				
6.7 是否分隔開發、測試及運作之設施、系統、軟體？	◎	◎				
6.8 運作測試系統是否使用不同的使用者剖繪（profile），且功能選單需顯示適切的識別訊息，降低錯誤之風險？	◎	◎				
6.9 是否與第三方服務交付廠商簽訂適當之資訊安全協定，並納入契約條款，包含安全控制措施、服務定義及交付等級，並賦予相關安全管理責任？	◎	◎				
6.10 是否規劃必要轉換（資訊、資訊處理設施及其他任何需要移動者）之安全控制措施，並確保轉換期間安全的維護？	◎	◎				
6.11 是否定期對第三方所提供之服務、報告及紀錄等進行適當之監視與審查，並定期執行稽核？	◎	◎	◎			
6.12 第三方提供之服務如有任何異動時，是否重新進行風險評鑑？	◎	◎	◎			
6.13 資訊處理設施及資通訊設備設置前，是否進行容量規劃及預留安全容量，並於正式運作時，持續監控其容量狀態？	◎	◎				
6.14 是否建立新資訊系統、系統升級或新版本之驗收準則，在新資訊系統、系統升級及新版本正式驗收後，才可移轉	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
上線？						
6.15 是否全面使用防毒軟體，並即時更新病毒掃描引擎及病毒碼？	◎	◎				
6.16 電腦系統及資料儲存媒體是否定期進行惡意程式病毒及後門程式掃描？	◎	◎				
6.17 是否訂定正式政策，禁止使用未經授權的軟體？	◎	◎				
6.18 是否對支援重要營運程序之系統軟體與資料，執行定期審查？若出現任何未經核准的檔案或未經授權的增補修補程式，應進行正式調查。	◎	◎				
6.19 是否訂定使用電子郵件附件及下載之檔案前，檢查有無惡意程式軟體(含病毒、木馬或後門等程式）之程序？	◎	◎				
6.20 是否定義處理電腦病毒、木馬等惡意程式之管理程序與責任，並訓練員工如何通報惡意程式攻擊，及復原程序？	◎	◎				
6.21 是否準備遭惡意程式攻擊後復原之營運持續計畫，並包括所有必要之資料與軟體備份及復原準備工作？	◎	◎				
6.22 重要資訊及軟體是否定期作備份處理，並定義備份資訊之必要等級？	◎	◎				
6.23 備份複本是否定期回復測試，並將回覆程序文件化，確保備份複本之可用性及有效性？	◎	◎				
6.24 重要及機敏資訊之備份程度及頻率，是否反應組織的營運要求？	◎	◎				
6.25 備份資訊是否儲存於遠端地點？距離須足以避免主要場地發生災難時遭波及？	◎	◎				
6.26 備份資訊是否給予適切等級之實體與環境保護，並與主要場域使用一致	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
之標準？						
6.27 主要場域採用之控制措施是否延伸至涵蓋備份作業場域？	◎	◎				
6.28 是否定期檢查及測試復原程序，確保有效性，且能夠在復原程序分配之時間內完成復原運作？	◎	◎				
6.29 是否訂定網路及網路遠端設備之使用權責及程序？	◎	◎				
6.30 是否使用網路安全防禦設備，並適當的隔離外部網際網路與組織內部網路？	◎	◎				
6.31 組織建立之網路控制措施，是否能反應資訊之機密性、完整性與可用性要求？	◎	◎				
6.32 對於機敏性資訊之傳輸過程，是否採取資訊加密等保護措施？	◎	◎				
6.33 是否訂定確保網路服務連線品質及可用性之保護措施，提供最佳服務？	◎	◎				
6.34 是否定期檢討網路安全控管事項之執行？	◎	◎				
6.35 是否定期檢測網路運作環境之安全漏洞？	◎	◎				
6.36 是否使用適當之網路安全解決方案？如防火牆、入侵偵測系統？防火牆存取政策（security policy）設定是否適當？	◎	◎				
6.37 是否建立各種可攜式媒體之操作管理程序，防止文件、電腦媒體（例如：磁帶、磁碟）、輸入或輸出資料及系統文件，遭受未經授權的揭露、修改、移除及破壞？	◎	◎	◎			
6.38 含有敏感性資訊之媒體是否以正	◎	◎	◎			

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
式程序加以安全地汰除，例如：焚化或絞碎，或清除資料後由組織內其他應用系統使用？						
6.39 具機密性或敏感性資訊之媒體是否有安全之保存和報廢程序？	◎	◎	◎			
6.40 機密性、敏感性資訊之儲存或處理是否有安全處理程序及分級標示？	◎	◎				
6.41 是否建立資訊的處理及儲存的程序，以保護免於未經授權的揭露或誤用?	◎	◎				
6.42 對應用程式、程序、資料結構及授權過程等說明之系統文件，是否有適當的存取保護措施？	◎	◎				
6.43 是否對於所有形式之資訊交換，訂定適當交換政策、程序及控制措施？	◎	◎				
6.44 是否對高度機敏性資訊在傳輸或儲存中使用加密技術？	◎	◎				
6.45 是否訂定組織與任何外部團體間，交換資訊與軟體之協議？	◎	◎	◎			
6.46 重要電腦資訊、媒體（含報表）之運送，是否有安全保護措施及完整監控記錄（含收送人、時間及內容）？	◎	◎	◎			
6.47 是否訂定適當控制措施，保護含有資訊之媒體，在組織實體邊界外傳送時，不受未經授權的存取、誤用或毀損？	◎	◎	◎			
6.48 採行電子交換之資訊，是否視資訊安全等級，採行識別碼與通行碼管制、電子資訊加密或電子簽章認證等保護措施，確保資訊的機密性、完整性、可用性及符合其他法律要求？	◎	◎				
6.49 涉及敏感性資訊及機密文件之營運資訊系統，是否提供適當之存取控制與保護？	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
6.50 是否實施適當控制措施，保護在公眾網路上傳輸且涉及電子商務之資訊，使其不受詐欺行為、契約爭議及未經授權之揭露與修改？	◎	◎	◎			
6.51 線上交易服務，是否訂定適當控制措施，防止下列事項：(1)不完整傳輸、(2)誤選路徑、(3)未經授權之訊息修改、揭露及(4)未經授權的訊息複製或重送(replay)等發生？	◎	◎	◎			
6.52 對外開放供公眾取得之資訊，是否訂定保護措施，確保資訊完整性，防止未經授權之修改？	◎	◎				
6.53 是否依據法律要求，如個資法，實施適當之稽核存錄措施，以紀錄使用者活動、異常及資訊安全事故？	◎	◎	◎			
6.54 是否採用適切的存錄與監控設備，記錄資通訊相關活動？	◎	◎				
6.55 是否建立適當之控制措施，監控資訊處理設施之使用，及定期審查？	◎	◎				
6.56 各項日誌是否有適當的保護措施，不受竄改與未經授權之存取，並針對留存之通信資訊設定適當之留存期限（例如：會計、帳務、客訴的處理、防止濫用及執法機關的要求）？	◎	◎				
6.57 是否定期稽查各項作業日誌？	◎	◎				
6.58 是否適當規劃存錄設施與日誌資訊之儲存媒體容量，避免無法記錄事故或覆蓋以往所記錄事故？	◎	◎				
6.59 作業日誌是否留有管理者與操作~~者~~所涉及活動之詳細過程，並定期予以審查？	◎	◎	◎			
6.60 是否加以存錄由使用者或系統程	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
式所通報之資訊處理或通信系統問題，迅速處理及通報？						
6.61 所有系統鐘訊是否與議定之鐘訊來源校正，以確保時間紀錄正確？	◎	◎				
7.存取控制						
7.1 是否根據營運與安全要求，建立、文件化及審查存取控制政策？	◎	◎				
7.2 是否在存取政策文件中明確陳述每個使用者或使用群組之存取控制規則與權限？	◎	◎				
7.3 資訊存取控制政策是否符合相關法律、法規命令及契約規定，如電信法、個資法等？	◎	◎				
7.4 是否對所有資訊系統與服務核准和撤銷存取，訂定適當之使用者註冊與註銷程序？	◎	◎	◎			
7.5 是否於使用者變更角色、調職或離職後，立即移除或封鎖其存取權限？	◎	◎	◎			
7.6 是否維持所有使用者註冊服務、系統或資訊等之正式紀錄？	◎	◎	◎			
7.7 基於系統管理或特殊作業需要，需設定特殊權限時（如系統管理、高階管理者），是否透過正式授權過程，控制特殊權限之配置？	◎	◎				
7.8 是否維護所有配置特殊權限之授權過程和紀錄，並於完成授權過程後才授予特殊權限？	◎	◎				
7.9 是否在提供使用者通行碼前，進行身份鑑別程序？	◎	◎				
7.10 是否以安全之程序轉交預設之通行碼給使用者，使用者取得通行碼，確認無誤後，需回應系統管理者？	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
7.11 軟體安裝完畢後，是否立即更新廠商所預設之通行碼？	◎	◎				
7.12 是否要求使用者於聘僱任期與條件中，簽署對個人通行碼保密聲明？	◎	◎				
7.13 是否強制要求使用者，初次登入電腦系統後，必須立即更改預設通行碼，或一定期限內未登入，則預設通行碼將失效，必須重新申請建立？	◎	◎				
7.14 是否規定通行碼不得以無保護之型式儲存於電腦系統中？	◎	◎				
7.15 所有使用者存取權限，是否定期檢查（建議每六個月一次、特權者每三個月一次）及任何變更(如升職、降職、調職或聘僱終止等)後審查？	◎	◎				
7.16 通行碼長度是否規定須超過6個字元（建議以 9 個字元位或以上）？	◎	◎				
7.17 通行碼是否規定需以大小寫字母、特殊符號及數字組成？	◎	◎				
7.18 通行碼輸入錯誤，是否訂有三次以內之限制？	◎	◎				
7.19 是否定期、依規定期限或使用次數限制，要求變更通行碼，並避免重複或循環使用舊通行碼？	◎	◎				
7.20 是否規定不得在任何自動登入過程中內含通行碼，例如：儲存在巨集或功能鍵中。	◎	◎				
7.21 是否規定避免使用與個人有關資訊（如生日、身分證統一編號、單位簡稱、電話號碼等）當做通行碼？	◎	◎				
7.22 是否避免保留通行碼的紀錄（例如：紙張、軟體檔案或手持裝置）， 除非其能被安全地存放，且該存放方式經	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
過核准？						
7.23 應用系統是否具有作業結束後或在一定期間未操作時即自動登出之保護機制？	◎	◎				
7.24 是否避免將輸入之通行碼以明文方式顯示在螢幕上？	◎	◎				
7.25 是否 對於無人看管之資訊設施有適當保護措施？	◎	◎				
7.26 是否訂有桌面淨空及螢幕淨空政策？	◎	◎	◎			
7.27 主機、伺服器、個人電腦、終端機等電腦設備於不使用、人員離座時是否即刻進行保護措施如關機、登出、設定螢幕保護密碼或是以其他控制措施進行保護？	◎	◎	◎			
7.28 下班後經辦之機密性及敏感性資訊是否妥為收存？	◎	◎	◎			
7.29 是否訂定適當之控制措施，防止未經授權使用影印機和其他複製設備（例如：掃瞄器、數位相機）？	◎	◎	◎			
7.30 敏感性或機密性資訊文件，是否立即從印表機上取走？	◎	◎	◎			
7.31 網路使用者（含外單位人員）是否取得正式存取授權？	◎	◎				
7.32 是否於登入作業完成後，顯示前一次登入日期與時間，或提供登入失敗之詳細資訊？	◎	◎				
7.33 是否限制登入失敗次數超過上限時，需強制延遲一段時間或重新取得授權後才允許再登入？	◎	◎				
7.34 是否訂定網路服務存取安全政策，確保使用者係經特定授權允許存取	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
網路與網路服務？						
7.35 對於外部連線使用者是否進行身份鑑別機制，如密碼技術、硬體符記或詰問/應答（challenge/response）協定等安全技術？	◎	◎				
7.36 是否採用自動設備識別方法，鑑別存取敏感或機密資訊之設備，方可允許其存取行為？	◎	◎				
7.37 對於遠端使用者的存取控制，是否有適當的鑑別機制？	◎	◎				
7.38 如需採用遠端診斷作業方式，是否訂定診斷埠之存取作業規範（如用金鑰管理及人員身份查驗或稽核等機制）？	◎	◎				
7.39 無線網路之存取及應用，是否訂有嚴謹之鑑別、加密方式及頻率選擇等控制措施？	◎	◎				
7.40 是否依據網路服務需要，區隔出獨立邏輯網域（如組織內部網路或外部網路），每個網域皆有定義的安全邊界，及通訊閘道管制過濾網域間資料之存取（如網路防火牆）？	◎	◎				
7.41 是否針對電子郵件、單雙向檔案傳輸、互動式存取或應用系統之存取時段作必要之限制？	◎	◎				
7.42 是否實施網路路徑控制，以確保電腦連線及資訊流，不會破壞營運應用程式之存取控制政策？	◎	◎				
7.43 是否提供登入程序最小限之系統輔助訊息，避免提供未經授權使用者任何不必要協助？	◎	◎				
7.44 是否依據系統機敏度，限制登入失敗次數之上限，並於登入失敗後中斷連	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
線？						
7.45 是否對於異常登入程序，留有紀錄及定期檢視？	◎	◎				
7.46 系統登入或存取重要資訊時，是否對連線過程提供加密之程序與措施？	◎	◎				
7.47 使用者是否採用具有唯一性之識別符號（使用者 ID）？	◎	◎				
7.48 重要系統使用者，是否採用適切之身分鑑別技術，例如：一次性密碼、智慧卡、符記或生物特徵？	◎	◎				
7.49 是否以保護的形式儲存和傳送通行碼，並告知申請者？通行碼檔案是否和應用系統資料分開存放？	◎	◎				
7.50 使用系統公用程式是否進行授權管制（如最低實務需求的授權）及身分鑑別程序？需要職務區隔時，是否有管制措施不讓具備系統應用程式存取權限的使用者，取得系統公用程式之權限？	◎	◎				
7.51 是否設定網路會談結束或超過定義的無動作時限後，即中斷連線或關閉設備？	◎	◎				
7.52 對風險高之應用系統，是否限制連線時間，如連線時間限制在正常辦公時間內？	◎	◎				
7.53 是否訂定使用者及支援人員，對應用系統存取權限之管制措施？	◎	◎				
7.54 處理機密及敏感性資訊，是否採用專屬（隔離）電腦作業環境？	◎	◎	◎			
7.55 是否訂定行動運算及通信設備之管理政策（如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求）?	◎	◎	◎			
7.56 遠距工作是否得到管理階層授權	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
（如活動政策、計畫及流程等）和施以必要之保護措施？						
7.57 遠距工作活動結束後，是否撤銷相關授權與存取權限及歸還管制設備？	◎	◎				
8.資訊系統獲取、開發及維護						
8.1 在規劃應用系統需求時，是否將安全需求納入分析及規格文件中？	◎	◎	◎			
8.2 是否檢查輸入資料，確認其正確性及適切性？	◎	◎				
8.3 是否針對輸入錯誤，設計及實作回應程序？	◎	◎				
8.4 應用程式內部處理是否加入確認查核（validation check），偵測可能經由處理錯誤或故意行為之任何資訊毀損，並提供適當程式從失效中復原，確保資料之正確處理？	◎	◎				
8.5 應用系統是否使用密碼技術，鑑別與保護其訊息之完整性？	◎	◎				
8.6 輸出資訊是否具合理性查核及一致性控制計數（reconciliation control count），確保所有資料都已合理處理？	◎	◎				
8.7 是否設計與實作輸出確認測試與回應之程序？	◎	◎				
8.8 是否設計並實作資料輸出確認過程之活動日誌，並定義所有涉及資料輸出過程人員之責任？	◎	◎				
8.9 是否基於風險評鑑結果，識別所需的保護等級，設計所需加解密演算法之型式、強度及品質？	◎	◎				
8.10 是否基於風險評鑑結果管理密碼金鑰，並發展適當之控制措施？	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
8.11 作業系統升級前，是否考量營運要求及該版本之安全性？	◎	◎				
8.12 處理作業系統軟體更新之人員，是否經管理階層授權？	◎	◎				
8.13 是否限定由經過訓練合格之管理人員，才可執行應用程式可執行碼更新作業？	◎	◎				
8.14 是否使用組態控制系統，以保持對所有已實作的軟體與系統文件之控制，且維護所有變更紀錄？	◎	◎				
8.15 是否避免以真實資訊進行測試作業？	◎	◎				
8.16 存取程式原始碼（program source code），是否訂有適當之控制措施，並留存稽核日誌？	◎	◎				
8.17 是否建立變更應用系統之管制程序？	◎	◎				
8.18 應用系統變更後，是否立即更新系統文件？	◎	◎				
8.19 作業系統變更後，是否對應用系統作技術性審查？	◎	◎				
8.20 作業系統變更後，是否主動公告異動範圍、時間及可能的影響？	◎	◎				
8.21 作業系統變更後，是否檢查其相關控管措施與程序仍然有效？	◎	◎				
8.22 是否僅限於必要的範圍，變更套裝軟體之，並嚴格管制所有變更？	◎	◎	◎			
8.23 是否檢查組織內可能之隱匿通道(covert channel)，降低資訊洩漏的風險？	◎	◎				
8.24 委外開發之系統上線前，是否偵測有無惡意程式存在？	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
8.25 委外開發合約中，是否規範著作權之歸屬？	◎	◎				
8.26 訂約時，是否簽訂安全履行條款與相關罰則？	◎	◎				
8.27 是否及時取得使用中通訊傳播系統之技術脆弱性資訊，並定期執行各項系統漏洞修補程式？	◎	◎				
8.28 進行系統修補前，是否先作系統影響評估與測試，再採取必要措施？	◎	◎				
9.資訊安全事故管理						
9.1 是否建立資安事故（含安全漏洞、系統弱點、病毒、非法入侵及系統異常）之正式通報應變程序？	◎	◎	◎			
9.2 事故回應小組是否建立單一聯繫窗口，授權在處理事故時採取立即之決定，並與外部團體（例如：執法機關、政府緊急應變中心、客戶、商業夥伴）建立聯繫管道？	◎	◎	◎			
9.3 資訊安全事故處理過程，是否留有完整記錄，如有必要，應經由直接發送電子郵件及/或網站首頁，及時回報事故給相關客戶？	◎	◎	◎			
9.4 是否建立資訊安全事故通報之聯絡點，並確保全組織都知道該聯絡點，隨時可聯繫，能夠有充分與及時的回應？	◎	◎	◎			
9.5 機關員工及外部使用者是否知悉資安事故通報及處理程序並依規定辦理?	◎	◎	◎			
9.6 是否要求資訊系統與服務的所有員工、承包商及第三方使用者，注意並通報任何觀察到或可疑的系統或服務之安全弱點？	◎	◎	◎			
9.7 是否依不同型式之資訊安全事故，	◎	◎	◎			

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
建立資安事故管理責任及應變程序？						
9.8 是否建立資安事件或事故等事後管理會議，以協助單位能從資安事件及事故中學習？	◎	◎	◎			
9.9 是否擬定營運中斷後之各項風險處理優先順序或處理準則（含處理順序說明、最低營運水準定義）？	◎	◎	◎			
9.10 是否建立資安事故管理機制，如記錄事故型式、處理方法、處理成本及矯正預防措施？	◎	◎	◎			
9.11 是否已建立及使用各項指標，以協助偵測安全事故，並預防安全事故？	◎	◎	◎			
9.12 已發生之資訊安全事故，是否在安全政策審查過程中納入考量？	◎	◎	◎			
9.13 資安事故中相關證據資料是否有適當保護措施，以符合證據能力之要求，作為問題分析及法律必要依據？	◎	◎				
10.營運持續管理						
10.1 是否發展與實作營運持續計畫，以因應組織營運持續所需的資訊安全要求？	◎	◎				
10.2 是否針對所有營運過程，可能造成營運中斷之機率及衝擊進行風險評鑑？	◎	◎				
10.3 是否識別營運持續過程中之關鍵資通訊設備及資訊處理設施？	◎	◎				
10.4 營運持續計畫是否以人員安全為優先，並保護資通訊設備和組織財產？	◎	◎				
10.5 是否訂定營運持續計畫（含啟動條件、參與人員、緊急程序、後撤程序、回復程序、維護時程、教育訓練、職責說明、所須資源、往來單位之應變規劃及合約適當性等）？	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
10.6 是否維持營運持續計畫之單一框架， 以確保所有計畫有一致性， 持續一致地因應資訊安全要求，並識別測試與維護的優先順序？	◎	◎				
10.7 營運持續計畫（含緊急應變處理程序）是否配合業務、組織及人員之變更而更新？	◎	◎				
10.8 營運持續計畫是否定期完整測試、演練並予更新維護?	◎	◎				
11.遵循性						
11.1 是否確保所有通訊系統與組織均不違反任何法律、法規命令、行政規則、契約義務及相關安全要求？	◎	◎				
11.2 軟體取得（含自行開發、委外開發、購置或租用）等可能涉及智慧財產權規定，是否符合法律、法規命令及契約的要求？	◎	◎				
11.3 是否公布智慧財產權遵循政策，定義軟體與資訊產品的合法使用，並告知違反政策人員將遭懲處？	◎	◎				
11.4 是否維護使用版權、原版碟片、手冊等所有權之證明和證據，並定期檢核是否只安裝經授權之軟體與有使用版權之產品？	◎	◎				
11.5 組織重要紀錄（如資料庫紀錄、系統日誌、操作日誌、稽核日誌）是否依安全等級加以保護及儲存（如檔案加密或數位簽章）？	◎	◎				
11.6 稽核後是否產生稽核報告，並追踪改善情形（包括稽核發現之摘要、稽核區域、缺失說明及改進建議等）？	◎	◎				
11.7 組織中對於所經管或處理之資	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
訊，涉及個人隱私及個人資料之保護是否有適當之保護機制？						
11.8 是否發展和實作符合法律、法規及若適用的契約條文所要求的資料保護與隱私政策？	◎	◎				
11.9 是否依據個人資料保護法擬定個人資料檔案安全維護計畫及業務終止個人資料處理方法？	◎	◎				
11.10 是否有監視設備或其他可偵測未經授權使用之設備，防止資訊設施被不當使用？	◎	◎				
11.11 管理人員是否定期審查其責任範圍內之資訊處理設施與其安全政策、標準及符合其他相關安全要求？	◎	◎				
11.12 組織訂定之安全程序，是否確保相關人員能正確執行？	◎	◎				
11.13 資訊系統是否定期進行安全技術符合性檢查（如滲透測試或系統弱點檢測）？	◎	◎				
11.14 技術遵循性之查核人員是否經過訓練，並作事前工作分配？	◎	◎				
11.15 技術遵循性檢查是否由合格資安技術單位執行？	◎	◎				
11.16 技術遵循性查核時之存取行為，是否作監控，並適當保存紀錄？	◎	◎				
11.17 技術遵循性查核結果是否文件化？	◎	◎				
11.18 是否訂定資訊安全內部稽核計畫（含稽核目標、範圍、時間、程序、人員）？	◎	◎				
11.19 是否定期辦理資訊安全內部稽核？	◎	◎				

通訊傳播事業資通安全管理內部稽核表						
檢查項目	企業安全等級			檢查結果		
	A 級	B 級	C 級	符合	不符合	不適用
11.20 內部稽核範圍是否含括資通系統、供應商、資產負責人、使用者和管理階層？	◎	◎				
11.21 是否有保護資訊系統稽核工具之存取，防止可能誤用或破解之措施？	◎	◎				
合計	277	277	49			

附錄 7 通訊事業增項稽核表

公司名稱			
資通安全等級	□電信事業 A 級		
單位主管		稽核日期：	
稽核人員		稽核日期：	
聯絡窗口	電話：	傳真：	行動：
	Email：		

通訊事業增項稽核表				
檢查項目	ISO/IEC 27011 電信事業增項控制措施	檢查結果		
		符合	不符合	不適用
資訊安全之組織				
1.1 通訊事業對保密協議之內容，是否包含：對於通訊之有無、對象、時間及內容等，以確保不得有不當揭露之情事發生？ (註：僅適用於電信事業)	◎			
1.2 組織是否訂定執法機關或研究機構請求提供資訊時之控管程序，確認此申請係符合法規命令之合法程序？	◎			
1.3 提供客戶服務前，是否訂定清楚之協議內容，要求不得毀損或減低通訊服務之能力？	◎			
1.4 提供第三方服務廠商存取權限之前，是否訂定清楚之協議內容，包含提供服務所需之相關安全政策與應注意事項，並確保沒有誤解之情形存在？	◎			
資產管理				
2.1 是否明確定義組織的電信機線設備，與其他組織相連結或相關之部份的管理責任，並加以文件化？	◎			

附錄 7 通訊事業增項稽核表

通訊事業增項稽核表				
檢查項目	ISO/IEC 27011 電信事業增項控制措施	檢查結果		
		符合	不符合	不適用
2.2 除一般、敏感及關鍵資訊之分類外，通訊事業是否對於通訊之有無、對象、時間及內容等，加以標示，並確保資訊存取之可歸責性？ (註：僅適用於電信事業)	◎			
人力資源安全				
3.1 是否詳細檢查員工、承包商及第三方使用者職務上被授權能夠存取之必要服務：如：客戶個人資料或客戶通話內容等，並納入相關安全責任之中？	◎			
3.2 對於人員進用，是否考量相關電信證照或具備適當的電信知識和技能？	◎			
3.3 對所有聘僱之應徵者、承包商及第三方使用者的之進用或委派，是否作適當之背景查驗工作，例如：工作職務涉及客戶個人資料或是通訊內容之存取者？	◎			
3.4 聘請第三方機構前，是否明確定義和溝通其安全角色和職責？	◎			
3.5 對於委外承包商或第三方使用者，是否在合約中加入安全角色與職責的要求？	◎			
3.6 是否要求組織內任何人從事電信服務時，應保護職務上所知悉之營業秘密？	◎			
3.7 組織是否依據相關法規命令，訂定防止不當揭露之責任？	◎			
實體及環境安全				
4.1 有權責人員是否於安全邊界發生異	◎			

附錄 7 通訊事業增項稽核表

通訊事業增項稽核表				
檢查項目	ISO/IEC 27011 電信事業增項控制措施	檢查結果		
		符合	不符合	不適用
常狀況時，可立即處理？				
4.2 通訊系統之機房控制中心與操作室是否有適當強度之門禁管制措施(strong entry controls）？	◎			
4.3 電信事業維運中心是否設置於適當地點（如避免易遭水災、風災、地震影響，或臨近強烈電磁及儲存危險物之場所）？	◎			
4.4 電信事業維運中心是否裝設自動火災警報系統？	◎			
4.5 電信事業維運中心是否為抗震建物？樓層地板是否有足夠之承載能力？	◎			
4.6 電信事業維運中心是否依據消防法規，使用防火建材？	◎			
4.7 通訊設備機房，是否選擇於適當地點，具備防範風災、水災、地震及火災之能力，並配備適當之偵測設備，防止未經授權之入侵？	◎			
4.8 無人看管之隔離操作區，如：行動電話中繼臺，是否具備以下安全措施：(1)自動消防設備、(2)遠端監控及自動告警系統，包含設備失效、電力失效、火警及溫濕度監控、(3)適當之實體安全維護設施等？	◎			
4.9 不同客戶之代管設備是否加以分隔，並實施適當保護措施？	◎			
4.10 關鍵設施是否有不斷電系統或是足夠之備援電力保護？	◎			
4.11 通訊系統放置於其他組織處之設	◎			

附錄 7 通訊事業增項稽核表

通訊事業增項稽核表				
檢查項目	ISO/IEC 27011 電信事業增項控制措施	檢查結果		
		符合	不符合	不適用
備，是否有足夠安全防護，且有定義清楚的邊界與介面，可以輕易加以隔離？				
4.12 放置於使用者端設備，是否具備遠端監控功能，必要時，可以輕易加以隔離？	◎			
4.13 是否持續監控與其它通信服務互連狀態，並有適當之控制措施，檢查與其它通訊服務互連是否正常？發生問題時，是否有方法可以矯正？	◎			
4.14 其它通信服務之互連是否已妥善定義邊界與介面？是否已定義用戶發生斷線時，如何處理之協議或合約？	◎			
通訊及作業管理				
5.1 通訊系統操作程序是否包含事故、緊急或危機處理程序？	◎			
5.2 是否建立資訊處理設施與資通訊設備變更之管理程序？管理程序之紀錄是否包括設施之安裝、更改位置及移除？	◎			
5.3 系統開發、測試及正式運作，是否區隔在不同的作業環境處理？	◎			
5.4 如採用敏感資訊進行測試，是否採取適當措施，避免程序或程式錯誤，導致不可預期之洩漏？	◎			
5.5 安裝可攜碼（mobile code）是否作必要之授權處理或限制使用？是否考慮內嵌可攜碼之中介軟體（middleware）之限制使用？	◎			
5.6 是否訂定網路服務供應商及使用者之服務協議，內容包含使用範圍、相關	◎			

附錄 7 通訊事業增項稽核表

通訊事業增項稽核表				
檢查項目	ISO/IEC 27011 電信事業增項控制措施	檢查結果		
		符合	不符合	不適用
權責及程序？				
5.7 是否針對不同營業項目，提供客戶適當之安全水準，且於服務協議中描述提供之安全功能、服務水準及管理需求，並辦理認知活動，提醒客戶防範垃圾郵件、網路犯罪及電腦病毒等危害？	◎			
5.8 是否訂定相關政策，防範垃圾郵件，並建置適切控管措施，建立一個合適的、令人期待的電子郵件通信環境？	◎			
5.9 是否訂定相關政策，防範阻斷服務（DoS）或分散式阻斷服務（DDoS）攻擊，並建置適切控管措施，建立一個合適的、令人期待的通訊環境？	◎			
5.10 是否具備經由 IP 位置、通訊埠與通訊協定等個別過濾通訊或限制通訊頻寬之機制，適當的保護易遭受網路攻擊之網路設施，如伺服器、路由器等？	◎			
5.11 是否具備偵測偽造來源地址（IP spoofing）之能力？	◎			
5.12 是否運用嚴格之密碼控制措施及/或高強度鑑別（strong authentication）功能，防範來源造假（source impersonation）？	◎			
5.13 是否事先經由定期收集與量測有關於災難、意外事件、社會現象等導致電信設備失效與網路壅塞之相關資訊，並彙集關鍵知識？	◎			
5.14 資通訊設備是否具備偵測網路壅塞及避免網路壅塞時通訊集中之機制？	◎			

附錄 7 通訊事業增項稽核表

通訊事業增項稽核表				
檢查項目	ISO/IEC 27011 電信事業增項控制措施	檢查結果		
		符合	不符合	不適用
5.15 是否訂定作業程序，預先收集可能造成網路雍塞或是預期事件之資訊？	◎			
5.16 是否建置分散式處理中心，採用輔助設備及適當之組態，提升系統峰值處理能力，防範潛在系統崩潰或是災難之發生？	◎			
5.17 是否能鑑別及給予必要的通訊優先權，協助災難發生後之交通維護、緊急通訊、電力供應或維持社會秩序？	◎			
5.18 個人資料檔案之留存期限，是否遵守相關法規命令？	◎			
存取控制				
6.1 通訊事業是否對於用戶端設備，訂定適切之存取控制規則（例如：控制的要求應基於資訊擁有者而非設備擁有者；採原則禁止、例外開放之規則）？	◎			
6.2 是否提供使用者能有效辨識與認可正確之電信服務營運商（如用戶無法證實時，應有的警示措施）的適切的控制措施？	◎			
資訊系統獲取、開發及維護				
7.1 操作系統環境中，應只能保持一套經批准之程式碼，不能有發展中程式碼與安裝編譯器程式？	◎			
7.2 所有資訊系統變更實作前，是否均有適當之回復策略？	◎			
7.3 是否針對所有運作中程式原始碼之更新及維護，留存稽核日誌？	◎			
7.4 是否針對屬敏感性系統（如交換器	◎			

通訊事業增項稽核表				
檢查項目	ISO/IEC 27011 電信事業增項控制措施	檢查結果		
		符合	不符合	不適用
設備等）之作業系統軟體或應用軟體，實施涵蓋所有路徑之完整測試？				
7.5 是否針對屬敏感性系統之應用軟體，至少保留前三代版本相關備份？	◎			
資訊安全事故管理				
8.1 是否建立資安事故之通報及事故回應與提報處理程序的管理責任與職掌定義？	◎			
8.2 是否建立資安事件或事故等事後管理會議，以協助單位能從資安事件、事故中學習？	◎			
營運持續管理				
8.3 是否訂定營運中斷後之各風險之處理優先順序或處理準則？	◎			
合計	55			

附錄 7 通訊事業增項稽核表

附錄 8 傳播事業增項稽核表

公司名稱			
資通安全等級	□傳播事業 A 級		
單位主管		稽核日期：	
稽核人員		稽核日期：	
聯絡窗口	電話：	傳真：	行動：
	Email：		

傳播事業增項稽核表				
檢查項目	ISO/IEC 27011 傳播事業增項控制措施	檢查結果		
		符合	不符合	不適用
資訊安全之組織				
1.4 提供第三方服務廠商存取權限之前，是否訂定清楚之協議內容，包含提供服務所需之相關安全政策與應注意事項，並確保沒有誤解之情形存在？	◎			
資產管理				
2.1 是否明確定義組織的廣播電視系統，與其他組織(如路權管理機關或是附掛單位等)相連結或相關之部份的管理責任，並加以文件化？	◎			
人力資源安全				
3.1 是否詳細檢查員工、承包商及第三方使用者職務上被授權能夠存取之必要服務：如：客戶個人資料，並納入相關安全責任之中？	◎			
3.2 對於人員進用，是否考量相關傳播證照或具備適當的傳播知識和技能？從業人員與工程人員資格是否符合主管機關之規定？	◎			

附錄 8 傳播事業增項稽核表

傳播事業增項稽核表				
檢查項目	ISO/IEC 27011 傳播事業增項控制措施	檢查結果		
		符合	不符合	不適用
3.3 對所有聘僱之應徵者、承包商及第三方使用者的之進用或委派，是否作適當之背景查驗工作，例如：工作職務涉及客戶個人資料或是傳播內容之存取者？	◎			
3.4 聘請第三方機構前，是否明確定義和溝通其安全角色和職責？	◎			
3.5 對於委外承包商或第三方使用者，是否在合約中加入安全角色與職責的要求？	◎			
3.6 是否要求組織內任何人從事傳播服務時，應保護職務上所知悉之營業秘密？	◎			
3.7 組織是否依據相關法規命令，訂定防止不當揭露之責任？	◎			
實體及環境安全				
4.1 有權責人員是否於安全邊界發生異常狀況時，可立即處理？	◎			
4.2 傳播系統之機房控制中心與操作室是否有適當強度之門禁管制措施(strong entry controls）？	◎			
4.3 傳播事業維運中心是否設置於適當地點（如避免易遭水災、風災、地震影響，或臨近強烈電磁及儲存危險物之場所）？	◎			
4.4 傳播事業維運中心是否裝設自動火災警報系統？	◎			
4.5 傳播事業維運中心是否為抗震建物？樓層地板是否有足夠之承載能力？	◎			

附錄 8 傳播事業增項稽核表

傳播事業增項稽核表				
檢查項目	ISO/IEC 27011 傳播事業增項控制措施	檢查結果		
		符合	不符合	不適用
4.6 傳播事業維運中心是否依據消防法規，使用防火建材？	◎			
4.7 傳播設備機房，是否選擇於適當地點，具備防範風災、水災、地震及火災之能力，並配備適當之偵測設備，防止未經授權之入侵？	◎			
4.8 無人看管之隔離操作區，如：廣播電視中繼臺等，是否具備以下安全措施：(1)自動消防設備、(2)遠端監控及自動告警系統，包含設備失效、電力失效、火警及溫濕度監控、(3)適當之實體安全維護設施等？	◎			
4.10 關鍵設施是否有不斷電系統或是足夠之備援電力保護？	◎			
4.11 傳播系統放置於其他組織處之設備，是否有足夠安全防護，且有定義清楚的邊界與介面，可以輕易加以隔離？	◎			
4.12 放置於使用者端設備，是否具備遠端監控功能，必要時，可以輕易加以隔離？	◎			
4.13 是否持續監控與其它通信服務互連狀態，並有適當之控制措施，檢查與其它通訊服務互連是否正常？發生問題時，是否有方法可以矯正？	◎			
4.14 其它通信服務之互連是否已妥善定義邊界與介面？是否已定義用戶發生斷線時，如何處理之協議或合約？	◎			
通訊及作業管理				
5.1 傳播系統操作程序是否包含事故、	◎			

附錄 8 傳播事業增項稽核表

傳播事業增項稽核表				
檢查項目	ISO/IEC 27011 傳播事業增項控制措施	檢查結果		
		符合	不符合	不適用
緊急或危機處理程序？				
5.2 是否建立資訊處理設施與資通訊設備變更之管理程序？管理程序之紀錄是否包括設施之安裝、更改位置及移除？	◎			
5.3 系統開發、測試及正式運作，是否區隔在不同的作業環境處理？	◎			
5.4 如採用敏感資訊進行測試，是否採取適當措施，避免程序或程式錯誤，導致不可預期之洩漏？	◎			
5.5 安裝可攜碼（mobile code）是否作必要之授權處理或限制使用？是否考慮內嵌可攜碼之中介軟體（middleware）之限制使用？	◎			
5.9 是否訂定相關政策，防範阻斷服務（DoS）或分散式阻斷服務（DDoS）攻擊，並建置適切控管措施，建立一個合適的、令人期待的傳播環境？	◎			
5.10 是否具備經由 IP 位置、通訊埠與通訊協定等個別過濾通訊或限制通訊頻寬之機制，適當的保護易遭受網路攻擊之網路設施，如伺服器、路由器等？	◎			
5.15 是否訂定作業程序，預先收集可能造成廣播中斷或是預期事件之資訊？	◎			
5.16 是否建置分散式處理中心，採用輔助設備及適當之組態，提升系統傳播能力，防範潛在系統崩潰或是災難之發生？	◎			
5.18 個人資料檔案之留存期限，是否遵守相關法規命令？	◎			

附錄 8 傳播事業增項稽核表

傳播事業增項稽核表				
檢查項目	ISO/IEC 27011 傳播事業增項控制措施	檢查結果		
		符合	不符合	不適用
資訊系統獲取、開發及維護				
7.1 操作系統環境中，應只能保持一套經批准之程式碼，不能有發展中程式碼與安裝編譯器程式？	◎			
7.2 所有資訊系統變更實作前，是否均有適當之回復策略？	◎			
7.3 是否針對所有運作中程式原始碼之更新及維護，留存稽核日誌？	◎			
7.4 是否針對屬敏感性系統（如交換器設備等）之作業系統軟體或應用軟體，實施涵蓋所有路徑之完整測試？	◎			
7.5 是否針對屬敏感性系統之應用軟體，至少保留前三代版本相關備份？	◎			
資訊安全事故管理				
8.1 是否建立資安事故之通報及事故回應與提報處理程序的管理責任與職掌定義？	◎			
8.2 是否建立資安事件或事故等事後管理會議，以協助單位能從資安事件、事故中學習？	◎			
營運持續管理				
8.3 是否訂定營運中斷後之各風險之處理優先順序或處理準則？	◎			
合計	40			

附錄 8 傳播事業增項稽核表

附錄 9 通訊傳播事業個資保護控制措施內部稽核表

公司名稱			
資通安全等級	□適用於擁有個人資料之資產		
單位主管		稽核日期：	
稽核人員		稽核日期：	
聯絡窗口	電話：	傳真：	行動：
	Email：		

通訊傳播事業個資保護控制措施內部稽核表				
檢查項目 （以下之檢查項目編號，係參考附錄 6）	個資保護控制措施	檢查結果		
		符合	不符合	不適用
6.通訊及作業管理				
6.5 對於涉及個人資料蒐集、處理及利用之業務，是否區隔其職務與責任，以授與執行業務所需之最小權限為原則？	◎			
6.6 個人資料之使用、資料建檔、系統操作、網路管理、行政管理、系統發展維護、變更管理、安全管理等工作是否授權由不同的人員執行？	◎			
6.15 是否全面使用防毒軟體，並即時更新病毒掃描引擎及病毒碼？	◎			
6.16 電腦系統及資料儲存媒體是否定期進行惡意程式病毒及後門程式掃描？	◎			
6.17 是否訂定正式政策，禁止使用未經授權的軟體？	◎			
6.18 是否對支援重要營運程序之系統軟體與資料，執行定期審查？若出現任何未經核准的檔案或未經授權的增補修補程式，應進行正式調查。	◎			
6.19 是否訂定使用電子郵件附件及下載之檔案前，檢查有無惡意程式軟體(含	◎			

附錄 9 通訊傳播事業個資保護控制措施內部稽核表

通訊傳播事業個資保護控制措施內部稽核表				
檢查項目 （以下之檢查項目編號，係參考附錄 6）	個資保護控制措施	檢查結果		
		符合	不符合	不適用
病毒、木馬或後門等程式）之程序？				
6.20 是否定義處理電腦病毒、木馬等惡意程式之管理程序與責任，並訓練員工如何通報惡意程式攻擊，及復原程序？	◎			
6.21 是否準備遭惡意程式攻擊後復原之營運持續計畫，並包括所有必要之資料與軟體備份及復原準備工作？	◎			
6.37 是否建立各種可攜式媒體之操作管理程序，防止文件、電腦媒體（例如：磁帶、磁碟）、輸入或輸出資料及系統文件，遭受未經授權的揭露、修改、移除及破壞？	◎			
6.38 含有敏感性資訊之媒體是否以正式程序加以安全地汰除，例如：焚化或絞碎，或清除資料後由組織內其他應用系統使用？	◎			
6.39 具機密性或敏感性資訊之媒體是否有安全之保存和報廢程序？	◎			
6.40 機密性、敏感性資訊之儲存或處理是否有安全處理程序及分級標示？	◎			
6.41 是否建立資訊的處理及儲存的程序，以保護免於未經授權的揭露或誤用?	◎			
6.43 是否對於所有形式之資訊交換，訂定適當交換政策、程序及控制措施？	◎			
6.44 是否對高度機敏性資訊在傳輸或儲存中使用加密技術？	◎			
6.45 是否訂定組織與任何外部團體間，交換資訊與軟體之協議？	◎			

附錄 9 通訊傳播事業個資保護控制措施內部稽核表

通訊傳播事業個資保護控制措施內部稽核表				
檢查項目 （以下之檢查項目編號，係參考附錄 6）	個資保護控制措施	檢查結果		
		符合	不符合	不適用
6.46 重要電腦資訊、媒體（含報表）之運送，是否有安全保護措施及完整監控記錄（含收送人、時間及內容）？	◎			
6.47 是否訂定適當控制措施，保護含有資訊之媒體，在組織實體邊界外傳送時，不受未經授權的存取、誤用或毀損？	◎			
6.48 採行電子交換之資訊，是否視資訊安全等級，採行識別碼與通行碼管制、電子資訊加密或電子簽章認證等保護措施，確保資訊的機密性、完整性、可用性及符合其他法律要求？	◎			
6.49 涉及敏感性資訊及機密文件之營運資訊系統，是否提供適當之存取控制與保護？	◎			
6.50 是否實施適當控制措施，保護在公眾網路上傳輸且涉及電子商務之資訊，使其不受詐欺行為、契約爭議及未經授權之揭露與修改？	◎			
6.51 線上交易服務，是否訂定適當控制措施，防止下列事項：(1)不完整傳輸、(2)誤選路徑、(3)未經授權之訊息修改、揭露及(4)未經授權的訊息複製或重送(replay)等發生？	◎			
6.53 是否依據法律要求，如個資法，實施適當之稽核存錄措施，以紀錄使用者活動、異常及資訊安全事故？	◎			
6.54 是否採用適切的存錄與監控設備，記錄資通訊相關活動？	◎			
6.55 是否建立適當之控制措施，監控資	◎			

附錄 9 通訊傳播事業個資保護控制措施內部稽核表

通訊傳播事業個資保護控制措施內部稽核表				
檢查項目 （以下之檢查項目編號，係參考附錄 6）	個資保護控制措施	檢查結果		
		符合	不符合	不適用
訊處理設施之使用，及定期審查？				
6.56 各項日誌是否有適當的保護措施，不受竄改與未經授權之存取，並針對留存之通信資訊設定適當之留存期限（例如：會計、帳務、客訴的處理、防止濫用及執法機關的要求）？	◎			
6.57 是否定期稽查各項作業日誌？	◎			
6.58 是否適當規劃存錄設施與日誌資訊之儲存媒體容量，避免無法記錄事故或覆蓋以往所記錄事故？	◎			
6.59 作業日誌是否留有管理者與操作者所涉及活動之詳細過程，並定期予以審查？	◎			
6.60 是否加以存錄由使用者或系統程式所通報之資訊處理或通信系統問題，迅速處理及通報？	◎			
6.61 所有系統鐘訊是否與議定之鐘訊來源校正，以確保時間紀錄正確？	◎			
7.存取控制				
7.4 是否對所有資訊系統與服務核准和撤銷存取，訂定適當之使用者註冊與註銷程序？	◎			
7.5 是否於使用者變更角色、調職或離職後，立即移除或封鎖其存取權限？	◎			
7.6 是否維持所有使用者註冊服務、系統或資訊等之正式紀錄？	◎			
7.7 基於系統管理或特殊作業需要，需設定特殊權限時（如系統管理、高階管理者），是否透過正式授權過程，控制	◎			

通訊傳播事業個資保護控制措施內部稽核表				
檢查項目 （以下之檢查項目編號，係參考附錄 6）	個資保護控制措施	檢查結果		
		符合	不符合	不適用
特殊權限之配置？				
7.8 是否維護所有配置特殊權限之授權過程和紀錄，並於完成授權過程後才授予特殊權限？	◎			
7.9 是否在提供使用者通行碼前，進行身份鑑別程序？	◎			
7.10 是否以安全之程序轉交預設之通行碼給使用者，使用者取得通行碼，確認無誤後，需回應系統管理者？	◎			
7.11 軟體安裝完畢後，是否立即更新廠商所預設之通行碼？	◎			
7.12 是否要求使用者於聘僱任期與條件中，簽署對個人通行碼保密聲明？	◎			
7.13 是否強制要求使用者，初次登入電腦系統後，必須立即更改預設通行碼，或一定期限內未登入，則預設通行碼將失效，必須重新申請建立？	◎			
7.14 是否規定通行碼不得以無保護之型式儲存於電腦系統中？	◎			
7.15 所有使用者存取權限，是否定期檢查（建議每六個月一次、特權者每三個月一次）及任何變更(如升職、降職、調職或聘僱終止等)後審查？	◎			
7.16 通行碼長度是否規定須超過6個字元（建議以 9 個字元位或以上）？	◎			
7.17 通行碼是否規定需以大小寫字母、特殊符號及數字組成？	◎			
7.18 通行碼輸入錯誤，是否訂有三次以內之限制？	◎			

附錄 9 通訊傳播事業個資保護控制措施內部稽核表

通訊傳播事業個資保護控制措施內部稽核表				
檢查項目 （以下之檢查項目編號，係參考附錄 6）	個資保護控制措施	檢查結果		
		符合	不符合	不適用
7.19 是否定期、依規定期限或使用次數限制，要求變更通行碼，並避免重複或循環使用舊通行碼？	◎			
7.20 是否規定不得在任何自動登入過程中內含通行碼，例如：儲存在巨集或功能鍵中。	◎			
7.21 是否規定避免使用與個人有關資訊（如生日、身分證統一編號、單位簡稱、電話號碼等）當做通行碼？	◎			
7.22 是否避免保留通行碼的紀錄（例如：紙張、軟體檔案或手持裝置）， 除非其能被安全地存放，且該存放方式經過核准？	◎			
7.23 應用系統是否具有作業結束後或在一定期間未操作時即自動登出之保護機制？	◎			
7.24 是否避免將輸入之通行碼以明文方式顯示在螢幕上？	◎			
7.26 是否訂有桌面淨空及螢幕淨空政策？	◎			
7.27 主機、伺服器、個人電腦、終端機等電腦設備於不使用、人員離座時是否即刻進行保護措施如關機、登出、設定螢幕保護密碼或是以其他控制措施進行保護？	◎			
7.28 下班後經辦之機密性及敏感性資訊是否妥為收存？	◎			
7.29 是否訂定適當之控制措施，防止未經授權使用影印機和其他複製設備（例	◎			

附錄 9 通訊傳播事業個資保護控制措施內部稽核表

通訊傳播事業個資保護控制措施內部稽核表				
檢查項目 （以下之檢查項目編號，係參考附錄 6）	個資保護控制措施	檢查結果		
		符合	不符合	不適用
如：掃瞄器、數位相機）？				
7.30 敏感性或機密性資訊文件，是否立即從印表機上取走？	◎			
7.32 是否於登入作業完成後，顯示前一次登入日期與時間，或提供登入失敗之詳細資訊？	◎			
7.33 是否限制登入失敗次數超過上限時，需強制延遲一段時間或重新取得授權後才允許再登入？	◎			
7.34 是否訂定網路服務存取安全政策，確保使用者係經特定授權允許存取網路與網路服務？	◎			
7.35 對於外部連線使用者是否進行身份鑑別機制，如密碼技術、硬體符記或詰問/應答（challenge/response）協定等安全技術？	◎			
7.36 是否採用自動設備識別方法，鑑別存取敏感或機密資訊之設備，方可允許其存取行為？	◎			
7.40 是否依據網路服務需要，區隔出獨立邏輯網域（如組織內部網路或外部網路），每個網域皆有定義的安全邊界，及通訊閘道管制過濾網域間資料之存取（如網路防火牆）？	◎			
7.41 是否針對電子郵件、單雙向檔案傳輸、互動式存取或應用系統之存取時段作必要之限制？	◎			
7.43 是否提供登入程序最小限之系統輔助訊息，避免提供未經授權使用者任	◎			

附錄 9 通訊傳播事業個資保護控制措施內部稽核表

通訊傳播事業個資保護控制措施內部稽核表				
檢查項目 （以下之檢查項目編號，係參考附錄 6）	個資保護控制措施	檢查結果		
		符合	不符合	不適用
何不必要協助？				
7.44 是否依據系統機敏度，限制登入失敗次數之上限，並於登入失敗後中斷連線？	◎			
7.45 是否對於異常登入程序，留有紀錄及定期檢視？	◎			
7.46 系統登入或存取重要資訊時，是否對連線過程提供加密之程序與措施？	◎			
7.47 使用者是否採用具有唯一性之識別符號（使用者 ID）？	◎			
7.48 重要系統使用者，是否採用適切之身分鑑別技術，例如：一次性密碼、智慧卡、符記或生物特徵？	◎			
7.51 是否設定網路會談結束或超過定義的無動作時限後，即中斷連線或關閉設備？	◎			
7.52 對風險高之應用系統，是否限制連線時間，如連線時間限制在正常辦公時間內？	◎			
7.53 是否訂定使用者及支援人員，對應用系統存取權限之管制措施？	◎			
7.54 處理機密及敏感性資訊，是否採用專屬（隔離）電腦作業環境？	◎			
7.55 是否訂定行動運算及通信設備之管理政策（如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求）？	◎			
7.56 遠距工作是否得到管理階層授權（如活動政策、計畫及流程等）和施以必要之保護措施？	◎			

附錄 9 通訊傳播事業個資保護控制措施內部稽核表

通訊傳播事業個資保護控制措施內部稽核表				
檢查項目 （以下之檢查項目編號，係參考附錄 6）	個資保護控制措施	檢查結果		
		符合	不符合	不適用
7.57 遠距工作活動結束後，是否撤銷相關授權與存取權限及歸還管制設備？	◎			
9.資訊安全事故管理				
9.1 是否建立資安事故（含安全漏洞、系統弱點、病毒、非法入侵及系統異常）之正式通報應變程序？	◎			
9.2 事故回應小組是否建立單一聯繫窗口，授權在處理事故時採取立即之決定，並與外部團體（例如：執法機關、政府緊急應變中心、客戶、商業夥伴）建立聯繫管道？	◎			
9.3 資訊安全事故處理過程，是否留有完整記錄，如有必要，應經由直接發送電子郵件及/或網站首頁，及時回報事故給相關客戶？	◎			
9.4 是否建立資訊安全事故通報之聯絡點，並確保全組織都知道該聯絡點，隨時可聯繫，能夠有充分與及時的回應？	◎			
11.遵循性				
11.13 資訊系統是否定期進行安全技術符合性檢查（如滲透測試或系統弱點檢測）？	◎			
11.14 技術遵循性之查核人員是否經過訓練，並作事前工作分配？	◎			
11.15 技術遵循性檢查是否由合格資安技術單位執行？	◎			
11.16 技術遵循性查核時之存取行為，是否作監控，並適當保存紀錄？	◎			
11.17 技術遵循性查核結果是否文件	◎			

附錄 9 通訊傳播事業個資保護控制措施內部稽核表

通訊傳播事業個資保護控制措施內部稽核表				
檢查項目 （以下之檢查項目編號，係參考附錄 6）	個資保護控制措施	檢查結果		
		符合	不符合	不適用
化？				
11.18 是否訂定資訊安全內部稽核計畫（含稽核目標、範圍、時間、程序、人員）？	◎			
11.19 是否定期辦理資訊安全內部稽核？	◎			
11.20 內部稽核範圍是否含括資通系統、供應商、資產負責人、使用者和管理階層？	◎			
合計	90			

附錄 10 國家通訊傳播委員會資通安全事故通報單

國家通訊傳播委員會通報小組 電話：(02) 2343-3560／2343-3768 傳真：(02) 2343-3556 或 e-mail：jmpd@ncc.gov.tw

行政院國家資通安全會報通報應變組 電話：(02) 2733-9922、0932-214-565 傳真：(02) 2733-1655 或逕送：106 台北市大安區富陽街 116 號

填報時間： 年 月 日 時 分 編號：

一、發生資通安全事故之通訊傳播事業聯絡資料：

通訊傳播事業名稱： 部門：

通報人：

電話： 傳真： E-mail：

二、各通訊傳播事業因受外在因素所產生資通安全事故時通報事項：

1.事故發生時間： 年 月 日 時 分

2.設備資料：

◎IP 位址（IP Address）：

外部 IP： 內部 IP： （無；可免填）

◎網際網路位址（Web-URL）： （無；可免填）

◎設備廠牌、機型：

◎作業系統名稱、版本：□Windows 系列□Linux 系列 □其他作業平台 版本：

◎已裝置之安全機制：□防火牆 □防毒軟體 □入侵防禦系統 □其他：

3.資通安全事故資料：

◎請分別評估資安事故造成之機密性、完整性以及可用性衝擊：

資安事故影響等級為機密性、完整性及可用性衝擊最嚴重者(數字最大者)

－機密性衝擊：(單選)

□機密資料遭洩漏(4 級)

□密級或敏感公務資料遭洩漏(3 級)

□非屬密級或敏感之關鍵業務資料遭洩漏(2 級)

□非關鍵業務資料遭洩漏(1 級)

□無資料遭洩漏(無需通報)

－完整性衝擊：(單選)

□重要資訊基礎建設系統或資料遭竄改(4 級)

□關鍵業務系統或資料遭嚴重竄改(3 級)

□關鍵業務系統或資料遭輕微竄改(2 級)

□非關鍵業務系統或資料遭竄改(1 級)

□無系統或資料遭竄改(無需通報)

－可用性衝擊：(單選)

□重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內，回復正常運作(4 級)

□關鍵業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作(3 級)

□關鍵業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作(2 級)

□非關鍵業務運作遭影響或短暫停頓(1 級)

□無系統或設備運作受影響(無需通報)

◎事故分類：（單選）□非法入侵 □感染病毒 □阻斷服務 □其他：
◎破壞程度：(單選）□系統當機 □資料庫毀損 □網頁篡改 □其他：
◎事故說明：(請勿超過 200 中文字）

◎可能影響範圍及損失評估：(請勿超過 200 中文字）

◎是否影響其他機關(構)或重要民生設施運作：□是 □否
◎應變措施：(請勿超過 200 中文字）

三、期望支援項目：(文字勿超過 200 中文字）
◎是否需要支援：□是（請續填期望支援內容） □否（免填期望支援內容）
期望支援內容：(請勿超過 200 字）

四、解決辦法：
◎是否同時結案：□是（請續填解決辦法及解決時間） □否（免填解決辦法及解決時間）
解決辦法：(請勿超過 200 字）

五、已解決時間：　　年　　月　　日　　時　　分

附錄 11 資通安全管理矯正／預防措施一覽表

公司名稱			
單位名稱			
單位主管		評估日期：	
承辦人員		評估日期：	
聯絡窗口	電話：	傳真：	行動：
	Email：		頁次：第　頁/共　頁

表單編號	檢查項目編號	矯正／預防措施概述	結案狀態		備註
			結案／未結案	完成日／預計完成日	

附件 4

附錄 12 資通安全管理矯正／預防措施單

<table>
<tr><td>公司名稱</td><td colspan="3"></td></tr>
<tr><td>單位名稱</td><td colspan="3"></td></tr>
<tr><td>單位主管</td><td></td><td>評估日期：</td><td></td></tr>
<tr><td>承辦人員</td><td></td><td>評估日期：</td><td></td></tr>
<tr><td rowspan="2">聯絡窗口</td><td>電話：</td><td>傳真：</td><td>行動：</td></tr>
<tr><td colspan="2">Email：</td><td>頁次：第　頁/共　頁</td></tr>
<tr><td>檢查項目
內容</td><td colspan="3"></td></tr>
<tr><td>提出</td><td colspan="3">不符合事項說明（發現日期：　　年　　月　　日）：</td></tr>
<tr><td rowspan="3">矯正預防</td><td colspan="3">1.原因調查分析：</td></tr>
<tr><td colspan="3">2.矯正措施：</td></tr>
<tr><td colspan="3">3.預防措施：</td></tr>
<tr><td>確認</td><td colspan="3">結案與否：☐是（結案日期：　　年　　月　　日）
☐否（預定結案日期：　　年　　月　　日）

措施成效確認（未結案案件不需填寫）：</td></tr>
</table>

附件 4

附錄 13 內部稽核表檢查項目勾選不適用之說明

公司名稱			
單位名稱			
單位主管		評估日期：	
承辦人員		評估日期：	
聯絡窗口	電話：	傳真：	行動：
	Email：		頁次：第　頁/共　頁
檢查項目編號	說明不適用理由或提出佐證資料		

備註：本表如不敷使用時，請自行增加頁數。

附件 4

附錄 14 增項稽核表檢查項目勾選不適用之說明

公司名稱			
單位名稱			
單位主管		評估日期：	
承辦人員		評估日期：	
聯絡窗口	電話：	傳真：	行動：
	Email：		頁次：第　頁/共　頁
檢查項目編號	說明不適用理由或提出佐證資料		

備註：本表如不敷使用時，請自行增加頁數。

附件 4

通訊傳播事業資通安全管理手冊

修訂建議草案(英文版)

Information and Communication Security Manual for Communication and Broadcasting Industries (amended draft)

National Communications Commission

October 2011

Contents

1. Basis **1**

2. Purpose **1**

3. Descriptions of key topics **2**

(1) ICS standards 2
(2) Evaluating ICS levels 2
(3) ICS policy and training 3
(4) The required ICS training hours 5
(5) Personal data protection 5
(6) ICS reports and responses 6
(7) Assessment on the implementation of ICS 7
(8) Annual reporting requirements. 7

Appendix **10**

Appendix 1 Communication and broadcasting businesses ICS level self-assessment **10**

Appendix 2 Communication and broadcasting businesses ICS level description **10**

Appendix 3 Communication and broadcasting businesses ICS detailed risk assessment sheet **10**

Appendix 4 Communication and broadcasting businesses sample of ICS policy implementation plan **10**

Appendix 5 List of ICS implementation tasks **10**

Appendix 6 Communication and broadcasting businesses ICS internal audit worksheet (with revision history) **10**

Appendix 7 List of additional audit focuses for communication businesses **10**

Appendix 8 List of additional audit focuses for broadcasting businesses **10**

Appendix 9 Personal data protection and security measures **10**

Appendix 10 National Communications Commission ICS incidental report **10**

Appendix 11 List of ICS rectifications / precautions **10**

Appendix 12 ICS rectification / precaution order **10**

Appendix 13 Descriptions on non-applicable items specified in the internal audit worksheet **10**

Appendix 14 Descriptions on non-applicable items specified in the list of additional audit focuses **10**

Information and Communication Security Manual for Communication and Broadcasting Industries

1. Basis

This manual was created according to Note 2 of the Guidelines on Information and Communication Security Management for Communication and Broadcasting Businesses[1], and is aimed to provide industry-wide governance and to guide all target businesses through their implementation of information and communication security policies.

The clauses below were added to accommodate the addition of Section 56 to the Telecommunications Act: carriers are required to complete the following objectives in order to ensure the security of its equipment, data, and network, thereby securing users' interests in using communication services:
1. Establish an information and communication security policy.
2. Establish information and communication protection and detection facilities.
3. Establish a joint defense mechanism which enforces information and communication security, and create measures for reporting, handling, and responding security events.

Communication and broadcasting businesses are advised to make arrangements in the earliest time possible to build their own corporate risk cultures and fulfill their legal obligations.

2. Purpose

To ensure information and communication security[2], protect users' interests, and warrant the security of equipment, data, and networks used in communication and broadcasting[3]. The manual addresses the following key topics:
(1) ICS standards.
(2) Evaluating ICS levels.
(3) ICS policy and training.
(4) ICS reports and responses.
(5) Assessment on the implementation of ICS.
(6) Annual reporting requirements.

---

[1] Communication and broadcasting businesses: refer to businesses that are involved in communication or broadcasting

[2] Information and communication security shall be abbreviated as ICS.

[3] Communication and broadcasting: refers to the transmission of audio, video, text, or data through wired or wireless means, satellite, or other electronic transmission devices

3. Descriptions of key topics

(1) ICS standards.

Communication and broadcasting businesses are advised to refer to the Chinese National Standards (CNS) or ISO/IEC 27000 standards below when implementing ICS policies over their target businesses:

A. ICS system requirements: CNS/ISO/IEC 27001

B. ICS processes: CNS/ISO/IEC 27002

C. ICS system implementation guidelines: ISO/IEC 27003

D. ICS measurement methods: ISO/IEC 27004

E. ICS risk management: CNS/ISO/IEC 27005

F. ICS practical guides for carriers: ISO/IEC 27011

(2) Evaluating ICS levels

A. Communication and broadcasting businesses should follow the steps below and conduct High-Level Risk Assessments to evaluate their ICS level, define ICS coverage and boundary, and ascertain their own ICS requirements. The outcome of the assessment shall provide references for prioritizing companies' efforts toward future risk events:

(A) Identify the asset groups needed by communication and broadcasting businesses to perform their licensed activities. Organizations of substantial sizes may identify asset groups according to business segments or departments and classify into the three main categories below:

- Principal activities:

  Which may include the following items:

  For carriers - telecommunication equipment, networking equipment, microwave radio station, wiring infrastructure, terminal equipment, etc.

  For cable radio and TV enterprises - head end, signal processor, distribution network, distribution hub, fiber node, subscribers' terminal equipment, etc.

  For wireless radio and TV enterprises - broadcasting station, relay station, booster station, cables, signal processors, etc.

  For satellite radio and TV enterprises - Earth station, satellite institution, satellite transponder, etc.

- Supporting activities:

  This category includes data processing facilities needed by communication and broadcasting businesses to perform non-principal activities such as: customer service, bookkeeping, accounting, or the collection, processing, or uses of customers' personal information.

- Administrative activities:

  This category includes assets that are used by administrative functions within

communication and broadcasting businesses; e.g.: human resources, administration, general affairs, etc.

(B) Evaluate the asset security level based on the "degree of impact" under the circumstance that each asset group fails to function. Prioritize improvements to the ICS policy and update on an annual basis.

(C) Fill out the "Communication and broadcasting businesses ICS level self-assessment" (see Appendix 1) and the "Communication and broadcasting businesses ICS level description" (see Appendix 2).

B. Steps toward evaluating ICS levels:

(A) Consolidate all assets needed by communication and broadcasting businesses to perform "Principal activities", "Supporting activities", and "Administrative activities"; establish ICS policy based on their asset security level.

(B) For each asset group, evaluate the impacts of failure in the following aspects: "Loss of reputation", "Casualty", "Business disruption", "Damage to data protection", "Regulatory compliance", and "Others". Assign asset security levels "Ordinary", "Medium", and "High" based on the assessed impacts.

(C) The degree of impact given the failure of a particular asset group is evaluated based on the highest rating assessed for the various aspects; i.e. if the degree of impact is rated "High" in any aspects of the asset group, then the ICS level shall be determined as "High" for the entire asset group. If the degree of impact is rated "Ordinary" in all aspects, then the asset security level shall be determined as "Ordinary" for the entire asset group.

(D) Finally all the assets security level of the asset groups are assessed. Whichever is highest as a basis for enterprise security rating, and then carry out the assessment of the assets security levels as “A”, “B”, or “C”. For example, the highest security level of asset groups to "high", its enterprise security level to "A" grade; such as the highest security level of asset groups of "medium", their enterprise security level to "B" grade; such as the highest security level of asset groups of "fair", their enterprise security level to "C" grade.

(3) ICS policy and training

A. Communication and broadcasting businesses with asset groups rated "High" may refer to the CNS/ISO/IEC 27005 standards if necessary to conduct Detailed Risk Assessments (see Appendix 3), or define their own risk management practices to determine appropriate risk strategies.

B. Communication and broadcasting businesses need to conduct self-assessments to determine the ICS levels and plan for their ICS policy implementation. The implementation plan must cover the following items and is subject to internal audits once a year (see Appendix 4 for a sample of ICS policy implementation plan).

C. Communication and broadcasting businesses shall plan for the implementation of their ICS policies according to the "List of ICS implementation tasks" (Appendix 5), and complete the following tasks on a yearly basis depending on the corresponding ICS levels:

(A) Depth of protection

- For those whose enterprise security levels are rated "A", the depth of protection must at least include the establishment of a firewall, an intrusion detection system (IDS), an intrusion prevention system (IPS), anti-virus software, junk mail filter, webpage filter, and network security monitoring equipment. These protection measures must deliver the level of security expected from advanced equipment, as defined in the "Guidelines on the Inspection of Information and Communication Security Equipment (draft)".
- For those whose enterprise security levels are rated "B", the depth of protection must at least include the establishment of a firewall, IDS, IPS, anti-virus software, and junk mail filter. These protection measures must deliver the level of security expected from fundamental equipment, as defined in the "Guidelines on the Inspection of Information and Communication Security Equipment (draft)".
- For those whose enterprise security levels are rated "C", the depth of protection must at least include the establishment of a firewall, IDS, IPS, anti-virus software, and junk mail filter.

(B) Implementation method

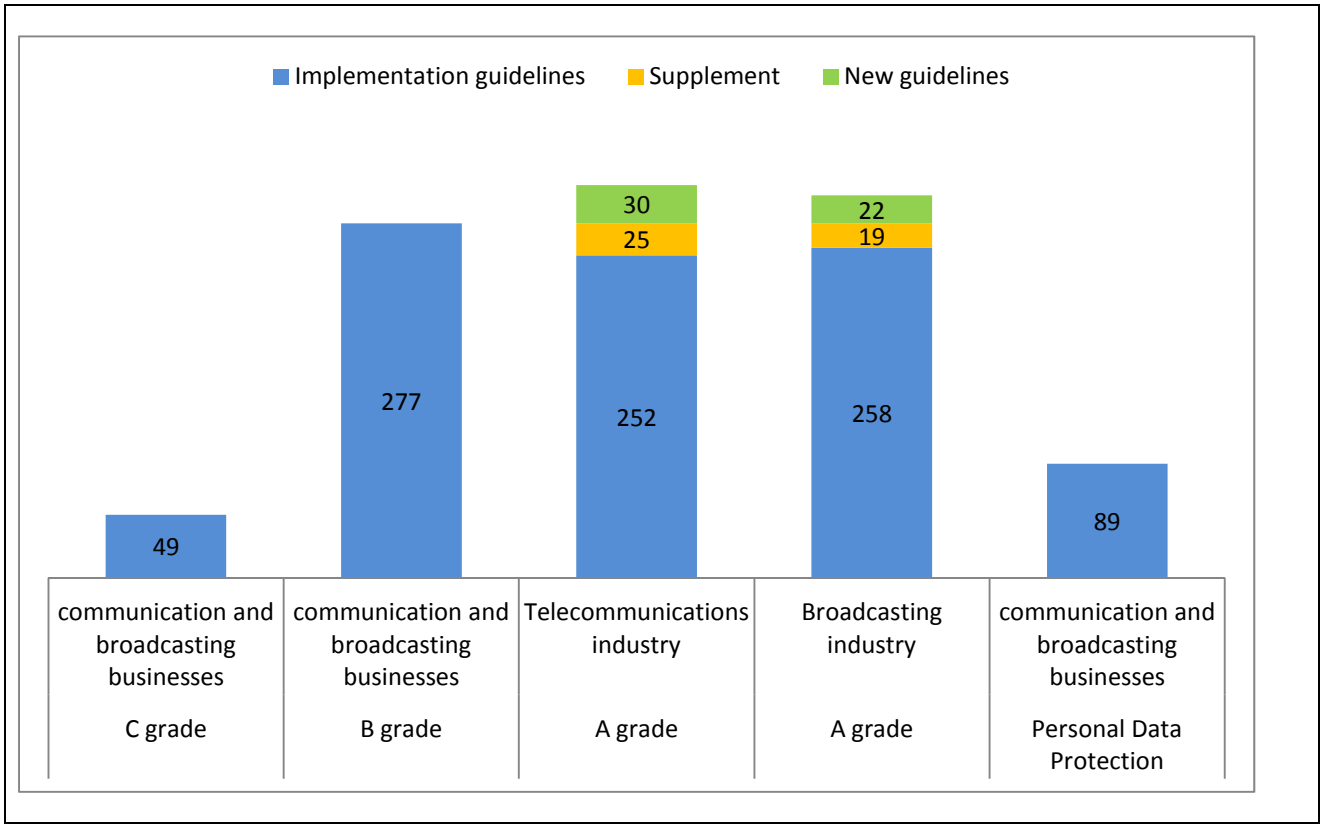


Figure 1 Security Protection Standards Applicable to Communication and Broadcasting Businesses - by ICS Levels

All communication and broadcasting businesses must assemble their own ICS Action Teams to create ICS policies in one of three levels: "A", "B", and "C", depending on the applicable security level. See Figure 1 for details.

- If enterprise security level is rated "C", the minimum security requirement under the "ICS internal audit worksheet" is applicable (see Appendix 6).
- If enterprise security level is rated "B", the full control under the "ICS internal audit worksheet" is applicable.
- If enterprise security level is rated "A", the full control under the "ICS internal audit worksheet" is applicable. In addition, the "List of additional audit focuses for communication businesses" (see Appendix 7) or the "List of additional audit focuses for broadcasting businesses"(see Appendix 8) may also apply wherever appropriate. Companies with ICS levels rated "High" shall make progressive improvements throughout the organization and aim to pass the ICS system certification of a third-party institute.
- Please see Appendix 9 for a list of security measures applicable for the protection of personal data, files, and information.

(C) Audit method

- Perform internal audits at least once a year.
- Asset groups which pass the ICS system certification are exempted from the internal audit, and are subject to regular updates.

(4) The required ICS training hours

In order to promote employees' proper awareness toward ICS and improve the intensity of security protection, all communication and broadcasting businesses are required to organize internal ICS training. Appendix 5 has outlined the minimum hours of ICS training and promotion required per year:

- Supervisors, IT/communication personnel, business personnel, and general staffs must complete 3, 12, 6, and 3 hours of ICS training, respectively, on a yearly basis.

(5) Personal data protection

A. If the ICS implementation plan involves collecting, processing, or making uses of personal data, then the company must comply with the Personal Information Protection Act and implementation rules thereof to establish its policies on "Personal data security maintenance plan" and "Handling of non-business personal data". In addition, the company must also ensure to undertake proper security measures and keep audit trails on personal data gathering, processing, and utilization as evidence to its due diligence.

B. The notion of proper security maintenance measures, security maintenance tasks, or proper security measures refer to any attempts taken by communication and broadcasting businesses, whether through technological improvements or internal discipline, to protect personal data from theft,

alteration, damage, loss, or unauthorized disclosure. These measures may include the following:

(A) Assembling a dedicated administrative team and configuring considerable resources.
(B) Outlining the boundary in which personal data may circulate.
(C) Risk assessment and management mechanisms of personal data.
(D) The accident prevention, reporting and response mechanisms change.
(E) Internal management procedure for personal data collection, processing, and utilization.
(F) Data security management and member management.
(G) Advocacy and awareness training.
(H) Equipment management.
(I) Data audit mechanism.
(J) Retention of access records and evidence.
(K) Personal information to improve the overall maintenance.
(L) Other efforts relating to security maintenance. For example: policy for the handling of non-business data.

The necessity of the abovementioned measures is limited to the amount of costs needed to accomplish the intended protection on personal data to a proper extent.

C. If the communication or broadcasting business serves as a consignee to collect, process, or make use of personal data on behalf of others, all conducts within the governance of the Personal Information Protection Act will be treated as the actions of the consignor. The consignor must exercise proper supervision over the consignee, with respect to the following details:

(1) The extent, types, purposes, and timeframe at which the consignee is expected to gather, process, or make use of personal data.
(2) Measures taken by the consignee to secure and audit personal data, manage equipment, and carry out security maintenance.
(3) Any additional agreements for re-consigning to others.
(4) Issues which must be reported to the consignor should the consignee or its employees violate against the Personal Information Protection Act, or against the terms of the consignment agreement.
(5) The consignor's instructions to the consignee.
(6) The return of storage device carrying personal data, and the removal of personal data saved on the consignee's storage upon the expiry or termination of the consignment relationship.

(6) ICS reports and responses

All communication and broadcasting businesses must establish systematic responses to ICS incidents. When an ICS incident arises, companies must take proper responsive measures and report immediately to the commission by completing the "National Communications Commission ICS incidental report"

(Appendix 10).

(7) Assessment on the implementation of ICS

A. Internal audit

All communication and broadcasting businesses must perform annual self-assessments to determine the security levels of their various asset groups; and based on which the suitable security measures are chosen. Internal audits are conducted at least once a year, and the audit findings shall be reported in the relevant appendices of this manual:

The following rules apply when conducting internal audits according to Appendices 6, 7, and 8:

(A) Supporting documents must be attached for any audit items answered with a "Yes".

(B) The "List of ICS rectifications / precautions" (Appendix 11) and the "ICS rectification / precaution order" (Appendix 12) must be completed for any audit items answered with a "No".

(C) For audit items answered with "Not applicable", the "Descriptions on non-applicable items specified in the internal audit worksheet" (Appendix 13) and the "Descriptions on non-applicable items specified in the list of additional audit focuses" (Appendix 14) must be completed.

B. External certification

All communication and broadcasting businesses are encouraged to seek certification from external ICS system certifiers. The coverage of ICS system certification must be consistent with the CNS/ISO/IEC 27001 standards and the requirements specified in Appendices 7 and 8 to be considered effective.

The abovementioned certifier must be one that is recognized by the commission and approved through the nation's certification system. The commission will publish on it website all certified communication and broadcasting businesses.

C. Administrative inspections

Should any ICS incident listed in Appendix 10 occurs, for which the communication or broadcasting business rates the degree of impact at level 3 or 4, the company must prepare the relevant information below according to its self-rated ICS level for administrative inspection by the commission.

(A1) Descriptions on the execution of responsive measures toward major ICS incident.

(B) The ICS policy implementation plan.

(C) Supporting documents to all audit items listed in Appendix 11 ~ 13; or an audit report produced by a recognized ICS system certifier.

(8) Annual reporting requirements.

A. All communication and broadcasting businesses must report the following information to the commission based on their self-rated ICS levels no later than the end of September each year:

(A) Appendices 1, 2, 6, 7, and 8. Those in possession of personal data need to submit Appendix 9 as well.

(B) When conducting internal audits according to the Description to key topics No. 3(6), Appendices 11 and 12 must be submitted for audit items that are answered "No".

(C) When conducting internal audits according to the Description to key topics No. 3(6), Appendices 13 and 14 must be submitted for audit items that are answered "Not applicable".

B. For those who are certified by recognized ICS system certifiers and have obtained the ISO/IEC 27001 certificate, only Appendices 1, 2, 7 (or 8), and 14 are required. Although these companies are exempted from submitting Appendices 6 and 13, they must attach copies of certificate, certification report or other relevant documents.

C. For those who are certified by recognized ICS system certifiers and have achieved the ISO/IEC 27001 standard and are certified to have passed all additional ISO/IEC 27011 requirements listed in Appendix 7 (or 8), only Appendices 1 and 2 are required. Although these companies are exempted from submitting Appendices 6 ~ 14, they must attach copies of certificate, certification report or other relevant documents.

Table of Annual reporting

Distinguish	**Internal audit**	**External certification CNS/ISO/IEC 27001**	**External certification ISO/IEC 27011**
Appendix 1 Communication and broadcasting businesses ICS level self-assessment	**V**	**V**	**V**
Appendix 2 Communication and broadcasting businesses ICS level description	**V**	**V**	**V**
Appendix 6 Communication and broadcasting businesses ICS internal audit worksheet	**V**		
Appendix 7 List of additional audit focuses for communication businesses	⊙	⊙	
Appendix 8 List of additional audit focuses for broadcasting businesses	⊙	⊙	
Appendix 9 Personal data protection and security measures	⊙	⊙	⊙
Appendix 11 List of ICS rectifications / precautions	⊙		
Appendix 12 ICS rectification / precaution order	⊙		
Appendix 13 Descriptions on non-applicable items specified in the internal audit worksheet	⊙		
Appendix 14 Descriptions on non-applicable items specified in the list of additional audit focuses	⊙	⊙	

Distinguish	**Internal audit**	**External certification CNS/ISO/IEC 27001**	**External certification ISO/IEC 27011**
Remarks：**V** Must submit project ⊙ Submit the project as required			

Appendix

Appendix 1 Communication and broadcasting businesses ICS level self-assessment
Appendix 2 Communication and broadcasting businesses ICS level description
Appendix 3 Communication and broadcasting businesses ICS detailed risk assessment sheet
Appendix 4 Communication and broadcasting businesses sample of ICS policy implementation plan
Appendix 5 List of ICS implementation tasks
Appendix 6 Communication and broadcasting businesses ICS internal audit worksheet (with revision history)
Appendix 7 List of additional audit focuses for communication businesses
Appendix 8 List of additional audit focuses for broadcasting businesses
Appendix 9 Personal data protection and security measures
Appendix 10 National Communications Commission ICS incidental report
Appendix 11 List of ICS rectifications / precautions
Appendix 12 ICS rectification / precaution order
Appendix 13 Descriptions on non-applicable items specified in the internal audit worksheet
Appendix 14 Descriptions on non-applicable items specified in the list of additional audit focuses

Appendix 1 Communication and broadcasting businesses ICS level self-assessment

Company name								
Unit supervisor						Date of assessment:		
Assessor						Date of assessment:		
Contact	TEL:		Fax:			Mobile:		
	Email:							
Asset group	Activities category	Aspects / levels of impact (Note 2)						
		Loss of reputation	Casualty	Business disruption	Damage to data protection	Regulatory compliance	Others	ICS level
	☐ Principal							
	☐ Supporting							
	☐ Administrative							
	☐ Principal							
	☐ Supporting							
	☐Administrative							
	☐ Principal							
	☐ Supporting							
	☐ Administrative							
(Add more fields where appropriate)								

Guidelines to Appendix 1

Note 1: Types of business activities subject to ICS evaluation

Activities category	Description
Principal activities	For carriers - networking equipment, microwave radio station, wiring infrastructure, terminal equipment, etc. For cable radio and TV enterprises - head end, signal processor, distribution network, distribution hub, fiber node, subscribers' terminal equipment, etc. For wireless radio and TV enterprises - broadcasting station, relay station, booster station, cables, signal processors, etc. For satellite radio and TV enterprises - Earth station, satellite institution, satellite transponder, etc.
Supporting activities	Supporting activities: This category includes data processing facilities needed by communication and broadcasting businesses to perform non-principal activities such as: customer service, bookkeeping, accounting, or the collection, processing, or uses of customers' personal information.
Administrative activities	Administrative activities: This category includes assets that are used by administrative functions within communication and broadcasting businesses; e.g.: human resources, administration, general affairs, etc.

Note 2: Aspects of impact / security level

ICS level / **Aspects of impact**	**Ordinary (Level 1)**	**Medium (Level 2)**	**High (Level 3)**
1. Loss of reputation	● If a security incident occurs, the institution will suffer minor damage to its image and reputation.	● If a security incident occurs, the institution will suffer heavy damage to its image and reputation.	● If a security incident occurs, the institution will suffer severe damage to its image and reputation.
2. Casualty	● The occurrence of a security incident causes no casualties.	● The possibility of casualties caused by the occurrence of a security incident cannot be eliminated entirely.	● If a security incident occurs, it is very likely to cause injuries or even death.
3. Business disruption	● The system tolerates a longer downtime.	● The system tolerates a shorter downtime.	● If a security incident occurs, it is very

	● A system malfunction causes minor or even no impacts to the order of the society or to the public.	● A system malfunction causes major impacts to the order of the society or to the public. ● A system malfunction significantly reduces the efficiency of principal activities.	likely to cause injuries or even death. ● A system malfunction severely impairs the efficiency of principal activities, or even disrupts the entire business.

ICS level / Aspects of impact	Ordinary (Level 1)	Medium (Level 2)	High (Level 3)
4. Damage to data protection	● General information ● The leakage or alteration of information has no or little impacts on the interests of the individual.	● Sensitive information ● The leakage or alteration of information has major impacts on the interests of the individual.	● Confidential information ● The leakage or alteration of information has severe impacts on the interests of the individual, or causes damage to an extremely large number of individuals.
5. Regulatory compliance	Non-compliant system functioning, data protection, or use of information-related assets do not constitute violations against regulations.	Non-compliant system functioning, data protection, or use of information-related assets do constitute regulatory violations, and bear minor consequences such as administrative penalties or fines.	Non-compliant system functioning, data protection, or use of information-related assets constitute regulatory violations, and result in severe consequences such as damage compensation, fines, or even criminal liability.
6. Others	The communication/broadcasting business may consider other aspects of any possible impacts (e.g.: loss of property) and set measurement standards as deemed necessary.		

Appendix 2 Communication and broadcasting businesses ICS level description

Company name					
Unit supervisor			Date of assessment:		
Assessor			Date of assessment:		
Contact	TEL:		Fax:		Mobile:
	Email:				Page: of
Asset group	Activities category	Aspects of impact	Impact level		Reasons and descriptions
	□ Principal □ Supporting □ Administrative	Loss of reputation	Previous year		
			Current year		
		Casualty	Previous year		
			Current year		
		Business disruption	Previous year		
			Current year		
		Damage to data protection	Previous year		
			Current year		
		Regulatory compliance	Previous year		
			Current year		
		Others	Previous year		
			Current year		
(Add more fields wherever appropriate)	□ Principal □ Supporting □ Administrative	Loss of reputation	Previous year		
			Current year		
		Casualty	Previous year		
			Current year		
		Business disruption	Previous year		
			Current year		
		Damage to data protection	Previous year		
			Current year		
		Regulatory compliance	Previous year		
			Current year		
		Others	Previous year		
			Current year		

Appendix 3 Communications and Broadcastings industry Information Security Management Detailed Risk Assessment Table

NO.	Department	Custodian	Explain	Information assets	Asset classes	Quantity	Confidentiality	Integrity	Availability	The value of information assets	Threat	Vulnerability	Risk Estimation			
													Threat Level	Vulnerability rating	Value of risk	Level of risk

<Company name> Information and Communication Security Policy Implementation Plan

Document number:	ISMS-1-001
Version:	1.0
Document date:	1 November 2011
Level of confidentiality:	Restricted Access

Company LOGO

Document establishment / revision history

Establishment (revision) Version	Establishment (revision) Date	Description on establishment (revision)	Author	Remarks
V1.0	20111101	Initial publication	Information and Communication Security Action Team	

Contents

I. INFORMATION SECURITY POLICY 20

A. Information security goals 20
B. Goal execution 20

II. REQUIREMENTS BY REGULATIONS AND ADMINISTRATIVE ORDERS 22

A. Telecommunications Act 22
B. Personal Information Protection Act 22

III. THE INFORMATION AND COMMUNICATION SECURITY ORGANIZATION 23

IV. THE SCOPE OF INFORMATION AND COMMUNICATION SECURITY MANAGEMENT 24

A. Evaluating ICS levels 24
B. Steps toward evaluating ICS levels: 26

V. INFORMATION AND COMMUNICATION SECURITY POLICY 26

A. General requirements 26
B. Risk assessment method 27
C. Executed tasks 27
D. Implementation method 28
E. Audit method 30
F. ICS awareness training 30
G. ICS reports and responses 30
H. Assessment on the implementation of ICS 30
I. Annual reporting requirements 31

VI. ICS DOCUMENT MANAGEMENT 32

A. Level one document 33
B. Level two document 33
C. Level three document 33
D. Level four document 33
E. Approval of ICS documents 34

VII. ATTACHMENTS 34

I. Information security policy

The company is dedicated in introducing integrated services into the information and communication market with "customers relations, service qualities, innovation, and continual growth" as its primary goals. The company is also committed to developing mobile applications and enhancing retail service qualities to provide consumers the ultimate mobile lifestyle.

Driven by the most basic "human needs", the company centers its services around "customers" and continues to enhance its core strengths. Meanwhile, the company takes initiative in developing mobile business and network applications, and broadband multimedia through alliances and co-operations with other business partners. The broadened integration between telecommunication networks and information technologies has incorporated the company's services into the lifestyles of the public, and made it the preferred business partner for a wide range of companies.

In order to enhance information security management while ensuring the confidentiality, integrity, and accessibility of all assets used in information and communication, and promoting employees' awareness toward information security, the company has established this "Information and Communication Security Policy Implementation Plan" according to the national and international information security standards, and the "Information and Communication Security Manual for Communication and Broadcasting Industries" ("ICS Manual") promulgated by the competent authority. The goals of this policy are as follows:

A. Information security goals

(i) Improve corporate competitiveness

(ii) Reduce the risks of information/communication security

(iii) Raise efficiencies in information security management

B. Goal execution

(i) The promotion of information and communication security is a management issue which requires the support and participation of senior executives. All department supervisors must supervise their staffs to help achieve the company's information and communication security targets.

(ii) All employees must fully understand the importance of an ICS policy, and commit themselves to its establishment.

(iii) Ensure the confidentiality, integrity, and accessibility of all assets used for information/communication, thereby preventing unauthorized disclosures of sensitive and personal information.

(iv) All ICS protections and rules must comply with the regulations and orders promulgated by the competent authority and the requirements of relevant ICS policies.

(v) The company will provide ICS training courses to build up information security awareness and develop employees' information security management skills.

(vi) The company may segregate its licensed activities into different business segments or departments when investigating the asset groups needed for business operations, and apply the ICS evaluation methods specified by the competent authority for impact analysis and risk assessment, in order to determine the most appropriate scope of coverage.

(vii) All assets covered by the information and security framework are subject to proper protection and security measures, and regular rehearsals on backup/recovery.

(viii) All security incidents and suspected security weaknesses must be reported and highlighted immediately according to procedures, and are subject to proper investigations and handling.

(ix) Any security issues raised must be discussed immediately. Find solutions to improve the current practices and strengthen the information security management system.

(x) Identify problems associated with information security through audit procedures; recommend improvements that will reduce the risks of information security.

(xi) Violations against this policy or any relevant rules on information security are subject to the company's disciplinary review or penalties by law.

(xii) Provide any technical assistance necessary to enforce information and communication security in outsourced vendors and third-party organizations.

(xiii) Take into consideration the time and resources available; list out the company's priorities and implement information security progressively throughout the entire company. Aim to pass the certification of an external certifier. The coverage of the ICS system certification must be consistent with the CNS/ISO/IEC 27001 standards and the competent authority's requirements.

(xiv) This policy is subject to annual regular reviews to reflect the latest changes in government regulations, technological development, and business requirements.

(xv) This policy is subject to review by the Information and Communication Security Action Team, and becomes effective once approved by the Chairman. The same applies to all subsequent revisions.

II. Requirements by regulations and administrative orders

All company employees must prepare in advance for the regulatory requirements below in order to build up proper risk culture and fulfill legal obligations:

A. Telecommunications Act

The newly Section 56 of the Telecommunications ActCarriers are required to complete the following objectives in order to ensure the security of its equipment, data, and network, thereby securing users' interests in using communication services:

(i) Establish an information and communication security policy.

(ii) Establish information and communication protection and detection facilities.

(iii) Establish a joint defense mechanism which enforces information and communication security, and create measures for reporting, handling, and responding to security events.

B. Personal Information Protection Act

Section 27 All non-government institutions in possession of personal data or files must undertake proper security measures to protect personal data from theft, alteration, damage, loss, or unauthorized disclosure.

III. The information and communication security organization

The company has designated the audit supervisor as its Head of Information Security, and assembled an Information and Communication Security Action Team consisting of deputy supervisors from various departments. The organizational structure is depicted in Figure.1. This organization is responsible for promoting the following tasks:

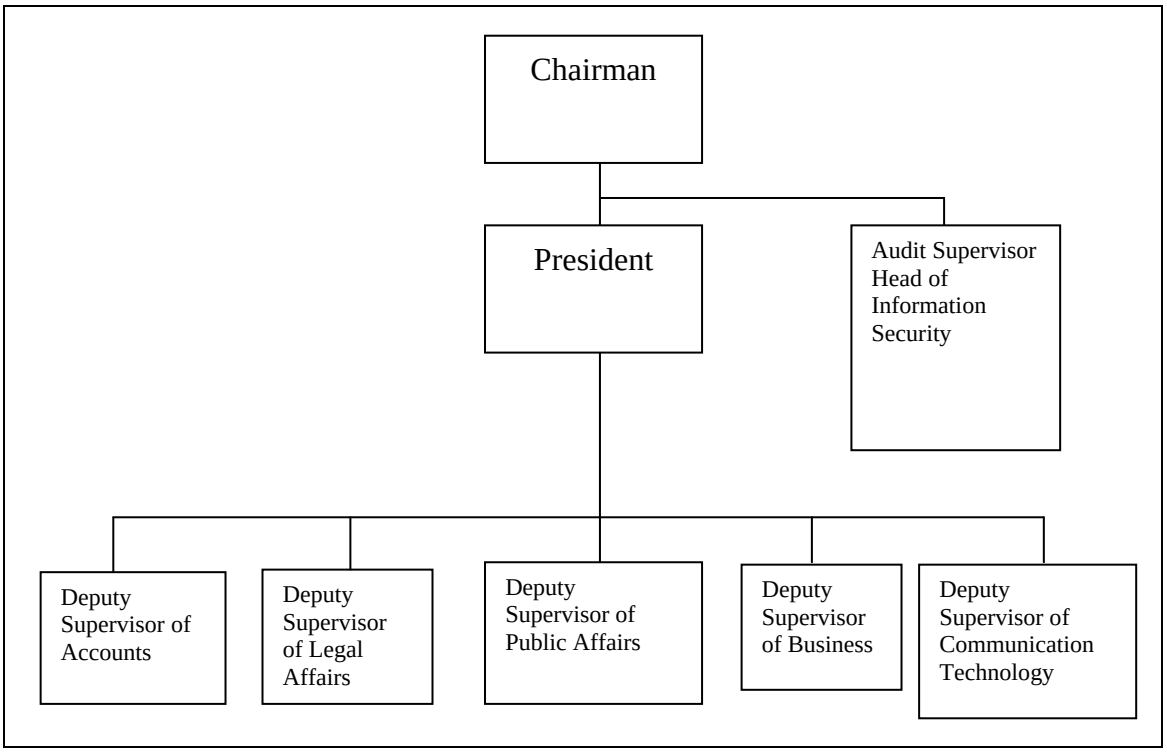


Figure.1 Structure of the company's Information and Communication Security Action Team

(1) The drafting of information security policies.

(2) Coordination and allocation of responsibilities within the information security organization.

(3) Policy-making for the security management of information-related assets.

(4) Policy-making for personnel management and information security training.

(5) Policy-making for the security of physical equipment and the business environment.

(6) Policy-making for the communication business and the related processes.

(7) Policy-making for access control.

(8) Policy-making for system acquisition, development, and security

maintenance.

(9) Policy-making for security incident management.

(10) Policy-making for continuing business operation.

(11) Policy-making for regulatory compliance.

(12) Policy-making for other security management issues.

(13) The handling and execution of other affairs relating to the information security management system.

IV. The scope of information and communication security management

Identify all asset groups incorporated by the company to perform its licensed business activities; evaluate the information and communication security level for each asset group.

A. Evaluating ICS levels

ICS levels are evaluated based on the three main activities below. Businesses of substantial size may conduct asset group evaluation in smaller business segments or departments.

(i) Principal activities

1. Type I telecommunication
   Refers to networking equipment, microwave radio station, wiring infrastructure, terminal equipment, etc., incorporated within the company's Type I telecommunication license to perform the following activities:

   - Fixed network telecommunication
   - Mobile network telecommunication
   - Fixed satellite telecommunication

2. Type II telecommunication
   Refers to networking and terminal equipment incorporated within the company's Type II telecommunication license to perform the following activities:

   - Data exchange
   - Internet connection

- Non-E. 164 Internet telephony
- E. 164 Internet telephony
- Intranet communication
- Call conferencing
- Network access
- Video conferencing

3. Broadcasting business
   Refers to head end, signal processor, distribution network, distribution hub, fiber node, subscribers' terminal equipment, broadcasting station, relay station, booster station, cables, Earth station, satellite institution, satellite transponder, etc., incorporated within the company's broadcast license to perform the following activities:

   - Cable radio and TV
   - TV broadcasting
   - Satellite radio and TV

(ii) Supporting activities

1. Resale of Type II telecommunication services
   Refers to information processing facilities needed to perform the resale and supporting services permitted under the company's Type II telecommunication license, which include the following:

   - Voice simple resale service
   - Wholesale resale service
   - Bandwidth resale service
   - Store and forward network
   - Premium rate voice information service
   - MVNO resale service
   - MVNO resale and value-added

2. Radio and television program supply
   Refers to data processing facilities incorporated by the company to make radio and television program supplies. They include systems used in: customer service, bookkeeping, accounting, or the collection, processing, or use of customers' personal information.

(iii) Administrative activities

Refers to the company's administrative functions such as: human resources, administration, general affairs, etc.

Evaluate the ICS level based on the "degree of impact" under the circumstance that each asset group fails to function. Prioritize improvements to the ICS policy and update on an annual basis.

Upon completing the evaluation, fill out the "ICS level self-assessment" sheet (see Attachment 1 of the ISMS manual) and the "ICS level description" (see Attachment 2 of the ISMS manual).

B. Steps toward evaluating ICS levels:

(i) Consolidate all assets needed to perform "Principal activities", "Supporting activities", and "Administrative activities"; establish ICS policy based on their priorities.

(ii) For each asset group, evaluate the impacts of failure in the following aspects: "Business disruption", "Damage to data protection", and "Regulatory compliance". Assign security levels "Ordinary", "Medium", and "High" based on the assessed impacts.

(iii) The degree of impact given the failure of a particular asset group is evaluated based on the highest rating assessed for the various aspects; i.e. if the degree of impact is rated "High" in any aspect of the asset group, then the ICS level shall be determined as "High" for the entire asset group. If the degree of impact is rated "Ordinary" in all aspects, then the ICS level shall be determined as "Ordinary" for the entire asset group.

V. Information and communication security policy

A. General requirements

The company implements, enforces, executes, monitors, reviews, maintains, and improves information and communication security based on the risks involved in its overall business activities. It adopted the PDCA model (Plan, Do, Check, Act) to establish its information and communication security policy, as depicted in Figure.2, and complied with the rules on "Information and Communication Security Manual for Communication and Broadcasting Industries" promulgated by the competent authority.

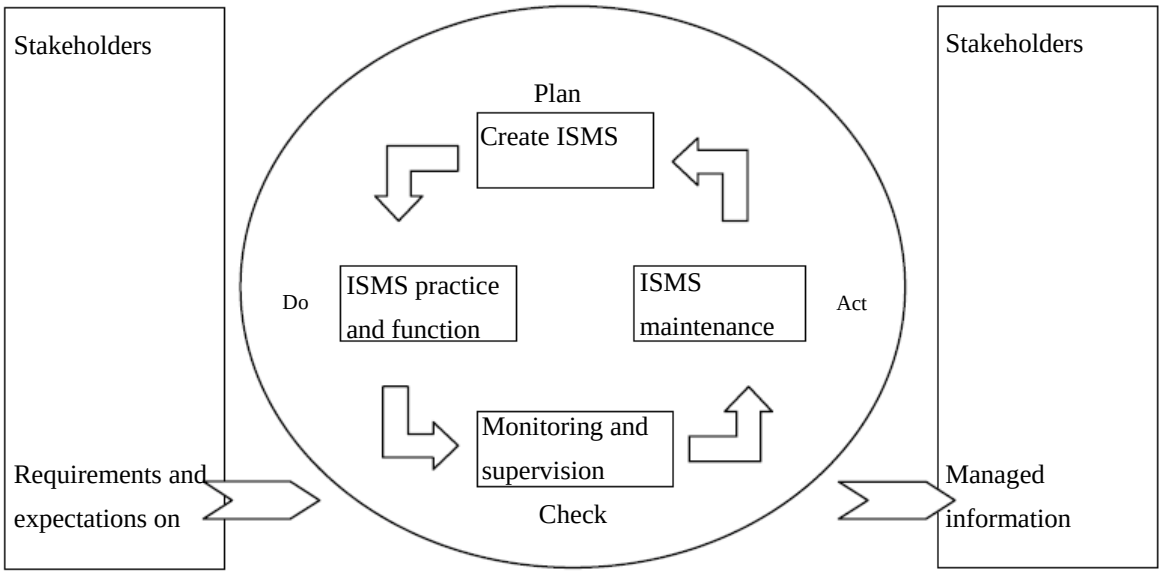


Figure.2 The PDCA model incorporated in the information and communication security policy

B. Risk assessment method

For asset groups above whose security levels are rated "High", the company may refer to the CNS/ISO/IEC 27005 standards if necessary to conduct Detailed Risk Assessments and determine appropriate risk strategies (see Attachment 3 of the ISMS manual).

C. Executed tasks

Once the security levels of the abovementioned asset groups have been finalized, the company will complete the following tasks according to the approved security levels, as shown in Table 1:

Table 1 List of ICS implementation tasks

Name of process / Contents / Level	Data processing facilities / Depth of protection	Implementation method	Audit method	ICS training hours (for supervisors, IT/communication personnel, business personnel, and general staffs, respectively)	Personal data protection
High	Firewall, IDS, IPS, anti-virus software, junk mail filter, webpage filter, and network security monitoring equipment. These protection measures must deliver the level of security expected from advanced equipment, as defined in the "Guidelines on the Inspection of Information and Communication Security Equipment (draft)"	Aim to pass the certification of a third-party ISMS certifier	Perform internal audits at least once a year.	At least 3, 12, 6, and 3 hours per year	Companies that deal with personal data must establish personal data security plans and undertake proper security measures according to the implementation rules of the Personal Information Protection Act
Medium	Firewall, IDS, IPS, anti-virus software, and junk mail filter. These protection measures must deliver the level of security expected from fundamental equipment, as defined in the "Guidelines on the Inspection of Information and Communication Security Equipment (draft)".	Outline and assemble an ICS Action Team	Perform internal audits at least once a year.	At least 3, 12, 6, and 3 hours per year	
Ordinary	Firewall, IDS, IPS, anti-virus software, and junk mail filter	Enhance propaganda on information and communication security	Perform internal audits at least once a year.	At least 3, 12, 6, and 3 hours per year	

D. Implementation method

Once the security levels have been finalized, the company shall assign proper security standards and establish ISC policies for the various asset group ratings - "Ordinary", "Medium", and "High". See Figure.3.

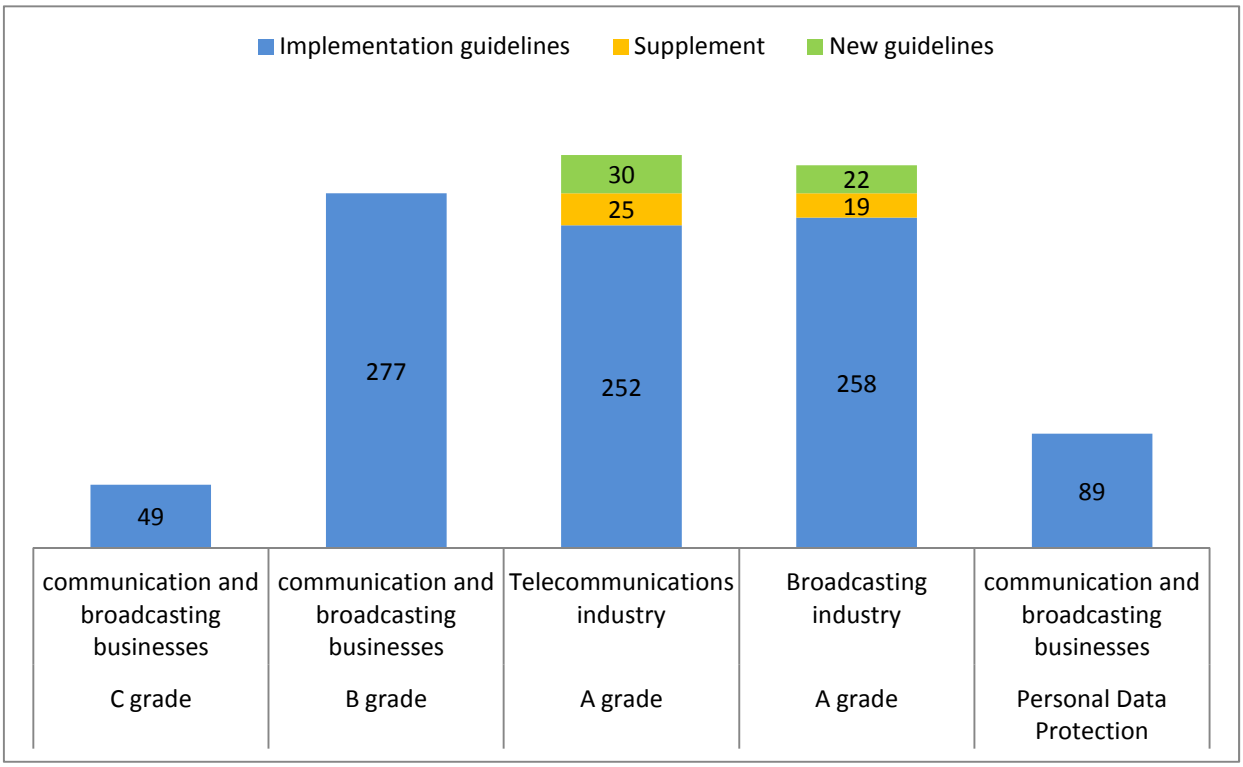


Figure.3 Security Protection Standards Applicable to Communication and Broadcasting Businesses - by ICS Levels

(i) If ICS level is rated "Ordinary", the minimum security requirement under the "ICS internal audit worksheet" is applicable (see Attachment 6 of the ISMS manual).

(ii) If ICS level is rated "Medium", the full control under the "ICS internal audit worksheet" is applicable.

(iii) If ICS level is rated "High", the full control under the "ICS internal audit worksheet" is applicable. In addition, the "List of additional audit focuses for communication businesses" (see Attachment 7 of the ISMS manual) or the "List of additional audit focuses for broadcasting businesses" (see Attachment 8 of the ISMS manual) may also apply depending on the type of business activities. Companies with ICS levels rated "High" shall make progressive improvements throughout the organization and aim to pass the ICS system certification by a third-party institute.

(iv) Companies that deal with personal data must establish personal data security plans according to the Personal Information Protection Act, and undertake suitable security measures for personal data protection (please refer to Attachment 9 of the ISMS manual).

E. Audit method

(i) Perform internal audits at least once a year.

(ii) Asset groups which pass the ICS system certification are exempted from the internal audit, and are subject to regular updates.

F. ICS awareness training

In order to promote employees' proper awareness toward ICS and improve the intensity of security protection, all communication and broadcasting businesses are required to organize internal ICS training. The minimum hours of ICS training and promotion required per year are as follows:

Supervisors, IT/communication personnel, business personnel, and general staffs must complete 3, 12, 6, and 3 hours of ICS awareness training, respectively, on a yearly basis.

G. ICS reports and responses

Companies must establish systematic responses for ICS incidents. When an ICS incident arises, companies must take proper responsive measures and report immediately to the competent authority by completing the "National Communications Commission ICS incidental report" (see Attachment 10 of the ISMS manual).

H. Assessment on the implementation of ICS

(i) Internal audit

The company must conduct internal audits at least once per year before the end of August. All audit findings must be documented with the following details:

The additional documents below are required when conducting internal audits according to Attachments 6, 7, and 8:

(1) Supporting documents must be attached for any audit items answered with a "Yes".

(2) The "List of ICS rectifications / precautions" (Attachment 11 of the ISMS manual) and the "ICS rectification / precaution order" (Attachment 12 of the ISMS manual) must be completed for any audit items answered with a "No".

(3) For audit items answered with "Not applicable", the "Descriptions on non-applicable items specified in the internal audit worksheet" (Attachment 13 of the ISMS manual) and the "Descriptions on

non-applicable items specified in the list of additional audit focuses" (Attachment 14 of the ISMS manual) must be completed.

(ii) Administrative inspections

Should the company encounter any security incidents rated at level 3 or 4, all relevant information below must be prepared within 3 days for administrative inspection by the competent authority.

(1) Descriptions on the execution of responsive measures toward major ICS incidents.
(2) The ICS implementation plan and its execution results.
(3) Supporting documents to all audit items listed in Attachments 11 ~ 13 of the ISMS manual; or an audit report produced by a recognized ICS system certifier.

I. Annual reporting requirements

(i) The company must report the following information to the competent authority based on its self-rated ICS level no later than the end of September each year:

(1) Attachments 1, 2, 6, 7, and 8 of the ISMS manual. Those in possession of personal data need to submit Attachment 9 of the ISMS manual as well.
(2) When conducting internal audits according to the Description to key topics No. 3(6), Attachments 11 and 12 of the ISMS manual must be submitted for audit items that are answered "No".
(3) When conducting internal audits according to the Description to key topics No. 3(6), Attachments 13 and 14 of the ISMS manual must be submitted for audit items that are answered "Not applicable".

(ii) For those who are ISO/IEC 27001 certified, only Attachments 1, 2, 7 (or 8), and 14 of the ISMS manual are required. Although these companies are exempted from submitting Attachments 6 and 13, they must attach copies of certificates, certification reports or other relevant documents.

(iii) For those who are ISO/IEC 27001 certified, and are certified to have passed all additional ISO/IEC 27011 requirements listed in Attachment 7 (or 8) of the ISMS manual, only Attachments 1 and 2 are required. Although these companies are exempted from submitting Attachments 6 ~ 14, they must attach copies of certificates, certification reports or other relevant documents.

VI. ICS document management

The company's ICS documents contain the procedures and documentary framework necessary to control information security and to facilitate managerial and supporting activities. See Figure.4. Documents of all levels are subject to updates whenever necessary, and must be made accessible to anyone in need.

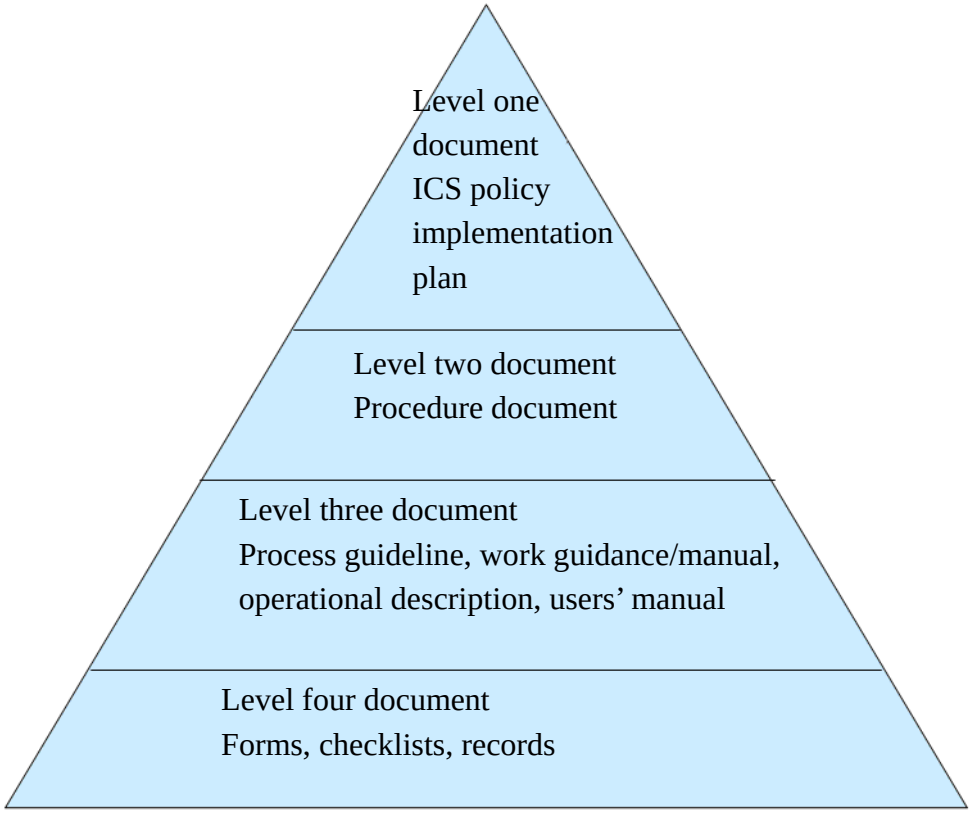


Figure.4 The ICS document hierarchy

A. Level one document

This is the company's ICS implementation plan that provides an overall description of the company's information security management system. It outlines the scope of the company's information and communication security, the ICS policy, all relevant procedures, and describes interactions and relationships between the company's procedures. All personnel related to information and communication security must be familiarized with the policies and goals described in this document, and use them as guidance principles for the various procedures, methods, and work rules.

B. Level two document

The company needs to plan and develop operating procedures for guiding information security-related activities and services based on its internal audit sheet.

C. Level three document

In order to provide proper guidance to the company's information security planning, maintenance, and operation support, all key technologies or processes mentioned in the procedures must be described in separate documents of their own, such as process guidance books (or manuals), work rules, operational descriptions (or users' manuals), etc., as guidance to the various processes.

D. Level four document

In order to facilitate the various processes within the company and thereby achieving systematic practices and consistency, detailed forms, summaries, and audit checklists on information/communication security requirements must be completed throughout the various procedures. These documents serve as guidance to employees' practices while maintaining track records of their execution results. These forms and reports can be processed through electronic media, but all necessary data must be retained.

E. Approval of ICS documents

(i) Level one documents are drafted by the Information and Communication Security Action Team, and shall become effective once approved by the Head of Information Security. The same applies to all subsequent revisions.

(ii) For document levels two, three, and four, the Information and Communication Security Action Team may authorize the drafting to various functional groups and implement accordingly once approved by the group convener.

VII.Attachments

Please refer to the attachments of the ISMS manual

Appendix 5 List of ICS implementation tasks

Name of process Contents Level	Data processing facilities / Depth of protection	Implementation method	Audit method	ICS training hours (for supervisors, IT/communication personnel, business personnel, and general staffs, respectively)	Personal data protection
A	firewall, IDS, IPS, anti-virus software, junk mail filter, webpage filter, and network security monitoring equipment. These protection measures must deliver the level of security expected from advanced equipment, as defined in the "Guidelines on the Inspection of Information and Communication Security Equipment (draft)"	Aim to pass the certification of a third-party ISMS certifier.	Perform internal audits at least once a year.	At least 3, 12, 6, and 3 hours per year.	Businesses that deal with personal data must establish personal data security plans.
B	Firewall, IDS, IPS, anti-virus software, and junk mail filter. These protection measures must deliver the level of security expected from fundamental equipment, as defined in the "Guidelines on the Inspection of Information and Communication Security Equipment (draft)"	Outline and assemble an ICS Action Team.	Perform internal audits at least once a year.	At least 3, 12, 6, and 3 hours per year.	
C	Firewall, IDS, IPS, anti-virus software, and junk mail filter	Strengthen information and communication security Advocacy	Perform internal audits at least once a year.	At least 3, 12, 6, and 3 hours per year.	

Appendix 6

Communications and Broadcastings industry information security management internal audit Checklist

Company Name			
Level of enterprise security	☐Class A ☐Class B ☐Class C		
Manager		Sign-off Date：	
Auditor		Auditing Date：	
Contact	Tel：	Fax：	mobile phone：
	Email：		

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
1. **Information security policy**						
1.1 Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.	◎	◎				
1.2 A Statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives	◎	◎				
1.3 A brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including consequences of information security policy violations.	◎	◎				
1.4 An information security policy document should be approved by management, and	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
published and communicated to all employees and relevant external parties.						
1.5 A definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing.	◎	◎				
1.6 A brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including: 1) compliance with legislative, regulatory, and contractual requirements; 2) security education, training, and awareness requirements; 3) business continuity management; 4) consequences of information security policy violations;	◎	◎				
1.7 A definition of general and specific responsibilities for information security management, including reporting information security incidents	◎	◎				
1.8 References to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.	◎	◎				
1.9 The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	◎	◎				
1.10 The review of the information security policy should take account of the results of	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
management reviews. There should be defined management review procedures, including a schedule or period of the review.						
1.11 The review should include assessing opportunities for improvement of the organization's information security policy and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions, or technical environment.	◎	◎				
1.12 A record of the management review should be maintained. Management approval for the revised policy should be obtained.	◎	◎				
2. **Organization of information security**						
2.1 Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.	◎	◎	◎			
2.2 Typically, information security co-ordination should involve the co-operation and collaboration of managers, users, administrators, application designers, auditors and security personnel, and specialist skills in areas such as insurance, legal issues, human resources, IT or risk management.	◎	◎				
2.3 Information security co-ordination should involve the co-operation and collaboration of managers, users, administrators, application designers, auditors and security personnel, and specialist skills in areas such as insurance, legal issues, human resources, IT or risk management.	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
This activity should ensure that security activities are executed in compliance with the information security policy;						
2.4 Allocation of information security responsibilities should be done in accordance with the information security policy. Responsibilities for the protection of individual assets and for carrying out specific security processes should be clearly identified.	◎	◎				
2.5 Areas for which individuals are responsible should be clearly stated; in particular the following should take place: a) the assets and security processes associated with each particular system should be identified and clearly defined; b) the entity responsible for each asset or security process should be assigned and the details of this responsibility should be documented.	◎	◎				
2.6 A management authorization process for new information processing facilities should be defined and implemented.	◎	◎				
2.7 Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information should be identified and regularly reviewed.	◎	◎				
2.8 Organizations should have procedures in place that specify when and by whom authorities (e.g. law enforcement, fire department, supervisory authorities) should be contacted, and how identified information security incidents should be reported in a	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
timely manner if it is suspected that laws may have been broken.						
2.9 Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.	◎	◎				
2.10 The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur.	◎	◎				
2.11 Any access to the organization's information processing facilities and processing and communication of information by external parties should be controlled. Where there is a business need for working with external parties that may require access to the organization's information and information processing facilities, or in obtaining or providing a product and service from or to an external party, a risk assessment should be carried out to determine security implications and control requirements. Controls should be agreed and defined in an agreement with the external party.	◎	◎				
2.12 The controls necessary to protect information that is not intended to be accessible by external parties.	◎	◎				
2.13 Where there is a need to allow an external party access to the information processing facilities or information of an	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
organization, a risk assessment (see also Section 4) should be carried out to identify any requirements for specific controls.						
2.14 All identified security requirements should be addressed before giving customers access to the organization's information or assets.	◎	◎				
2.15 Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.	◎	◎	◎			
3. **Asset management**						
3.1 All assets should be clearly identified and an inventory of all important assets drawn up and maintained.	◎	◎				
3.2 An organization should identify all assets and document the importance of these assets.	◎	◎				
3.3 The asset inventory should include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value.	◎	◎				
3.4 In addition, ownershipand information classificationshould be agreed and documented for each of the assets. Based on the importance of the asset, its business value and its security classification, levels of protection commensurate with the importance of the assets should be identified	◎	◎				
3.5 All information and assets associated with information processing facilities should be	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
owned by a designated part of the organization.						
3.6 Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.	◎	◎				
3.7 Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.	◎	◎				
3.8 An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization.	◎	◎	◎			
3.9 For each classification level, handling procedures including the secure processing, storage, transmission, declassification, and destruction should be defined. This should also include the procedures for chain of custody and logging of any security relevant event.	◎	◎	◎			
4. **Human resources security**						
4.1 Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy.	◎	◎	◎			
	◎	◎	◎			
4.2 Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
risks.						
4.3As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security.	◎	◎				
4.4 Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.	◎	◎				
4.5 All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.	◎	◎				
4.6 There should be a formal disciplinary process for employees who have committed a security breach.	◎	◎				
4.7 Responsibilities for performing employment termination or change of employment should be clearly defined and assigned.	◎	◎				
4.8 All employees, contractors and third party users should return all of the organization's assets in their possession upon termination of their employment, contract or agreement.	◎	◎				
4.9 The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement,	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
or adjusted upon change.						
5. **Physical and environmental security**						
5.1 Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.	◎	◎				
5.2 Information processing facilities managed by the organization should be physically separated from those managed by third parties.	◎	◎				
5.3 Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	◎	◎				
5.4 Access rights to secure areas should be regularly reviewed and updated, and revoked when necessary.	◎	◎				
5.5 Physical security for offices, rooms, and facilities should be designed and applied.	◎	◎	◎			
5.6 Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.	◎	◎				
5.7 Physical protection and guidelines for working in secure areas should be designed and applied.	◎	◎				
5.8 Unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities.	◎	◎				
5.9 Fallback equipment and back-up media should be sited at a safe distance to avoid damage from a disaster affecting the main	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
site.						
5.10 Hazardous or combustible materials should be stored at a safe distance from a secure area. Bulk supplies such as stationery should not be stored within a secure area	◎	◎				
5.11 Personnel should only be aware of the existence of, or activities within, a secure area on a need to know basis.	◎	◎				
5.12 Photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorized	◎	◎				
5.13 Vacant secure areas should be physically locked and periodically checked.	◎	◎				
5.14 Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	◎	◎				
5.15 Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	◎	◎				
5.16 Information processing facilities handling sensitive data should be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons during their use, and storage facilities secured to avoid unauthorized access.	◎	◎				
5.17 Controls should be adopted to minimize the risk of potential physical threats, e.g. theft, fire, explosives, smoke, water (or water	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism.						
5.18 Guidelines for eating, drinking, and smoking in proximity to information processing facilities should be established.	◎	◎				
5.19 Environmental conditions, such as temperature and humidity, should be monitored for conditions, which could adversely affect the operation of information processing facilities.	◎	◎				
5.20 Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. All supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning should be adequate for the systems they are supporting.	◎	◎	◎			
5.21 Power contingency plans should cover the action to be taken on failure of the UPS. A back-up generator should be considered if processing is required to continue in case of a prolonged power failure.	◎	◎				
5.22 Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.	◎	◎				
5.23 Power cables should be segregated from communications cables to prevent interference.	◎	◎				
5.24 Equipment should be correctly maintained to ensure its continued availability and integrity.	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
5.25 Equipment should be maintained in accordance with the supplier's recommended service intervals and specifications.	◎	◎				
5.26 Only authorized maintenance personnel should carry out repairs and service equipment.	◎	◎				
5.27 Records should be kept of all suspected or actual faults, and all preventive and corrective maintenance.	◎	◎				
5.28 Appropriate controls should be implemented when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organization; where necessary, sensitive information should be cleared from the equipment, or the maintenance personnel should be sufficiently cleared.	◎	◎				
5.29 Security should be applied to off-site equipment taking into account the different risks of working outside the organization's premises.	◎	◎	◎			
5.30 Information storing and processing equipment includes all forms of personal computers, organizers, mobile phones, smart cards, paper or other form, which is held for home working or being transported away from the normal work location.	◎	◎	◎			
5.31 All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.	◎	◎	◎			
5.32 Damaged devices containing sensitive	◎	◎	◎			

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
data may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded.						
5.33 Equipment, information or software should not be taken off-site without prior authorization.	◎	◎	◎			
6. **Communications and operations management**						
6.1 Operating procedures should be documented, maintained, and made available to all users who need them. Documented procedures should be prepared for system activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, backup, equipment maintenance, media handling, computer room and mail handling management, and safety.	◎	◎				
6.2 Changes to information processing facilities and systems should be controlled.	◎	◎				
6.3 Assessment of the potential impacts, including security impacts, of such changes.	◎	◎				
6.4 Fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.	◎	◎				
6.5 Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.	◎	◎				
6.6 Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Care should be taken that no	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.						
6.7 Development, test, and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational system.	◎	◎				
6.8 Users should use different user profiles for operational and test systems, and menus should display appropriate identification messages to reduce the risk of error.	◎	◎				
6.9 It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.	◎	◎				
6.10 Service delivery by a third party should include the agreed security arrangements, service definitions, and aspects of service management.	◎	◎				
6.11 The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.	◎	◎	◎			
6.12 Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.	◎	◎	◎			
6.13 The use of resources should be	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.						
6.14 Acceptance criteria for new information systems, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance.	◎	◎				
6.15 Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.	◎	◎				
6.16 Installation and regular update of malicious code detection and repair software to scan computers and media as a precautionary control, or on a routine basis	◎	◎				
6.17 Establishing a formal policy prohibiting the use of unauthorized software.	◎	◎				
6.18 Conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorized amendments should be formally investigated.	◎	◎				
6.19 Establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures should be taken.	◎	◎				
6.20 Defining management procedures and responsibilities to deal with malicious code protection on systems, training in their use, reporting and recovering from malicious code attacks.	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
6.21 Preparing appropriate business continuity plans for recovering from malicious code attacks, including all necessary data and software back-up and recovery arrangements.	◎	◎				
6.22 Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.	◎	◎				
6.23 Back-up media should be regularly tested to ensure that they can be relied upon for emergency use when necessary.	◎	◎				
6.24 The extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements of the organization, the security requirements of the information involved, and the criticality of the information to the continued operation of the organization.	◎	◎				
6.25 The back-ups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site.	◎	◎				
6.26 Back-up information should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site.	◎	◎				
6.27 The controls applied to media at the main site should be extended to cover the back-up site.	◎	◎				
6.28 Back-up media should be regularly tested to ensure that they can be relied upon for emergency use when necessary.	◎	◎				
6.29 Responsibilities and procedures for the management of remote equipment, including	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
equipment in user areas, should be established.						
6.30 Special controls may also be required to maintain the availability of the network services and computers connected.	◎	◎				
6.31 Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks, and to protect the connected systems and applications.	◎	◎				
6.32 Transmission of confidential information taken encryption and other protective measures.	◎	◎				
6.33 Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided inhouse or outsourced.	◎	◎				
6.34 Regularly review the implementation of network security controls.	◎	◎				
6.35 Regularly test network operating environment security vulnerabilities.	◎	◎				
6.36 Technology applied for security of network services, such as authentication, encryption, and network connection controls.	◎	◎				
6.37 There should be procedures in place for the management of removable media. Appropriate operating procedures should be established to protect documents, computer media (e.g. tapes, disks), input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction.	◎	◎	◎			

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
6.38 Media should be disposed of securely and safely when no longer required, using formal procedures.	◎	◎	◎			
6.39 Procedures should be in place to identify the items that might require secure disposal.	◎	◎	◎			
6.40 Handling and labelling of all media to its indicated classification level.	◎	◎				
6.41 Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse.	◎	◎				
6.42 System documentation should be protected against unauthorized access.	◎	◎				
6.43 Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.	◎	◎				
6.44 Use of cryptographic techniques e.g. to protect the confidentiality, integrity and authenticity of information.	◎	◎				
6.45 Agreements should be established for the exchange of information and software between the organization and external parties.	◎	◎	◎			
6.46 Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond an organization’s physical boundaries.	◎	◎	◎			
6.47 The following guidelines should be considered to protect information media being transported between sites: controls should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification; examples include	◎	◎	◎			

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
6.48 Information involved in electronic messaging should be appropriately protected. Protecting messages from unauthorized access, modification or denial of service.	◎	◎				
6.49 Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems.	◎	◎				
6.50 Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.	◎	◎	◎			
6.51 Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	◎	◎	◎			
6.52 The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification.	◎	◎				
6.53 Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.	◎	◎	◎			
6.54 Procedures for monitoring use of information processing facilities.	◎	◎				
6.55 Should be established and the results of the monitoring activities reviewed regularly.	◎	◎				
6.56 Logging facilities and log information	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
should be protected against tampering and unauthorized access.						
6.57 Should be established and the results of the logging facilities reviewed regularly.	◎	◎				
6.58 Controls should aim to protect against unauthorized changes and operational problems with the logging facility including: storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.	◎	◎				
6.59 System administrator and system operator activities should be logged and reviewed regularly.	◎	◎	◎			
6.60 Faults should be logged, analysed, and appropriate action taken.	◎	◎				
6.61 The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source.	◎	◎				
7. **Access control**						
7.1 An access control policy should be established, documented, and reviewed based on business and security requirements for access.	◎	◎				
7.2 Access control rules and rights for each user or group of users should be clearly stated in an access control policy.	◎	◎				
7.3 Relevant legislation and any contractual obligations regarding protection of access to data or services.	◎	◎				
7.4 There should be a formal user registration and de-registration procedure in place for granting and revoking access to all	◎	◎	◎			

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
information systems and services.						
7.5 Immediately removing or blocking access rights of users who have changed roles or jobs or left the organization.	◎	◎	◎			
7.6 Maintaining a formal record of all persons registered to use the service.	◎	◎	◎			
7.7 The allocation and use of privileges should be restricted and controlled. Multi-user systems that require protection against unauthorized access should have the allocation of privileges controlled through a formal authorization process.	◎	◎				
7.8 An authorization process and a record of all privileges allocated should be maintained. Privileges should not be granted until the authorization process is complete.	◎	◎				
7.9 Establish procedures to verify the identity of a user prior to providing a new, replacement or temporary password	◎	◎				
7.10 Temporary passwords should be given to users in a secure manner; the use of third parties or unprotected (clear text) electronic mail messages should be avoided.	◎	◎				
7.11 Default vendor passwords should be altered following installation of systems or software.	◎	◎				
7.12 Users should be required to sign a statement to keep personal passwords confidential; this signed statement could be included in the terms and conditions of employment.	◎	◎				
7.13 When users are required to maintain their own passwords they should be provided initially with a secure temporary password,	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
which they are forced to change immediately;						
7.14 Passwords should never be stored on computer systems in an unprotected form.	◎	◎				
7.15 Management should review users' access rights at regular intervals using a formal process.	◎	◎				
7.16 Select quality passwords with sufficient minimum length.	◎	◎				
7.17 Free of consecutive identical, all-numeric or all-alphabetic characters.	◎	◎				
7.18 Change passwords whenever there is any indication of possible system or password compromise.	◎	◎				
7.19 Change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid re-using or cycling old passwords.	◎	◎				
7.20 Not include passwords in any automated log-on process, e.g. stored in a macro or function key.	◎	◎				
7.21 Not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.	◎	◎				
7.22 Avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved.	◎	◎				
7.23 Limit the maximum and minimum time allowed for the log-on procedure. If exceeded, the system should terminate the log-on.	◎	◎				
7.24 Not display the password being entered or consider hiding the password characters by	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
symbols.						
7.25 Users should ensure that unattended equipment has appropriate protection.	◎	◎				
7.26 A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.	◎	◎	◎			
7.27 Computers and terminals should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and should be protected by key locks, passwords or other controls when not in use.	◎	◎	◎			
7.28 Sensitive or critical business information, e.g. on paper or on electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated	◎	◎	◎			
7.29 Unauthorized use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) should be prevented.	◎	◎	◎			
7.30 Documents containing sensitive or classified information should be removed from printers immediately.	◎	◎	◎			
7.31 Users should only be provided with access to the services that they have been specifically authorized to use.	◎	◎				
7.32 Display the following information on completion of a successful log-on: 1) date and time of the previous successful log-on; 2) details of any unsuccessful log-on attempts since the last successful log-on.	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
7.33 Limit the number of unsuccessful log-on attempts allowed, e.g. to three attempts, and consider: 1) recording unsuccessful and successful attempts; 2) forcing a time delay before further log-on attempts are allowed or rejecting any further attempts without specific authorization.	◎	◎				
7.34 Establish a network service access security policy to ensure that specific authorization by the Department to allow users to access the network and network services.	◎	◎				
7.35 Authentication of remote users can be achieved using, for example, a cryptographic based technique, hardware tokens, or a challenge/response protocol.	◎	◎				
7.36 Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.	◎	◎				
7.37 Physical and logical access to diagnostic and configuration ports should be controlled.	◎	◎				
7.38 Potential controls for the access to diagnostic and configuration ports include the use of a key lock and supporting procedures to control physical access to the port.	◎	◎				
7.39 Additional authentication controls should be implemented to control access to wireless networks. In particular, special care is needed in the selection of controls for wireless networks due to the greater opportunities for undetected interception and insertion of network traffic.	◎	◎				
7.40 One method of controlling the security	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
of large networks is to divide them into separate logical network domains, e.g. an organization's internal network domains and external network domains, each protected by a defined security perimeter.						
7.41 For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications.	◎	◎				
7.42 Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.	◎	◎				
7.43 The procedure for logging into an operating system should be designed to minimize the opportunity for unauthorized access. The log-on procedure should therefore disclose the minimum of information about the system, in order to avoid providing an unauthorized user with any unnecessary assistance.	◎	◎				
7.44 Limit the number of unsuccessful log-on attempts allowed, e.g. to three attempts, and consider recording unsuccessful and successful attempts.	◎	◎				
7.45 Login process for exceptions, leave records and regularly review.	◎	◎				
7.46 Not transmit passwords in clear text over a network. If passwords are transmitted in clear text during the log-on session over a network, they may be captured by a network	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
'sniffer' program on the network.						
7.47 All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.	◎	◎				
7.48 Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means, should be used.	◎	◎				
7.49 Systems for managing passwords should be interactive and should ensure quality passwords, store password files separately from application system data	◎	◎				
7.50 The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.	◎	◎				
7.51 Inactive sessions should shut down after a defined period of inactivity.	◎	◎				
7.52 Restrictions on connection times should be used to provide additional security for high-risk applications.	◎	◎				
7.53 Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy.	◎	◎				
7.54 Sensitive systems should have a dedicated (isolated) computing environment.	◎	◎	◎			
7.55 A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication	◎	◎	◎			

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
facilities.						
7.56 A policy, operational plans and procedures should be developed and implemented for teleworking activities. Organizations should only authorize teleworking activities if they are satisfied that appropriate security arrangements and controls are in place, and that these comply with the organization's security policy.	◎	◎				
7.57 Revocation of authority and access rights, and the return of equipment when the teleworking activities are terminated.	◎	◎				
8.**Information systems acquisition, development and maintenance**						
8.1 Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.	◎	◎	◎			
8.2 Data input to applications should be validated to ensure that this data is correct and appropriate.	◎	◎				
8.3 Procedures for responding to validation errors.	◎	◎				
8.4 Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.	◎	◎				
8.5 Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented.	◎	◎				
8.6 Data output from an application should be validated to ensure that the processing of	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
stored information is correct and appropriate to the circumstances. Plausibility checks to test whether the output data is reasonable; reconciliation control counts to ensure processing of all data.						
8.7 Procedures for responding to output validation tests.	◎	◎				
8.8 Defining the responsibilities of all personnel involved in the data output process, creating a log of activities in the data output validation process.	◎	◎				
8.9 A policy on the use of cryptographic controls for protection of information should be developed and implemented.	◎	◎				
8.10 Key management should be in place to support the organization’s use of cryptographic techniques.	◎	◎				
8.11 Any decision to upgrade to a new release should take into account the business requirements for the change, and the security of the release, i.e. the introduction of new security functionality or the number and severity of security problems affecting this version.	◎	◎				
8.12 The updating of the operational software, applications, and program libraries should upon appropriate management authorization.	◎	◎				
8.13 The updating of the operational software, applications, and program libraries should only be performed by trained administrators.	◎	◎				
8.14 A configuration control system should be used to keep control of all implemented	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
software as well as the system documentation.						
8.15 Test data should be selected carefully, and protected and controlled.	◎	◎				
8.16 Access to program source code should be restricted.	◎	◎				
8.17 The implementation of changes should be controlled by the use of formal change control procedures.	◎	◎				
8.18 Ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed.	◎	◎				
8.19 When operating systems are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	◎	◎				
8.20 Ensuring that notification of operating system changes is provided in time to allow appropriate tests and reviews to take place before implementation.	◎	◎				
8.21 Review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes.	◎	◎				
8.22 Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled.	◎	◎	◎			
8.23 Opportunities for information leakage should be prevented e.g. through the use and exploitation of covert channels.	◎	◎				
8.24 Testing before installation to detect malicious and Trojan code.	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
8.25 Licensing arrangements, code ownership, and intellectual property rights	◎	◎				
8.26 Escrow arrangements in the event of failure of the third party, rights of access for audit of the quality and accuracy of work done.	◎	◎				
8.27 Timely information about technical vulnerabilities of information and communication systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.	◎	◎				
8.28 Patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered.	◎	◎				
9.**Information security incident management**						
9.1 A formal information security event reporting procedure should be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event.	◎	◎	◎			
9.2 Information security events should be reported through appropriate management channels as quickly as possible.	◎	◎	◎			
9.3 Noting all important details (e.g. type of non-compliance or breach, occurring malfunction, messages on the screen, strange behaviour) immediately.	◎	◎	◎			
9.4 A point of contact should be established for the reporting of information security	◎	◎	◎			

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
events. It should be ensured that this point of contact is known throughout the organization, is always available and is able to provide adequate and timely response.						
9.5 All employees, contractors and third party users should be made aware of their responsibility to report any information security events as quickly as possible. They should also be aware of the procedure for reporting information security events and the point of contact.	◎	◎	◎			
9.6 All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services.	◎	◎	◎			
9.7 Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents. Procedures should be established to handle different types of information security incident.	◎	◎	◎			
9.8 There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.	◎	◎	◎			
9.9 The objectives for information security incident management should be agreed with management, and it should be ensured that those responsible for information security incident management understand the organization’s priorities for handling information security incidents.	◎	◎	◎			
9.10 The information gained from the	◎	◎	◎			

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
evaluation of information security incidents should be used to identify recurring or high impact incidents.						
9.11 There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.	◎	◎	◎			
9.12 The evaluation of information security incidents may indicate the need for enhanced or additional controls to limit the frequency, damage, and cost of future occurrences, or to be taken into account in the security policy review process.	◎	◎	◎			
9.13 To achieve admissibility of the evidence, the organization should ensure that their information systems comply with any published standard or code of practice for the production of admissible evidence.	◎	◎				
10.**Business continuity management**						
10.1 A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization’s business continuity.	◎	◎				
10.2 Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security.	◎	◎				
10.3 Business continuity risk assessments should be carried out with full involvement from owners of business resources and processes. This assessment should consider all business processes and should not be	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
limited to the information processing facilities, but should include the results specific to information security.						
10.4 The business continuity planning process should consider the following: identification and agreement of all responsibilities and business continuity procedures; identification of the acceptable loss of information and services.	◎	◎				
10.5 Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.	◎	◎				
10.6 A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.	◎	◎				
10.7 Business continuity plan tests should ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when a plan is invoked.	◎	◎				
10.8 Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective.	◎	◎				
11.**Compliance**						
11.1 All relevant statutory, regulatory, and contractual requirements and the organization’s approach to meet these	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.						
11.2 Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.	◎	◎				
11.3 Publishing an intellectual property rights compliance policy which defines the legal use of software and information products.	◎	◎				
11.4 Maintaining proof and evidence of ownership of licenses, master disks, manuals, etc.	◎	◎				
11.5 Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements. Records should be categorized into record types, e.g. accounting records, database records, transaction logs, audit logs, and operational procedures, each with details of retention periods and type of storage media, e.g. paper, microfiche, magnetic, optical.	◎	◎				
11.6 Generate audit reports, and track to improve the situation.	◎	◎				
11.7 Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.	◎	◎				
11.8 An organizational data protection and privacy policy should be developed and	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
implemented. This policy should be communicated to all persons involved in the processing of personal information.						
11.9 Compliance with this policy and all relevant data protection legislation and regulations requires appropriate management structure and control.	◎	◎				
11.10 Users should be deterred from using information processing facilities for unauthorized purposes.	◎	◎				
11.11 Management should approve the use of information processing facilities. Any use of these facilities for non-business purposes without management approval, or for any unauthorized purposes, should be regarded as improper use of the facilities.	◎	◎				
11.12 Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.	◎	◎				
11.13 Information systems should be regularly checked for compliance with security implementation standards.	◎	◎				
11.14 Technical compliance checking should be performed by an experienced system engineer.	◎	◎				
11.15 Any technical compliance check should only be carried out by competent, authorized persons, or under the supervision of such persons.	◎	◎				
11.16 All access should be monitored and logged to produce a reference trail; the use of time stamped reference trails should be	◎	◎				

Communications and Broadcastings industry information security management internal audit Checklist						
Checklist	Level of enterprise security			Results		
	Class A	Class B	Class C	Meet	Not meet	Not applicable
considered for critical data or systems						
11.17 Such tests should be planned, documented and repeatable.	◎	◎				
11.18 Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes.	◎	◎				
11.19 On a regular basis for information security internal audit.	◎	◎				
11.20 The scope of the checks should be agreed and controlled.	◎	◎				
11.21 Access to information systems audit tools should be protected to prevent any possible misuse or compromise.	◎	◎				
Summary	277	277	49			

Appendix 7. Communications industry auditing Checklist

Company Name			
Level of enterprise security	☐Class A telecommunications industry		
Manager		Sign-off Date：	
Auditor		Auditing Date：	
Contact	Tel：	Fax：	mobile phone：
	Email：		

Communications industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the telecommunications industry	Results		
		Meet	Not meet	Not applicable
1.Organization of information security				
1.1Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified and regularly reviewed.	◎			
1.2 Organizations should have procedures in place that specify when and by whom authorities (e.g., law enforcement, fire department, supervisory authorities) should be contacted, and how identified information security incidents should be reported in a timely manner if it is suspected that laws may have been broken.	◎			
1.3 All identified security requirements should be addressed before giving customers access to the organization's information or assets.	◎			

Communications industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the telecommunications industry	Results		
		Meet	Not meet	Not applicable
1.4 Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.	◎			
2.Asset management				
2.1 When developing and maintaining the inventory of assets, clear responsibilities between the telecommunications facilities of the organization and those of other connected or related telecommunications organizations should be specified and clearly documented.	◎			
2.2 Classifications and associated protective controls for information should take account of business needs for sharing or restricting information and the business impacts associated with such needs.	◎			
3.Human resources security				
3.1 Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy.	◎			
3.2 Telecommunications organizations should appoint telecommunications engineers and other staff, who have the right credentials or appropriate knowledge and skills, to be in	◎			

Communications industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the telecommunications industry	Results		
		Meet	Not meet	Not applicable
charge of the supervision of matters related to the installation, maintenance and operation of telecommunications facilities for the telecommunications business.				
3.3 Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.	◎			
3.4 As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security.	◎			
3.5 That all employees, contractors and third party users who are given access to sensitive information sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities.	◎			
3.6 The legal rights and responsibilities regarding non-disclosure of communications and essential communications, which telecommunications organizations should take into account, are included in the laws and regulations.	◎			
3.7 Telecommunications organizations should	◎			

Communications industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the telecommunications industry	Results		
		Meet	Not meet	Not applicable
clarify and state the responsibilities for maintaining the communications service provided by telecommunications organizations in the terms and conditions of employment.				
4.Physical and environmental security				
4.1 Physical barriers should be effectively installed, with all local security policies rigorously enforced to ensure the protection of corporate assets at all times; if a physical barrier is malfunctioning or a policy is not followed, it is imperative that the issue be resolved immediately by management with the appropriate level of responsibility.	◎			
4.2 Operation rooms and control centres to operate telecommunications facilities should be protected by adequate strong entry controls.	◎			
4.3 A site whose environment is least susceptible to damage from wind and water, etc., should be selected for communication centres; where a site is chosen that is vulnerable to environmental damage, appropriate measures should be taken against wind and water hazards. A site whose environment is least susceptible to damage from strong electromagnetic field should be selected for communication centres; where a site is chosen that is exposed to strong electromagnetic fields, appropriate	◎			

Communications industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the telecommunications industry	Results		
		Meet	Not meet	Not applicable
measures should be taken to protect telecommunications equipment rooms with electromagnetic shields.				
4.4 Automatic fire alarms should be installed in communication centres.	◎			
4.5 Communication centre buildings should be of earthquake-proof construction and have adequate structural stability to meet the necessary floor load.	◎			
4.6 Communication centre buildings should be of fire-proof or fire-resistant construction.	◎			
4.7 The telecommunications equipment room should be located where it is least susceptible to external effects such as natural disasters, and intrusion by unauthorized personnel, adequate measures should be taken to prevent such intrusions.	◎			
4.8 To protect physically isolated operating area (e.g., mobile base station) in which telecommunications facilities are located for providing telecommunications business (hereafter referred to as isolated operating area), the following controls should be considered: automatic fire control equipment, be monitored by a remote office for the purpose of detecting facility failures, power failures, fire, humidity and temperature and so on, physically secure perimeters should be provided in a proper manner.	◎			

Communications industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the telecommunications industry	Results		
		Meet	Not meet	Not applicable
4.9 If the systems of several organizations are sited in the same data centre as telecommunications facilities, the telecommunications organization should implement appropriate measures to protect customers' information stored in their systems. Such systems should be placed physically separate on a site, for example, on a different floor or in a different room.	◎			
4.10 In particular, power supply facilities in the isolated area such as mobile base stations should preferably provide an uninterruptible power supply with capacity for all loading and capable of withstanding primary power supply failures for the duration of likely outages. If that is impossible, a mechanism to provide uninterruptible power to critical equipment should be installed. Batteries may need to be augmented with a private electric generator, especially in isolated areas.	◎			
4.11 When telecommunications organizations install equipment outside of their own premises, the equipment should be sited in a protected area so that any risks from environmental threats or dangers and from the possibility of unauthorized access are reduced.	◎			
4.12 When telecommunications organizations install equipment within the telecommunications service customer	◎			

Communications industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the telecommunications industry	Results		
		Meet	Not meet	Not applicable
premises in order to connect with the customer equipment, the organizations' equipment should be protected in order to reduce risk from environmental threats or dangers and from the risk of unauthorized access.				
4.13 In the provision of interconnected telecommunications services, the telecommunications organizations should specify a well-defined boundary and interface with other telecommunications organizations, so that each organization may be partitioned and isolated in a timely manner in order to evade an identified risk.	◎			
4.14 Telecommunications organizations should specify in an agreement or a contract that the provision of telecommunications services for the customers may be suspended, whose communications pose a problem for the smooth service provision of the interconnected telecommunications organizations.	◎			
5.Communications and operations management				
5.1 In the operating procedures, telecommunications organizations should specify under which conditions the incident, emergency or crisis handling procedures are to be invoked.	◎			
5.2 Telecommunications organizations should	◎			

Communications industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the telecommunications industry	Results		
		Meet	Not meet	Not applicable
consider the procedures and records for installation, relocation and removal of facilities.				
5.3 In telecommunications organizations, the content of the data used in test and development environments should be adequate to test the system and service in a real telecommunications context.	◎			
5.4 When the test data includes sensitive information (e.g., personal information and telephone records), appropriate controls should be implemented in order to avoid unintended information leakage caused by program bugs or operational errors.	◎			
5.5 Where the use of mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing.	◎			
5.6 Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced.	◎			
5.7 Telecommunications organizations should set the security level for the various business propositions of telecommunications services provided, announce it to their customers prior	◎			

Communications industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the telecommunications industry	Results		
		Meet	Not meet	Not applicable
to service delivery, and maintain and manage their telecommunications services properly, awareness activities to protect telecommunications service users from spam, internet crime, computer virus and such like.				
5.8 Telecommunications organizations should stipulate the policies for responding to spam and implement appropriate controls in order to establish a favorable and desirable environment for e-mail communications.	◎			
5.9 Telecommunications organizations should stipulate the policies for responding to Dos/DDoS attacks and implement appropriate control in order to prepare a favorable and desirable environment for telecommunications services.	◎			
5.10 In order to protect IP network facilities, such as servers, routers from cyber attacks (e.g., DDoS attack), telecommunications organizations should have mechanisms to filter communications or limit communication bands in IP addresses, communication ports, and application protocols respectively. Depending on telecommunications services, such mechanisms of communications filters should be implemented associated with signal processing control, user authentication and access controls	◎			
5.11 Telecommunications organizations should implement measures to protect against	◎			

Communications industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the telecommunications industry	Results		
		Meet	Not meet	Not applicable
impersonation of IP addresses (IP spoofing).				
5.12 In order to prevent source impersonation by means of stepping-stone, appropriate security controls against unauthorized access should be implemented at the systems providing user authentication by introducing strict password controls and/or strong authentication functions, e.g., mandatory use of unpredictable password above a certain length, and introduction of one-time-password and strong token authentication.	◎			
5.13 Operating rules to collect information concerning disaster and planned events, which may cause network congestion, should be stipulated by telecommunications organization, e.g., the establishment of a framework to collect weather information and planned events information. Mechanisms and procedures to report the collected information should be set up, and the information should keep relevant personnel informed.	◎			
5.14 Telecommunications facilities should have mechanisms to detect network congestion and avoid the concentration of communications in case of network congestion.	◎			
5.15 Operating rules to collect information concerning disaster and planned events, which may cause network congestion, should	◎			

Communications industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the telecommunications industry	Results		
		Meet	Not meet	Not applicable
be stipulated by telecommunications organization.				
5.16 Taking account of the scale of potential disruption and disaster, the use of distributed processing centres, and implementation of supplementary facilities and adaptive configuration changes should be considered, where necessary.	◎			
5.17 Identify and give the necessary priority of communication, to help maintain traffic after a disaster, emergency communications, power supply or to maintain social order.	◎			
5.18 Telecommunications organizations should set the appropriate retention time period for retaining data of telecommunications data (e.g., accounting, billing, attending to complaints, and protection of abuse and lawful access by the authorities) and to delete the data at the end of the retention period or at the attainment of the purposes without any delay. This should be done in accordance with any business, legal and regulatory requirements that might apply.	◎			
6.Access control				
6.1 Telecommunications organizations should specify appropriate access control rules for equipment sited in user premises. Access should be based on information ownership not physical asset ownership. For example, only the user of telecommunications	◎			

Communications industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the telecommunications industry	Results		
		Meet	Not meet	Not applicable
equipment should have access to the address book stored on a mobile phone but denied access to any system design related information such as terminal ID.				
6.2 Telecommunications organizations should provide an appropriate control for the users to be able to identify and authenticate the telecommunications organizations.	◎			
7.Information systems acquisition, development and maintenance				
7.1 Operational systems should only hold approved executable code, and not development code or compilers.	◎			
7.2 A rollback strategy should be in place before changes are implemented.	◎			
7.3 An audit log should be maintained of all updates to operational program libraries.	◎			
7.4 If applications and operating system software are to be implemented to sensitive systems such as switching facility, the test should be carried out with a full coverage of path.	◎			
7.5 If application software is sensitive, then at least three generations of software should be retained.	◎			
8.Information security incident management				
8.1 Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to	◎			

Communications industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the telecommunications industry	Results		
		Meet	Not meet	Not applicable
information security incidents.				
8.2 Telecommunications organizations should establish mechanisms and/or procedures for sharing the lessons learnt and improving the incident management, taking account of the following actions: hold a post-incident meeting, which includes on the agenda the lessons learned; this meeting should consider ways for improving security measures and the incident handling process itself.	◎			
9.Business continuity management				
9.1A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity. Understanding the risks the organization is facing in terms of likelihood and impact in time, including an identification and prioritization of critical business processes.	◎			
Summary	55			

Appendix 8. Broadcastings industry auditing Checklist

Company Name			
Level of enterprise security	☐Class A broadcastings industry		
Manager		Manager	
Auditor		Auditor	
Contact	Tel：	Contact	Tel：
	Email：		

Broadcastings industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the broadcastings industry	Results		
		Meet	Not meet	Not applicable
1.**Organization of information security**				
1.4 Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.	◎			
2.**Asset management**				
2.1 When developing and maintaining the inventory of assets, clear responsibilities between the broadcastings facilities of the organization and those of other connected or related broadcastings organizations should be specified and clearly documented.	◎			
3.**Human resources security**				
3.1 Security roles and responsibilities of	◎			

Broadcastings industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the broadcastings industry	Results		
		Meet	Not meet	Not applicable
employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy.				
3.2 Broadcasting organizations should appoint broadcasting engineers and other staff, who have the right credentials or appropriate knowledge and skills, to be in charge of the supervision of matters related to the installation, maintenance and operation of broadcasting facilities for the broadcasting business.	◎			
3.3 Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.	◎			
3.4 As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security.	◎			
3.5 That all employees, contractors and third party users who are given access to sensitive information sign a confidentiality or non-disclosure agreement prior to being given	◎			

Broadcastings industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the broadcastings industry	Results		
		Meet	Not meet	Not applicable
access to information processing facilities.				
3.6 The legal rights and responsibilities regarding non-disclosure of communications and essential communications, which broadcastings organizations should take into account, are included in the laws and regulations.	◎			
3.7 Broadcastings organizations should clarify and state the responsibilities for maintaining the communications service provided by broadcastings organizations in the terms and conditions of employment.	◎			
4.**Physical and environmental security**				
4.1 Physical barriers should be effectively installed, with all local security policies rigorously enforced to ensure the protection of corporate assets at all times; if a physical barrier is malfunctioning or a policy is not followed, it is imperative that the issue be resolved immediately by management with the appropriate level of responsibility.	◎			
4.2 Operation rooms and control centres to operate broadcastings facilities should be protected by adequate strong entry controls.	◎			
4.3 A site whose environment is least susceptible to damage from wind and water, etc., should be selected for communication centres; where a site is chosen that is vulnerable to environmental damage,	◎			

Broadcastings industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the broadcastings industry	Results		
		Meet	Not meet	Not applicable
appropriate measures should be taken against wind and water hazards. A site whose environment is least susceptible to damage from strong electromagnetic field should be selected for communication centres; where a site is chosen that is exposed to strong electromagnetic fields, appropriate measures should be taken to protect broadcastings equipment rooms with electromagnetic shields.				
4.4 Automatic fire alarms should be installed in communication centres.	◎			
4.5 Communication centre buildings should be of earthquake-proof construction and have adequate structural stability to meet the necessary floor load.	◎			
4.6 Communication centre buildings should be of fire-proof or fire-resistant construction.	◎			
4.7 The broadcastings equipment room should be located where it is least susceptible to external effects such as natural disasters, and intrusion by unauthorized personnel, adequate measures should be taken to prevent such intrusions.	◎			
4.8 To protect physically isolated operating area (e.g., mobile base station) in which broadcastings facilities are located for providing broadcastings business (hereafter referred to as isolated operating area), the following controls should be considered:	◎			

Broadcastings industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the broadcastings industry	Results		
		Meet	Not meet	Not applicable
automatic fire control equipment, be monitored by a remote office for the purpose of detecting facility failures, power failures, fire, humidity and temperature and so on, physically secure perimeters should be provided in a proper manner.				
4.10 In particular, power supply facilities in the isolated area such as mobile base stations should preferably provide an uninterruptible power supply with capacity for all loading and capable of withstanding primary power supply failures for the duration of likely outages. If that is impossible, a mechanism to provide uninterruptible power to critical equipment should be installed. Batteries may need to be augmented with a private electric generator, especially in isolated areas.	◎			
4.11 When broadcastings organizations install equipment outside of their own premises, the equipment should be sited in a protected area so that any risks from environmental threats or dangers and from the possibility of unauthorized access are reduced.	◎			
4.12 When broadcastings organizations install equipment within the broadcastings service customer premises in order to connect with the customer equipment, the organizations' equipment should be protected in order to reduce risk from environmental	◎			

Broadcastings industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the broadcastings industry	Results		
		Meet	Not meet	Not applicable
threats or dangers and from the risk of unauthorized access.				
4.13 In the provision of interconnected broadcastings services, the broadcastings organizations should specify a well-defined boundary and interface with other broadcastings organizations, so that each organization may be partitioned and isolated in a timely manner in order to evade an identified risk.	◎			
4.14 Broadcastings organizations should specify in an agreement or a contract that the provision of broadcastings services for the customers may be suspended, whose communications pose a problem for the smooth service provision of the interconnected broadcastings organizations.	◎			
5. **Communications and operations management**				
5.1 In the operating procedures, broadcastings organizations should specify under which conditions the incident, emergency or crisis handling procedures are to be invoked.	◎			
5.2 Broadcastings organizations should consider the procedures and records for installation, relocation and removal of facilities.	◎			
5.3 In broadcastings organizations, the content of the data used in test and	◎			

Broadcastings industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the broadcastings industry	Results		
		Meet	Not meet	Not applicable
development environments should be adequate to test the system and service in a real broadcastings context.				
5.4 When the test data includes sensitive information (e.g., personal information and telephone records), appropriate controls should be implemented in order to avoid unintended information leakage caused by program bugs or operational errors.	◎			
5.5 Where the use of mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing.	◎			
5.9 Broadcastings organizations should stipulate the policies for responding to Dos/DDoS attacks and implement appropriate control in order to prepare a favorable and desirable environment for broadcastings services.	◎			
5.10 In order to protect IP network facilities, such as servers, routers from cyber attacks (e.g., DDoS attack), broadcastings organizations should have mechanisms to filter communications or limit communication bands in IP addresses, communication ports, and application protocols respectively. Depending on broadcastings services, such mechanisms of communications filters should	◎			

Broadcastings industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the broadcastings industry	Results		
		Meet	Not meet	Not applicable
be implemented associated with signal processing control, user authentication and access controls				
5.15 Operating rules to collect information concerning disaster and planned events, which may cause network congestion, should be stipulated by broadcastings organization.	◎			
5.16 Taking account of the scale of potential disruption and disaster, the use of distributed processing centres, and implementation of supplementary facilities and adaptive configuration changes should be considered, where necessary.	◎			
5.18 Broadcastings organizations should set the appropriate retention time period for retaining data of broadcastings data (e.g., accounting, billing, attending to complaints, and protection of abuse and lawful access by the authorities) and to delete the data at the end of the retention period or at the attainment of the purposes without any delay. This should be done in accordance with any business, legal and regulatory requirements that might apply.	◎			
7. **Information systems acquisition, development and maintenance**				
7.1 Operational systems should only hold approved executable code, and not development code or compilers.	◎			
7.2 A rollback strategy should be in place	◎			

Broadcastings industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the broadcastings industry	Results		
		Meet	Not meet	Not applicable
before changes are implemented.				
7.3 An audit log should be maintained of all updates to operational program libraries.	◎			
7.4 If applications and operating system software are to be implemented to sensitive systems such as switching facility, the test should be carried out with a full coverage of path.	◎			
7.5 If application software is sensitive, then at least three generations of software should be retained.	◎			
8.**Information security incident management**				
8.1 Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.	◎			
8.2 Broadcastings organizations should establish mechanisms and/or procedures for sharing the lessons learnt and improving the incident management, taking account of the following actions: hold a post-incident meeting, which includes on the agenda the lessons learned; this meeting should consider ways for improving security measures and the incident handling process itself.	◎			
9. **Business continuity management**				
9.1 A managed process should be developed and maintained for business continuity	◎			

Broadcastings industry auditing Checklist				
Checklist	ISO/IEC 27011 Controls for the broadcastings industry	Results		
		Meet	Not meet	Not applicable
throughout the organization that addresses the information security requirements needed for the organization's business continuity. Understanding the risks the organization is facing in terms of likelihood and impact in time, including an identification and prioritization of critical business processes.				
Summary	40			

Appendix 9.

Communications and Broadcastings industry personal information protection internal audit Checklist

Company Name			
Level of enterprise security	☐Apply to have personal information		
Manager		Sign-off Date：	
Auditor		Auditing Date：	
Contact	Tel：	Fax：	mobile phone：
	Email：		

Communications and Broadcastings industry personal information protection internal audit Checklist				
Checklist Check the below item number, the Department refer to Appendix 6	personal information protection Controls	Results		
		Meet	Not meet	Not applicable
6.**Communications and operations management**				
6.5 Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.	◎			
6.6 Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.	◎			
6.15 Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should	◎			

Communications and Broadcastings industry personal information protection internal audit Checklist				
Checklist Check the below item number, the Department refer to Appendix 6	personal information protection Controls	Results		
		Meet	Not meet	Not applicable
be implemented.				
6.16 Installation and regular update of malicious code detection and repair software to scan computers and media as a precautionary control, or on a routine basis.	◎			
6.17 Establishing a formal policy prohibiting the use of unauthorized software.	◎			
6.18 Conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorized amendments should be formally investigated.	◎			
6.19 Establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures should be taken.	◎			
6.20 Defining management procedures and responsibilities to deal with malicious code protection on systems, training in their use, reporting and recovering from malicious code attacks.	◎			
6.21 Preparing appropriate business continuity plans for recovering from malicious code attacks, including all necessary data and software back-up and recovery arrangements.	◎			
6.37 There should be procedures in place for the management of removable media. Appropriate operating procedures should be	◎			

Communications and Broadcastings industry personal information protection internal audit Checklist				
Checklist Check the below item number, the Department refer to Appendix 6	personal information protection Controls	Results		
		Meet	Not meet	Not applicable
established to protect documents, computer media (e.g. tapes, disks), input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction.				
6.38 Media should be disposed of securely and safely when no longer required, using formal procedures.	◎			
6.39 Procedures should be in place to identify the items that might require secure disposal.	◎			
6.40 Handling and labelling of all media to its indicated classification level.	◎			
6.41 Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse.	◎			
6.43 Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.	◎			
6.44 cryptographic techniques e.g. to protect the confidentiality, integrity and authenticity of information.	◎			
6.45 Agreements should be established for the exchange of information and software between the organization and external parties.	◎			
6.46 Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond an organization’s physical boundaries.	◎			

Communications and Broadcastings industry personal information protection internal audit Checklist				
Checklist Check the below item number, the Department refer to Appendix 6	personal information protection Controls	Results		
		Meet	Not meet	Not applicable
6.47 The following guidelines should be considered to protect information media being transported between sites: controls should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification.	◎			
6.48 Information involved in electronic messaging should be appropriately protected. Protecting messages from unauthorized access, modification or denial of service.	◎			
6.49 Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems.	◎			
6.50 Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.	◎			
6.51 Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	◎			
6.53 Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.	◎			

Communications and Broadcastings industry personal information protection internal audit Checklist				
Checklist Check the below item number, the Department refer to Appendix 6	personal information protection Controls	Results		
		Meet	Not meet	Not applicable
6.54 Procedures for monitoring use of information processing facilities.	◎			
6.55 Should be established and the results of the monitoring activities reviewed regularly.	◎			
6.56 Logging facilities and log information should be protected against tampering and unauthorized access.	◎			
6.57 Should be established and the results of the logging facilities reviewed regularly.	◎			
6.58 Controls should aim to protect against unauthorized changes and operational problems with the logging facility including: storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.	◎			
6.59 System administrator and system operator activities should be logged and reviewed regularly.	◎			
6.60 Faults should be logged, analysed, and appropriate action taken.	◎			
6.61 The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source.	◎			
7. **Access control**				
7.4 There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	◎			

Communications and Broadcastings industry personal information protection internal audit Checklist				
Checklist Check the below item number, the Department refer to Appendix 6	personal information protection Controls	Results		
		Meet	Not meet	Not applicable
7.5 Immediately removing or blocking access rights of users who have changed roles or jobs or left the organization.	◎			
7.6 Maintaining a formal record of all persons registered to use the service.	◎			
7.7 The allocation and use of privileges should be restricted and controlled. Multi-user systems that require protection against unauthorized access should have the allocation of privileges controlled through a formal authorization process.	◎			
7.8 An authorization process and a record of all privileges allocated should be maintained. Privileges should not be granted until the authorization process is complete.	◎			
7.9 Establish procedures to verify the identity of a user prior to providing a new, replacement or temporary password.	◎			
7.10 Temporary passwords should be given to users in a secure manner; the use of third parties or unprotected (clear text) electronic mail messages should be avoided.	◎			
7.11 Default vendor passwords should be altered following installation of systems or software.	◎			
7.12 Users should be required to sign a statement to keep personal passwords confidential; this signed statement could be included in the terms and conditions of employment.	◎			

Communications and Broadcastings industry personal information protection internal audit Checklist				
Checklist Check the below item number, the Department refer to Appendix 6	personal information protection Controls	Results		
		Meet	Not meet	Not applicable
7.13 When users are required to maintain their own passwords they should be provided initially with a secure temporary password, which they are forced to change immediately.	◎			
7.14 Passwords should never be stored on computer systems in an unprotected form.	◎			
7.15 Management should review users' access rights at regular intervals using a formal process.	◎			
7.16 Select quality passwords with sufficient minimum length.	◎			
7.17 Free of consecutive identical, all-numeric or all-alphabetic characters.	◎			
7.18 Change passwords whenever there is any indication of possible system or password compromise.	◎			
7.19 Change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid re-using or cycling old passwords.	◎			
7.20 Not include passwords in any automated log-on process, e.g. stored in a macro or function key.	◎			
7.21 Not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.	◎			
7.22 Avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely	◎			

Communications and Broadcastings industry personal information protection internal audit Checklist				
Checklist Check the below item number, the Department refer to Appendix 6	personal information protection Controls	Results		
		Meet	Not meet	Not applicable
and the method of storing has been approved.				
7.23 Limit the maximum and minimum time allowed for the log-on procedure. If exceeded, the system should terminate the log-on.	◎			
7.24 Not display the password being entered or consider hiding the password characters by symbols.	◎			
7.26 A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.	◎			
7.27 Computers and terminals should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and should be protected by key locks, passwords or other controls when not in use.	◎			
7.28 Sensitive or critical business information, e.g. on paper or on electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated.	◎			
7.29 Unauthorized use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) should be prevented.	◎			
7.30 Documents containing sensitive or classified information should be removed from printers immediately.	◎			

Communications and Broadcastings industry personal information protection internal audit Checklist				
Checklist Check the below item number, the Department refer to Appendix 6	personal information protection Controls	Results		
		Meet	Not meet	Not applicable
7.32 Display the following information on completion of a successful log-on: 1) date and time of the previous successful log-on; 2) details of any unsuccessful log-on attempts since the last successful log-on.	◎			
7.33 Limit the number of unsuccessful log-on attempts allowed, e.g. to three attempts, and consider: 1) recording unsuccessful and successful attempts; 2) forcing a time delay before further log-on attempts are allowed or rejecting any further attempts without specific authorization.	◎			
7.34 Establish a network service access security policy to ensure that specific authorization by the Department to allow users to access the network and network services.	◎			
7.35 Authentication of remote users can be achieved using, for example, a cryptographic based technique, hardware tokens, or a challenge/response protocol.	◎			
7.36 Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.	◎			
7.40 One method of controlling the security of large networks is to divide them into separate logical network domains, e.g. an organization’s internal network domains and external network domains, each protected by a defined security perimeter.	◎			

Communications and Broadcastings industry personal information protection internal audit Checklist				
Checklist Check the below item number, the Department refer to Appendix 6	personal information protection Controls	Results		
		Meet	Not meet	Not applicable
7.41 For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications.	◎			
7.43 The procedure for logging into an operating system should be designed to minimize the opportunity for unauthorized access. The log-on procedure should therefore disclose the minimum of information about the system, in order to avoid providing an unauthorized user with any unnecessary assistance.	◎			
7.44 Limit the number of unsuccessful log-on attempts allowed, e.g. to three attempts, and consider recording unsuccessful and successful attempts.	◎			
7.45 Login process for exceptions, leave records and regularly review.	◎			
7.46 Not transmit passwords in clear text over a network. If passwords are transmitted in clear text during the log-on session over a network, they may be captured by a network 'sniffer' program on the network.	◎			
7.47 All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.	◎			
7.48 Where strong authentication and identity	◎			

Communications and Broadcastings industry personal information protection internal audit Checklist				
Checklist Check the below item number, the Department refer to Appendix 6	personal information protection Controls	Results		
		Meet	Not meet	Not applicable
verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means, should be used.				
7.51 Inactive sessions should shut down after a defined period of inactivity.	◎			
7.52 Restrictions on connection times should be used to provide additional security for high-risk applications.	◎			
7.53 Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy.	◎			
7.54 Sensitive systems should have a dedicated (isolated) computing environment.	◎			
7.55 A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.	◎			
7.56 A policy, operational plans and procedures should be developed and implemented for teleworking activities. Organizations should only authorize teleworking activities if they are satisfied that appropriate security arrangements and controls are in place, and that these comply with the organization’s security policy.	◎			
7.57 Revocation of authority and access rights, and the return of equipment when the teleworking activities are terminated.	◎			

Communications and Broadcastings industry personal information protection internal audit Checklist				
Checklist Check the below item number, the Department refer to Appendix 6	personal information protection Controls	Results		
		Meet	Not meet	Not applicable
9. **Information security incident management**				
9.1 A formal information security event reporting procedure should be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event.	◎			
9.2 Information security events should be reported through appropriate management channels as quickly as possible.	◎			
9.3 Noting all important details (e.g. type of non-compliance or breach, occurring malfunction, messages on the screen, strange behavior) immediately.	◎			
9.4 A point of contact should be established for the reporting of information security events. It should be ensured that this point of contact is known throughout the organization, is always available and is able to provide adequate and timely response.	◎			
11. **Compliance**				
11.13 Information systems should be regularly checked for compliance with security implementation standards.	◎			
11.14 Technical compliance checking should be performed by an experienced system engineer.	◎			
11.15 Any technical compliance check should only be carried out by competent,	◎			

Communications and Broadcastings industry personal information protection internal audit Checklist				
Checklist Check the below item number, the Department refer to Appendix 6	personal information protection Controls	Results		
		Meet	Not meet	Not applicable
authorized persons, or under the supervision of such persons.				
11.16 All access should be monitored and logged to produce a reference trail; the use of time stamped reference trails should be considered for critical data or systems.	◎			
11.17 Such tests should be planned, documented and repeatable.	◎			
11.18 Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes.	◎			
11.19 On a regular basis for information security internal audit.	◎			
11.20 The scope of the checks should be agreed and controlled.	◎			
Summary	90			

Appendix 10. National Communications Commission ICS incidental report

National Communications Commission Incidental Reporting Unit - TEL: (02)2343-3560 / 2343-3768
Fax: (02)2343-3556e-mail: jmpd@ncc.gov.tw
Information & Communication Security Response Unit, Executive Yuan - TEL: (02)2733-9922, 0932-214-565
Fax: (02)2733-1655mailing address: No. 116 Fuyang Street, Da'an District, Taipei City 106
Time of report: YY MM DD hh mm Number:

1. Business contact for the security incident:
Name of business: Department:
Name of contact:
TEL: Fax: E-mail:

2. Items which communication/broadcasting businesses will report in the event of a security incident caused by external factors:
1. Time of incident: YY MM DD hh mm
(2) Equipment information:
◎IP Address:
External IP: Internal IP: (leave blank if none exists)
◎Internet IP (Web-URL): (leave blank if none exists)
◎Equipment brand and model:
◎Operating system name and version: □Windows □Linux □Other O/S; version:
◎Existing security mechanisms: □Firewall □Anti-virus software □Intrusion prevention
□Others:
3. Details of information and communication security incident:
◎Please evaluate the impacts caused by the security incident, in terms of confidentiality, integrity, and accessibility:
The overall impact of the security incident is determined as the highest level of severity between confidentiality, integrity, and accessibility aspects (i.e. the highest rating)
- Impacts to confidentiality: (choose one)
□ Leakage of top secret information (Severity 4)
□ Leakage of secret or sensitive business information (Severity 3)
□ Leakage of non-secret, non-sensitive information on principal activities (Severity 2)
□ Leakage of information on non-principal activities (Severity 1)
□ No information leakage (no reporting required)
- Impacts to integrity: (choose one)
□ Alteration to main IT infrastructure or data (Severity 4)
□ Severe alteration to principal systems or data (Severity 3)
□ Slight alteration to principal systems or data (Severity 2)
□ Alteration to non-principal systems or data (Severity 1)
□ No alteration to any system or data (no reporting required)
- Impacts to accessibility: (choose one)
□ Disruption to the IT infrastructure or system, where normal functions cannot be restored within

the tolerable downtime (Severity 4)

□ Disruption to principal activities or systems, where normal functions can not be restored within the tolerable downtime (Severity 3)

□ Affecting principal activities or reducing system efficiency, and is fully restored within the tolerable downtime (Severity 2)

□ Affecting non-principal activities or resulting in short disruptions only (Severity 1)

□ No impacts to systems or equipment (no reporting required)

◎Incident type: (choose one) □Illegal intrusion □Virus infection □Interrupted services □Others:

◎Extent of damage: (choose one) □System shutdown □Database damage □Alteration to webpage information □Others:

◎Incident description: (do not exceed 200 Chinese characters)

◎Evaluation of the possible consequences and losses: (do not exceed 200 Chinese characters)

◎Whether the incident affects other institutions or major public facilities: □Yes □No

◎Responsive measures: (do not exceed 200 Chinese characters)

3. Desired supports: (do not exceed 200 Chinese characters)

◎Whether support is needed: □Yes (please provide details on desired support) □No (no need to provide details on desired support)

Details of the desired support: (do not exceed 200 words)

4. Solutions:

◎Whether the incident was resolved at the time of this report: □Yes (please specify the solution and the time when resolved) □No (no need to specify the solution or time when resolved)

Solution: (do not exceed 200 words)

5. Time resolved: YY MM DD hh mm

Appendix 11. List of ICS rectifications / precautions

Company name					
Name of unit					
Unit supervisor			Date of assessment:		
Handling officer			Date of assessment:		
Contact	TEL:		Fax:	Mobile:	
	Email:			Page: of	
Form number	Serial number of checked item	Summary description on rectification and precaution measures	Closure status		Remarks
			Closed / unresolved	Completion date / expected completion date	

Appendix 12. ICS rectification / precaution order

Company name			
Name of unit			
Unit supervisor		Date of assessment:	
Handling officer		Date of assessment:	
Contact	TEL:	Fax:	Mobile:
	Email:		Page: of
Content of checked item			
Raise	Description on non-compliant issues (date discovered: YY MM DD):		
Rectification and precaution	1. Investigation and analysis of the underlying causes:		
	2. Rectification:		
	3. Precaution:		
Confirm	Case closure: □Yes (date of closure: YY MM DD) □No (expected date of closure: YY MM DD) Effectiveness of rectification/precaution measures (not required for unresolved cases):		

Appendix 13. Descriptions on non-applicable items specified in the internal audit worksheet

Company name			
Name of unit			
Unit supervisor		Date of assessment:	
Handling officer		Date of assessment:	
Contact	TEL:	Fax:	Mobile:
	Email:		Page: of
Serial number of checked item	Descriptions or supporting documents on inapplicability		

Remark: Please add additional fields wherever appropriate.

Appendix 14. Descriptions on non-applicable items specified in the list of additional audit focuses

Company name			
Name of unit			
Unit supervisor		Date of assessment:	
Handling officer		Date of assessment:	
Contact	TEL:	Fax:	Mobile:
	Email:		Page: of
Serial number of checked item	Descriptions or supporting documents on inapplicability		

Remark: Please add additional fields where appropriate.

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
1.資訊安全政策				A.5	安全政策			
				A.5.1		資訊安全政策 目標： 依據營運要求及相關法律與法規，管理階層提供資訊安全之指示與支持。		
1.1 是否依據相關法律、法規及營運要求，訂定組織資訊安全政策？	1.1 是否依照營運要求及相關法律、法規制定資訊安全政策？	文字措詞修訂		A.5.1.1			資訊安全政策之文件	6
1.2 是否考量組織之整體業務活動及其相關風險，訂定資訊安全政策？	1.2 規劃之資訊安全政策是否考量組織之整體業務活動及其相關風險？	文字措詞修訂						
1.3 是否識別違反資訊安全政策之後果及訂定處理程序？	1.3 是否識別且制定違反資訊安全政策之後果及處理程序？	文字措詞修訂						
1.4 是否由管理階層核准資訊安全政策文件，正式發布且轉知所有員工與各相關外部團體？	1.4 資訊安全政策文件是否由管理階層核准，並正式發布且轉知所有員工與相關各外部團體？	文字措詞修訂						
1.5 資訊安全政策文件是否包括資訊安全之定義、整體目標、範圍、實施內容、執行組織、權責分工、員工責任、事故通報處理流程？	1.5 資訊安全政策文件是否包括資訊安全之定義、整體目標、範圍、實施內容、執行組織、權責分工、員工責任、事故通報處理流程？							
1.6 是否依據資訊安全政策，訂定原則、標準及對組織特別重要之法規要求說明文件及資料（如法律、法規命令、行政規則、契約、安全教育、訓練、認知、營運持續管理、作業程序、資訊安全控管文件、使用者應遵守的安全規則）？	1.6 是否依據資訊安全政策，訂定原則、標準及對組織特別重要之遵循性要求說明文件及資料（如法律、法規、契約、安全教育、訓練、認知、營運持續管理、作業程序、資訊安全控管文件、使用者應遵循的安全規則）？	文字措詞修訂						
1.7 資訊安全政策是否就一般和特定責任之權責（包括通報資訊安全事故）加以定義？。	1.7 資訊安全政策文件是否就一般和特定責任之權責（包括通報資訊安全事故）分項說明？。	文字措詞修訂						
1.8 是否對支援資訊安全政策的文件建立補述文件？例如：針對特定資訊系統的更詳盡安全政策和程序，或使用者宜遵守的安全規則。	1.8 是否對可能支援資訊安全政策的文件建立參照？例如：針對特定資訊系統的更詳盡安全政策和程序，或使用者宜遵循的安全規則。	文字措詞修訂						
1.9 資訊安全政策是否由具有發展、審查及評估等核准權限之管理者，依規劃期間或有重大變更時，作必要之審查及調整？	1.9 資訊安全政策是否由經核准發展、審查及評估之管理階層依規劃之期間或有重大變更時對資訊安全政策、目標之適用性、充分性及有效性，定期作必要之審查及調整？	文字措詞修訂		A.5.1.2			資訊安全政策之審查	12
1.10 是否妥善維護資訊安全管理政策之審查紀錄與訂定管理審查程序，包括審查時程及週期?	1.10 是否妥善維護資訊安全政策審查的紀錄，並取得管理階層對已修訂政策的核准？	文字措詞修訂						
1.11 是否定期對組織人員及資訊設備進行安全評估，以確定其遵守資訊安全政策及相關規定？	1.11 是否定期對單位人員及資訊設備進行安全評估，以確定其是否遵守資訊安全政策及相關規定？							
1.12 是否指定專人或專責部門進行資訊安全政策的維護及檢討？	1.12 是否指定專人或專責部門進行資訊安全政策的維護及檢討？							

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
2.資訊安全之組織				A.6	資訊安全之組織			
				A.6.1		內部組織 目標：管理組織內之資訊安全。		
2.1管理階層是否在組織內藉由清楚的指派及確認資訊安全責任， 主動地展現承諾以支持安全？	2.1 管理階層是否制定、審查及核准跨越全組織之資訊安全實作？	參考CNS/ISO/IEC 27002 6.1.1條文內容修訂	◎	A.6.1.1			管理階層對資訊安全之承諾	8
2.2 是否指派擁有權責之管理階層或成立跨部門組織負責推動、協調及監督資訊安全管理事項？	2.2 是否指派適當權責之管理階層或成立跨部門組織負責推動、協調及監督資訊安全管理事項？			A.6.1.2			資訊安全協調~~工作~~	7
2.3 是否指定專人或專責部門，負責辦理下列資訊安全管理工作事項(1)資安政策、計畫、措施之研議，(2)風險評鑑、資訊分類、~~系統~~安全控管措施，(3)資料及資訊系統之使用管理及保護，(4)資安認知訓練及資安稽核？	2.3 是否指定專人或專責單位，負責辦理資安政策、計畫、措施之研議，資料、資訊系統之使用管理及保護，資安認知、教育、訓練、資安稽核等資訊安全範圍內之工作事項？	文字措詞修訂						
刪除與2.3點內容合併	2.4 是否指定部門辦理風險評鑑、資訊分類、系統安全控管措施？	與2.3點之內容合併						
2.4 資訊安全責任的配置是否依據資訊安全政策，並明確地識別~~需~~保護之個別資產與執行特定安全~~作業~~過程的責任，並加以文件化？	2.5 資訊安全責任的配置是否依據資訊安全政策，明確識別保護個別資產與執行特定安全作業過程的責任並文件化？	文字措詞修訂		A.6.1.3			資訊安全責任之配置	3
2.5 是否依據員工之職務~~內容~~，訂定員工資訊安全作業程序、權責規範或授權層級並予以文件化？（含經管使用設備及作業須知）	2.6 是否依據員工之職務內容訂定員工資訊安全作業程序、權責規範或授權層級並予以文件化？（含經管使用設備及作業須知）	文字措詞修訂		A.6.1.4			資訊處理設施之授權過程	3
2.6 是否訂定各項資訊處理設施之用途及使用授權，及~~其~~安全之作業程序？	2.7 是否訂定各項資訊處理設施之用途及使用授權，以及其安全之作業程序？	文字措詞修訂						
刪除	2.8 如使用膝上型電腦、家用電腦或手持裝置等個人或私人擁有的資訊處理設施來處理營運資訊，是否識別並實作必要的各項控制措施？	本項內容係2.7點內容之補充說明，建議刪除。						
2.7 是否識別並定期審查組織對於資訊保護之機密性或保密協議之要求？	2.9 是否依據資訊設備、安全區域及資訊的機密性，制定其保密協議？	參考XCNS/ISO/IEC 27002 6.1.5條文內容修訂		A.6.1.5			機密性協議	10
2.8 是否訂定當發生資安事故時，如何及時與主管機關聯繫並通報之適當程序或規定？	2.10 當有已違法之疑慮時，是否備有及時與權責機關聯繫、通報（例如：執法機關、消防單位及主管機關）所識別的資訊安全事故之適當程序或規定 ？	參考CNS/ISO/IEC 27002 6.1.6條文內容修訂		A.6.1.6			與權責機關之聯繫	2
2.9 是否~~訂定~~與各特殊利益團體、專家安全論壇及專業協會維持適當聯繫？	2.11 是否訂定與各特殊利害相關團體、專家安全性論壇、及專業協會聯繫管道？	文字措詞修訂		A.6.1.7			與特殊利益團體之聯繫	6

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
2.10 獨立審查組織對資訊安全管理之作法與其實作（例如：各項資訊安全的控制目標、控制措施、政策、過程及程序），是否定期召開管理審查會議？當資安作業環境發生重大變更時，亦依上述作法與實作，召開管理審查會議？	2.12 是否定期或資安作業環境發生重大變更時，召開管理審查會議，獨立審查組織對管理資訊安全的作法與其實作（例如：各項資訊安全的控制目標、控制措施、政策、過程及程序）	文字措詞修訂		A.6.1.8			資訊安全之獨立審查	1
				A.6.2		外部團體 目標： 維持外部團體存取、處理、通信或管理之組織資訊及資訊處理設施之安全。		
2.11 因營運需要開放給外部團體（含其他機關、往來業者、維護廠商、委外承包商、聘僱人員及一般民眾）使用之資訊，是否執行風險評鑑與實作安全控制措施？並於契約或規定中包含雙方權利、義務、資料保護、資訊保密、服務標的水準、智慧財產權、事故發生處理與違約處理等條款？	2.13 因營運需要開放給外部團體（含其他機關、往來業者、維護廠商、委外承包商、臨僱人員及一般民眾）使用之資訊，是否執行風險評鑑與識別，並於契約或規定中包含雙方權利、義務、資料保護、資訊保密、服務標的水準、智慧財產權、事故發生處理與違約處理等條款？	文字措詞修訂		A.6.2.1			識別與外部團體相關之風險	19
2.12 是否對不開放外部團體存取的資訊進行必要的控制措施？	2.15 是否對不打算被外部團體存取的資訊進行必要的控制措施？	文字措詞修訂						
2.13 因營運需要開放給外部組織或人員存取之資訊，其存取權限是否定期審查？	2.16 因營運需要開放給外部組織或人員存取之資訊，其存取權限是否定期審查？							
2.14 因營運需要開放給外部團體（含其他機關、往來業者、維護廠商、委外承包商、聘僱人員及一般民眾等）使用之資訊，於開放使用之前，是否闡明所有已識別之安全要求？	2.14 因營運需要開放給外部團體（含其他機關、往來業者、維護廠商、委外承包商、臨僱人員及一般民眾等）使用之資訊，其存取權限是否進行必要的控制措施？	參考CNS/ISO/IEC 27002 6.2.2條文內容修訂		A.6.2.2			處理客戶事務之安全說明	11
2.15 委外契約中有關安全需求內容，是否包含法律要求（如個人資料保護法）、雙方有關人員權責、安全控管措施、作業程序、事故通報程序、服務水準、對委外廠商稽核權等資訊安全責任與事宜，並得依實際需要適時修改安全控管措施及作業程序等？	2.17 委外契約中有關安全需求內容是否包含法律要求（如個人資料保護法）、雙方有關人員權責、安全控管措施、作業程序、事故通報程序、服務水準、對委外廠商稽核權等資訊安全責任與事宜，並得依實際需要隨時修改安全控管措施及作業程序等？	文字措詞修訂	◎	A.6.2.3			第三方協議中之安全說明	22

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
3.資產管理				A.7	資產管理			
				A.7.1		資產責任 目標： 達成及維持組織資產之適切保護。		
3.1 是否明確識別所有資產，並製作與維持所有重要資產的清冊？	3.1 是否明確識別所有資產，並製作與維持所有重要資產的清冊？			A.7.1.1			資產清冊	6
3.2 是否有明確之定義，如何分辨何種資產是重要資產，再依據該定義作資產盤點，並建立與維護重要資產清冊？	3.2 是否有明確之定義指出如何分辨何種資產是重要資產？再依據該定義作資產盤點並建立與維護重要資產盤點表。	文字措詞修訂						
3.3 現有之重要資產清冊是否包含災難回復所需之資訊，如：資產型態/格式/位置/備份資訊/使用版本/業務價值？	3.3 現有建立與維護之重要資產盤點表是否根據災難回復之所需並包含有（資產型態/格式/位置/備份資訊/合法版權/業務價值）？	文字措詞修訂						
3.4 資產清冊是否定期審查，確保資產處於適切狀態？	3.6 資產清冊是否定期審查、確保其隨時更新且處於適切狀態？	文字措詞修訂						
3.5 是否識別所有資訊資產之擁有者，並指派其依適切控制措施維護資訊資產之責任？	3.4 是否識別所有資訊資產之擁有者，並指派維護資訊資產之適切控制措施的責任？	文字措詞修訂		A.7.1.2			資產之擁有權	2
3.6 是否識別及實作所有與資訊處理設施相關（含電子郵件、網路使用及行動設備等）之使用規則，並加以文件化？	3.5 是否識別及實作所有資訊處理設施相關的資訊與資產（含電子郵件、網路使用及行動設備等）之使用規則並文件化？	文字措詞修訂		A.7.1.3			資產可被接受之使用	2
				A.7.2		資訊分類 目標： 確保資訊得到適切之保護等級。		
3.7 是否依據資訊對於組織的價值、法律要求、敏感性及重要性加以分類？	3.7 是否依據資訊資產對組織的價值、法律要求、敏感性及重要性加以分類？	文字措詞修訂		A.7.2.1			分類指導綱要	1
3.8 是否依據組織採用的分類法，訂定適當之資訊標示與處理程序？	3.8 是否依據組織採用的分類法，制定適當之資訊標示與處理的管理程序？	文字措詞修訂	◎	A.7.2.2			資訊標示與處理	1
3.9 是否對於機密性資訊、敏感性之手稿資訊、影印公文之廢紙及已過保存期限之公文，於棄置前予以銷毀？	3.9 若屬機密性、敏感性之手稿或影印公文廢紙及已過保存期限之公文，棄置之前是否予以銷毀？	文字措詞修訂	◎					
刪除	3.10 對於敏感或關鍵之資訊者，是否附上適當的分類標籤？	本項內容與3.8點內容雷同，建議刪除						

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
4.人力資源安全				A.8	人力資源安全			
				A.8.1		聘僱前 目標： 確保員工、承包商及第三方使用者瞭解其責任， 並勝任其所被賦予的角色，以降低竊盜、詐欺或設施誤用的風險。		
4.1 是否依照組織的資訊安全政策，訂定正式文件，規範所有員工、承包商或第三方使用者之安全角色與責任？	4.1 是否依照組織的資訊安全政策，定義與文件化所有員工、承包商或第三方使用者之安全角色與責任，包括關於機密性、資料保護、倫理及適切使用組織設備與設施？	文字措詞修訂	◎ ◎	A.8.1.1			角色與責任	5
4.2 是否明確定義所有聘僱之應徵者、承包商及第三方使用者背景查證檢核之限制與程序，確保符合隱私權、個人資料保護及/或聘僱勞工保護相關法令之要求？	4.2 是否明確定義背景查證檢核之限制與程序，確保符合隱私權、個人資料保護及/或聘僱相關法令？	文字措詞修訂		A.8.1.2			篩選	5
4.3 被賦予機敏資訊存取權的所有員工、承包商及第三方使用者，是否在被允許存取資訊處理設施之前，簽署適當之機密性或保密協議？	4.3 被賦予敏感資訊存取權的所有員工、承包商及第三方使用者，是否在被允許存取資訊處理設施之前，簽署適當之機密性或保密協議？	文字措詞修訂		A.8.1.3			聘僱任期與條件	7

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.8.2		聘僱期間 目標： 確保員工、承包商及第三方使用者認知資訊安全的威脅與關切事項、其責任與義務， 並有能力在日常工作中支持組織安全政策與降低人為錯誤的風險。		
刪除	4.4 員工、承包商及任何其他使用者的法定責任與權利是否明確定義且傳達給員工？	參考CNS/ISO/IEC 27002 8.2.1條文內容，本項應著重於聘僱期間管理階層之責任，建議刪		A.8.2.1			管理階層責任	6
刪除	4.5 由員工、承包商或第三方使用者所處理之資訊系統與服務的安全責任是否明確定義且傳達？	參考CNS/ISO/IEC 27002 8.2.1條文內容，本項應著重於聘僱期間管理階層之責任，建議刪除。						
刪除	4.6 對於可存取機密性、敏感性資訊或系統之員工以及配賦系統存取特別權限之員工是否有妥適分工與分散權責？	參考CNS/ISO/IEC 27002 8.2.1條文內容，本項應著重於聘僱期間管理階層之責任，建議刪除。						
4.4 管理階層是否有要求員工、承包商及第三方使用者，依照組織已訂定的政策與程序執行安全事宜？	4.8 管理階層是否有要求員工、承包商及第三方使用者，依照組織已制定的政策與程序施行安全事宜？	文字措詞修訂						
4.5 對所有員工、承包者及第三方使用者工作職務有關之安全程序及資訊處理設施，是否提供正確使用之認知、教育與訓練？	4.7 是否對所有員工、承包商及第三方使用者提供妥適等級之有關安全程序及資訊處理設施的正確使用之認知、教育與訓練？	文字措詞修訂		A.8.2.2			資訊安全認知、教育及訓練	1
刪除	4.9 組織所有員工和相關的承包商及第三方使用者，是否接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練？	本項與4.7點內容雷同，建議刪除						
4.6 是否訂定員工違反組織安全政策與程序之懲處規定？	4.10 是否訂有員工違反組織安全政策與程序之懲處規定？			A.8.2.3			懲處過程	1
				A.8.3		聘僱終止或變更目標： 確保員工、承包商及第三方使用者依規定離職或變更聘僱。		
4.7 是否在與員工、承包商或第三方使用者所訂之契約內規定，在聘僱終止後，與職務有關之責任仍然是有效的？		參考CNS/ISO/IEC 27002 8.3.1條文內容新增		A.8.3.1			終止責任	1
4.8 所有員工、承包商及第三方使用者離職或聘雇終止時，是否依規定繳回其任職期間保管之資訊資產？（包含所有的軟體、公司文件、設備、行動裝置、信用卡、存取卡、軟體、手冊及儲存於電子媒體的資訊等所有其他組織資產）	4.11 員工離職或第三方使用者於聘雇終止時，是否依規定繳回其使用或保管之資訊資產？（包含歸還所有先前發出的軟體、公司文件、設備、行動裝置、信用卡、存取卡、軟體、手冊及儲存於電子媒體的資訊等所有其他組織資產）	文字措詞修訂		A.8.3.2			資產之歸還	1

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
4.9 所有員工、承包商及第三方使用者之聘僱、契約或協議終止時，或因變更而調整時，是否對資訊及資訊處理設施之存取權限迅速予以移除？	4.12 是否於所有員工、承包商及第三方使用者對資訊及資訊處理設施的存取權限，在其聘僱、契約或協議終止時，或因變更而調整時，予以移除？	文字措詞修訂		A.8.3.3			存取權限之移除	3

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
5.實體及環境安全				A.9	實體及環境安全			
				A.9.1		安全區域 目標： 防止組織的場所及資訊遭未經授權的實體存取、損害及干擾。		
5.1 是否適當使用安全邊界（如圍牆、入口閘門或人員駐守的接待櫃檯等屏障），保護含有資訊與資訊處理設施的區域？	5.1 是否適當的使用安全周界（諸如牆、卡控入口閘門或人員駐守的接待櫃檯等屏障），以保護含有資訊與資訊處理設施的區域？	文字措詞修訂		A.9.1.1			實體安全周界	7
5.2 組織管理之資訊處理設施（如通訊服務設施），在實體上是否與第三方管理（如：客戶代管設備）之資訊處理設施區隔？	5.2 組織管理的資訊處理設施（如通訊服務設施）在實體上是否與第三方管理（如：客戶代管設備）的資訊處理設施區隔？	文字措詞修訂						
刪除	5.3 人員進入重要實體安全區域是否實施適當的安全控制措施，以確保只有經授權人員方可允許進出？	本項內容與5.4內容雷同，建議刪除。		A.9.1.2			實體進入控制措施	5
刪除	5.5 是否只於必要時才授權第三方支援服務人員限制性的進出安全區域或存取敏感資訊處理設施並受監視？	本項內容與5.4內容雷同，建議刪除。						
5.4 安全區域之進出權限是否定期審查並更新，並於必要時廢止？	5.6 安全區域的進出權限是否定期審查並更新，並於必要時廢止？	文字措詞修訂						
5.5 辦公處所是否實施必要之保護措施？	5.13 辦公處所是否實施必要之保護措施？		◎	A.9.1.3			辦公室、房間及設施之保全	4
5.6 是否檢查及評估重要資通訊設備設置地點，鄰近場所之任何安全威脅，如火災、灰塵、水災、震動、化學效應、電力供應、電磁幅射、民間暴動及其他天然或人爲災害等可能對設備之危害？	5.12 重要資訊設備之設置地點是否盡可能檢查及評估鄰近場所的任何安全威脅？如火災、灰塵、水災、震動、化學效應、電力供應、電磁幅射、民間暴動及其他天然或人爲災難等可能對設備之危害。	文字措詞修訂		A.9.1.4			防範外部與環境之威脅	3
5.7 是否設計並實施適當的控制措施，以保護敏感資訊處理設施之地點及內部人員通訊錄？	5.7 是否設計並施行適當的控制措施保護顯示敏感資訊處理設施地點的通訊錄和內部人員電話簿？	文字措詞修訂						
刪除	5.8 電腦機房操作人員是否熟悉自動滅火系統操作方法及滅火器位置？	參考CNS/ISO/IEC 27002 9.1.5條文內容，建議刪除。						
5.8 是否嚴禁在電腦機房內使用未經核准之電器或其他物品？	5.9 電腦機房內是否嚴禁使用未經核准之電器或其他物品？	文字措詞修訂						
5.9 備援設備及備份媒體存放位置，是否與主要場地保持安全距離？	5.10 備援設備及備份媒體存放位置是否與主要場地保持安全距離？	文字措詞修訂		A.9.1.5			在安全區域內工作	4

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
5.10 安全區域是否與易燃物或危險物料保持安全距離，並不宜儲存大量的物資？	5.11 安全區域是否與易燃物或危險物料保持安全距離，並不宜儲存大量的物資？	文字措詞修訂						
5.11 是否設計並實施適當之控制措施，監督安全區域內之工作，並確保其需知原則？	5.14 是否設計並施行適當之控制措施，以監督安全區域內之工作，並確保其需知原則？	文字措詞修訂						
5.12 是否訂定未經授權前，禁止拍照、錄影、錄音和其他記錄性設備之規定，如行動裝置上的照相機？	5.16 是否未經授權，不允許使用拍照、錄影、錄音和其他記錄性設備，諸如行動裝置上的照相機？	文字措詞修訂						
5.13 無人使用之安全區域是否上鎖並定期檢查？	5.15 無人使用之安全區域是否上鎖並定期檢查？							
5.14 對於收發、裝卸區及其他未經授權人員可進入之作業場所，是否有適當之進出控制措施，並應與資訊處理設施隔離，以避免未經授權的存取？	5.17 重要資訊處理設施是否與一般收發、裝卸區及其他未經授權人員可進入之作業場所作適當之進出控制措施？	文字措詞修訂		A.9.1.6			公共進出、收發及裝卸區	6
				A.9.1.7			維運中心之安全 Securing communication centres	8
				A.9.1.8			設備機房之安全 Securing telecommunications equipment room	15

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.9.1.9			隔離操作區之實體安全 Securing physically isolated operation areas	4
				A.9.2		設備安全 目標： 防止資產的遺失、損害、遭竊或洩漏及組織活動的中斷。		
5.15 是否明確訂定資通訊設備之控制措施（包括場外使用之設備，及財產之攜出），以降低資料未經授權存取、遺失及損壞之風險？	5.18 是否明確制定資訊設備（包括場外使用的設備，以及財產的攜出）之控制措施，以降低對資料未經授權存取的風險、遺失及損害？	文字措詞修訂		A.9.2.1			設備安置與保護	9
5.16 處理敏感資料的資通訊設備或資訊處理設施是否予特別保護並評估其有效性？	5.19 處理敏感資料的資訊處理設施是否予特別保護並評估其有效性？	文字措詞修訂						
5.17 是否採取適當控制措施，降低潛在實體威脅，如：竊盜、火災、爆裂物、煙害、水災（或水源供應停止）、閃電、溫度、濕度、灰塵、振動、化學效應、電力供應干擾、通信干擾、電磁輻射及蓄意破壞等？	5.20 是否採取適當控制措施以降低潛在的實體威脅，例如：竊盜、火災、爆裂物、煙害、水災（或水源供應停止）、閃電、溫度、濕度、灰塵、振動、化學效應、電力供應干擾、通信干擾、電磁輻射及蓄意破壞等？	文字措詞修訂						
5.18 電腦作業區（含機房）是否落實執行禁止抽煙及飲食？	5.21 電腦作業區（含機房）是否落實執行禁止抽煙及飲食？							
5.19 是否具備環境監控機制，掌握資通訊設備及資訊處理設施之溫度及溼度狀況？	5.22 是否具備環境監控機制，以掌握資訊處理設施溫度及溼度狀況？	文字措詞修訂						
5.20 是否對於支援性公共設施，如電源供應、水源供應、污水處理、暖氣/通風及空調，設計適當之保護措施，並施行之，確保不受公共設施失效所導致之中斷？	5.23 是否對於所有支援的公用設施，諸如電源、水源供應、污水處理、暖氣/通風及空調，設計並施行適當之保護，以確保對其所支援的系統不失效？	文字措詞修訂	◎	A.9.2.2			支援設施	1
5.21 備援電源是否定期檢查並測試，確保能在斷電期間正常運作？	5.24 備援電源是否定期檢查並測試，確保能在斷電期間運作？	文字措詞修訂						
5.22 電信機線設備（telecommunications lines）、網路佈纜（network cabling）及電源纜線，是否設計適當之安全保護措施，並施行之？	5.25 電信纜線（telecommunications lines）、網路佈纜（network cabling）及電源纜線是否設計施行適當之安全保護措施？	文字措詞修訂		A.9.2.3			佈纜的安全	6
5.23 通信纜線（communications cables）及電源纜線是否接地並隔離，防止互相干擾？	5.26 通信纜線（communications cables）及電源纜線是否隔離，以防止互相干擾？	文字措詞修訂						
5.24 設備是否定期且正確的維護保養，確保其可用性及完整性？	5.27 設備是否定期且正確的維護保養，以確保其可用性及完整性？							
5.25 各項設備是否依據供應商建議的間隔與保養手冊，定期檢查並維護？	5.28 各項安全設備是否依據供應者建議的保養間隔與規格來維護並定期檢查？	文字措詞修訂						

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
5.26 設備之維護與修理，是否由授權之維護人員執行？	5.29 設備之維護與修理是否僅由授權之維護人員執行？	文字措詞修訂		A.9.2.4			設備維護	5
5.27 是否妥適保存所有可疑、實際之系統錯誤資訊，及所有預防性、矯正性之維護紀錄？	5.30 是否宜保存所有可疑或實際的系統錯誤及所有預防性、矯正性的維護紀錄？	文字措詞修訂						
5.28 設備送場外維修，對於儲存在設備內資訊是否訂有安全保護措施？	5.31 設備送場外維修，對於儲存在設備內之資訊是否訂有安全保護措施？	文字措詞修訂						
5.29 攜出場所外之設備和媒體，是否訂有安全保護措施？	5.32 攜出場所外之設備和媒體是否訂有安全保護措施？	文字措詞修訂	◎	A.9.2.5			場所外設備之安全	4
5.30 行動裝置（設備）是否訂有嚴謹保護措施（如使用授權管理、設通行碼、檔案加密、專人看管）？	5.33 行動裝置（設備）是否訂有嚴謹的保護措施（如使用授權管理、設通行碼、檔案加密、專人看管）？	文字措詞修訂	◎					
5.31 設備汰除前，是否將機密性、敏感性資料及有版權的軟體予以移除或實施安全覆寫？	5.34 設備汰除前是否將機密性、敏感性資料及有版權的軟體予以移除或實施安全地覆寫？	文字措詞修訂	◎	A.9.2.6			設備汰除或再使用之安全	1
5.32 含有敏感性資訊之設備汰除後，是否根據風險評鑑決定實體銷毀與否？	5.35 含有敏感性資訊的設備汰除後，是否根據風險評鑑以決定是否宜實體銷毀？	文字措詞修訂	◎					
5.33 資訊資產如須攜出場外使用，是否經事前授權，並於攜出場外與歸還時，進行安全查核及紀錄？	5.36 資訊資產如須攜出場外使用，是否均經事前授權，並於攜出場外與歸還時進行安全查核且紀錄？	文字措詞修訂	◎	A.9.2.7			財產的攜出	4
				A.9.3		其他團體之安全管控 Security under the control of other party		
				A.9.3.1			位於其他服務供應商處之設備 Equipment sited in other carrier's premises	3
				A.9.3.2			位於使用者端之設備 Equipment sited in user premises	3
				A.9.3.3			互連之通訊服務 Interconnected telecommunications services	1
6.通訊及作業管理				A.10	通訊及作業管理			

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.10.1		作業程序與責任目標： 確保正確與安全地操作資訊處理設施。		
6.1 資訊處理設施與資通訊設備相關之各項作業程序及活動是否文件化、並適當維護？如電腦開機與關機程序、備份、設備維護、資訊的處理與處理、異常情況之處理、緊急聯絡資訊、重新啓動及復原程序、稽核存底與日誌資訊之維護、電腦機房與郵件處理管理，以及生命財產安全（safey）等。	6.1 資訊處理與通訊設施相關之各項作業程序及活動宜是否文件化？並適當維護？如電腦開機與關機程序、備份、設備維護、資訊的處理與處理、異常情況之處理、緊急聯絡資訊、重新啓動及復原程序、稽核存底與日誌資訊之維護、電腦機房與郵件處理管理，以及生命財產安全（safey）等。	文字措詞修訂		A.10.1.1			作業程序文件化	8
6.2 資訊處理設施與資通訊設備之變更，是否有正式核准之程序，並向相關人員通報變更細節？	6.2 資訊處理設施與系統的變更是否有正式核准之程序，並向所有人員通報變更細節？	文字措詞修訂		A.10.1.2			變更管理	6
6.3 資訊處理設施與資通訊設備之變更，是否詳實紀錄，並重新進行風險評鑑？	6.3 資訊處理設施與系統的變更是否詳實紀錄，並重新進行風險評鑑？	文字措詞修訂						
6.4 資訊處理設施與資通訊設備之變更，是否備有後撤(fallback)程序，包括不成功的變更、意外事故的中止及復原之程序與責任？	6.4 資訊處理設施與系統的變更是否備有後撤程序，包括由不成功的變更和意料之外事故的中止和復原之程序與責任？	文字措詞修訂						
6.5 對於安全要求較高的業務，是否區隔其職務與責任領域？	6.5 對於安全要求高的資訊業務，是否盡可能區隔其職務與責任領域？	文字措詞修訂		A.10.1.3			職務的區隔	1
6.6 業務資訊資產之使用、資料建檔、系統操作、網路管理、行政管理、系統發展維護、變更管理、安全管理等工作，是否授權由不同的人員執行？	6.6 業務系統之使用、資料建檔、系統操作、網路管理、行政管理、系統發展維護、變更管理、安全管理等工作是否盡可能授權由不同的人員執行？	文字措詞修訂						
6.7 是否分隔開發、測試及運作之設施、系統、軟體？	6.7 是否盡可能分隔開發、測試及運作之設施、系統、軟體？	文字措詞修訂		A.10.1.4			開發、測試及運作設施的分隔	6
6.8 運作測試系統是否使用不同的使用者剖繪（profile），且功能選單需顯示適切的識別訊息，降低錯誤之風險？	6.8 是否對於運作測試系統，使用不同的使用者剖繪（profile），功能選單宜顯示適切的識別訊息以降低錯誤的風險？	文字措詞修訂						

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.10.2		第三方服務交付管理 目標： 執行與維持適切之資訊安全等級服務交付，並與第三方服務交付協議一致。		
6.9 是否與第三方服務交付廠商簽訂適當之資訊安全協定，並納入契約條款，包含安全控制措施、服務定義及交付等級，並賦予相關安全管理責任？	6.9 是否與第三方服務交付廠商簽訂適當的資訊安全協定，包含安全控制措施、服務定義及交付等級，並賦予相關的安全管理責任，且納入契約條款？	文字措詞修訂		A.10.2.1			服務交付	1
6.10 是否規劃必要轉換（資訊、資訊處理設施及其他任何需要移動者）之安全控制措施，並確保轉換期間安全的維護？	6.10 是否規劃必要的轉換（資訊、資訊處理設施及其他任何需要移動者），並確保轉換期間安全的維護？	文字措詞修訂						
6.11 是否定期對第三方所提供之服務、報告及紀錄等進行適當之監視與審查，並定期執行稽核？	6.11 資訊業務由第三方提供服務期間，是否定期對廠商所提供之服務、報告及紀錄等進行適當之監視與審查，並定期執行稽核？	文字措詞修訂	◎	A.10.2.2			第三方服務的監視與審查	5
6.12 第三方提供之服務如有任何異動時，是否重新進行風險評鑑？	6.12 由第三方提供之服務如有任何異動時，是否評估資安措施之有效性？並作必要之調整。	參考CNS/ISO/IEC 27002 10.2.3條文內容修訂。	◎	A.10.2.3			第三方服務變更之管理	2
				A.10.3		系統規劃與驗收 目標： 使系統失效的風險最小化。		
6.13 資訊處理設施及資通訊設備設置前，是否進行容量規劃及預留安全容量，並於正式運作時，持續監控其容量狀態？	6.13 資訊相關設備設置前是否進行容量規劃並預留安全容量，並於正式運作時持續監控其容量狀態？	文字措詞修訂		A.10.3.1			容量管理	1
6.14 是否建立新資訊系統、系統升級或新版本之驗收準則，在新資訊系統、系統升級及新版本正式驗收後，才可移轉上線？	6.14 是否建立新系統或系統升級及新版本之驗收準則，並只有在正式驗收後，新資訊系統、系統升級及新版本才可移轉上線（含驗收標準及應有之測試）？	文字措詞修訂		A.10.3.2			系統驗收	10
				A.10.4		防範惡意碼與行動碼 目標： 保護軟體及資訊的完整性。		
6.15 是否全面使用防毒軟體，並即時更新病毒掃描引擎及病毒碼？	6.16 是否全面使用防毒軟體並即時更新病毒掃描引擎及病毒碼？	文字措詞修訂						
6.16 電腦系統及資料儲存媒體是否定期進行惡意程式病毒及後門程式掃描？	6.15 是否定期對電腦系統及資料儲存媒體進行病毒及後門程式掃描？	文字措詞修訂						

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
6.17 是否訂定正式政策，禁止使用未經授權的軟體？	6.17 是否制定正式政策禁止使用未經授權的軟體？	文字措詞修訂		A.10.4.1			防範惡意程式的控制措施	8
6.18 是否對支援重要營運程序之系統軟體與資料，執行定期審查？若出現任何未經核准的檔案或未經授權的增補修補程式，應進行正式調查。	6.18 是否對支援重要營運程序的系統之軟體與資料執行定期審查？若出現任何未經核准的檔案或未經授權的增補，宜正式調查。	文字措詞修訂						
6.19 是否訂定使用電子郵件附件及下載之檔案前，檢查有無惡意程式軟體（含病毒、木馬或後門等程式）之程序？	6.19 是否訂定電子郵件附件及下載檔案在使用前需檢查有無惡意軟體（含病毒、木馬或後門等程式）？	文字措詞修訂						
6.20 是否定義處理電腦病毒、木馬等惡意程式之管理程序與責任，並訓練員工如何通報惡意程式攻擊，及復原程序？	6.20 是否界定處理電腦病毒、木馬等惡意程式的管理程序與責任，訓練員工通報惡意程式之攻擊，並由其中復原？	文字措詞修訂						
6.21 是否準備遭惡意程式攻擊後復原之營運持續計畫，並包括所有必要之資料與軟體備份及復原準備工作？	6.21 是否準備遭惡意程式攻擊後復原的營運持續計畫，並包括所有必要的資料與軟體備份及復原安排？	文字措詞修訂						
				A.10.4.2			防範行動碼的控制措施	6
				A.10.5		備份 目標： 維持資訊及資訊處理設施的完整性與可用性。		
6.22 重要資訊及軟體是否定期作備份處理，並定義備份資訊之必要等級？	6.22 重要的資訊及軟體是否定期作備份處理，並界定備份資訊的必要等級？	文字措詞修訂		A.10.5.1			資訊備份	8
6.23 備份複本是否定期回復測試，並將回覆程序文件化，確保備份複本之可用性及有效性？	6.23 備份資訊是否定期回復測試，並將回覆程序及備份複本文件化，以確保備份資訊之可用性及有效性？	文字措詞修訂						
6.24 重要及機敏資訊之備份程度及頻率，是否反應組織的營運要求？	6.24 重要及機敏資訊的備份程度與頻率是否反應組織的營運要求？	文字措詞修訂						
6.25 備份資訊是否儲存於遠端地點？距離須足以避免主要場地發生災難時遭波及？	6.25 備份資訊是否儲存於遠端地點？距離須足以避免主要場地發生災難時遭波及？							
6.26 備份資訊是否給予適切等級之實體與環境保護，並與主要場域使用一致之標準？	6.26 備份資訊是否給予適切等級的實體與環境保護，並與主要場域使用的標準一致？	文字措詞修訂						
6.27 主要場域採用之控制措施是否延伸至涵蓋備份作業場域？	6.27 主要場域採用的控制措施是否延伸至涵蓋備份作業場域？	文字措詞修訂						
6.28 是否定期檢查及測試復原程序，確保有效性，且能夠在復原程序分配之時間內完成復原運作？	6.28 復原程序是否定期檢查與測試，以確保有效且能夠在用以復原之運作程序分配的時間內完成？	文字措詞修訂						

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.10.6		網路安全管理 目標： 確保網路資訊及支援基礎建設進行保護。		
刪除	6.29 有關網路安全之事項是否隨時公告？	參考CNS/ISO/IEC 27002 10.6.1條文內容，建議刪除。		A.10.6.1			網路控制措施	5
6.29 是否訂定網路及網路遠端設備之使用權責及程序？	6.30 是否訂定使用網路及網路遠端設備之使用權責及程序？	文字措詞修訂						
6.30 是否使用網路安全防禦設備，並適當的隔離外部網際網路與組織內部網路？	6.31 是否使用網路安全防禦設備，並適當的隔離外部網際網路與組織內部網路？							
6.31 組織建立之網路控制措施，是否能反應資訊之機密性、完整性與可用性要求？	6.32 組織建立之網路控制措施，是否能反應資訊的機密性、完整性與可用性要求？	文字措詞修訂						
6.32 對於機敏性資訊之傳輸過程，是否採取資訊加密等保護措施？	6.33 對於機敏性資訊之傳輸過程是否採取資訊加密等保護措施？	文字措詞修訂						
6.33 是否訂定確保網路服務連線品質及可用性之保護措施，提供最佳服務？	6.34 是否訂定爲確保網路服務連線品質及可用性之保護措施，以提供最佳服務？	文字措詞修訂		A.10.6.2			網路服務的安全	3
6.34 是否定期檢討網路安全控管事項之執行？	6.35 是否定期檢討網路安全控管事項之執行？							
6.35 是否定期檢測網路運作環境之安全漏洞？	6.36 是否定期檢測網路運作環境之安全漏洞？							
6.36 是否使用適當之網路安全解決方案？如防火牆、入侵偵測系統？防火牆存取政策（security policy）設定是否適當？	6.37 是否使用適當之網路安全解決方案？如防火牆、入侵偵測系統？防火牆存取政策（security policy）設定是否適當？							
				A.10.6.3			電信服務交付之安全管理 Security management of telecommunications services delivery.	10
				A.10.6.4			垃圾郵件之反應 Response to spam	1

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.10.6.5			DoS/DDoS攻擊之反應 Response to DoS/DDoS attacks	3

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.10.7		儲存媒體之處理 目標： 防止資產被未經授權的揭露、修改、移除或破壞，及中斷營運活動。		
6.37 是否建立各種可攜式媒體之操作管理程序，防止文件、電腦媒體（例如：磁帶、磁碟）、輸入或輸出資料及系統文件，遭受未經授權的揭露、修改、移除及破壞？	6.38 各種媒體是否建立操作程序，以防止文件、電腦媒體（例如：磁帶、磁碟）、輸入或輸出資料及系統文件被未經授權的揭露、修改、移除及破壞？	文字措詞修訂	◎	A.10.7.1			可攜式媒體的管理	6
刪除	6.39 是否訂定可移除式（磁帶、磁碟、快閃磁碟、抽取式硬碟、光碟（CD）、數位視訊影碟（DVD）及印出的媒體）管理程序？	本項內容與6.38點整併，建議刪除。						
6.38 含有敏感性資訊之媒體是否以正式程序加以安全地汰除，例如：焚化或絞碎，或清除資料後由組織內其他應用系統使用？	6.40 含有敏感資訊的媒體是否以正式程序加以安全地和無危險的汰除，例如：燬毀或撕碎，或清除資料後由組織內其他應用系統使用？	文字措詞修訂	◎	A.10.7.2			媒體的汰除	5
刪除	6.41 是否備妥程序以識別需要安全汰除的項目，並區分敏感項目？	本項內容與6.42點內容雷同，建議刪除。						
6.39 具機密性或敏感性資訊之媒體是否有安全之保存和報廢程序？	6.42 具機密性或敏感性資訊的媒體是否有安全之保存和報廢程序？	文字措詞修訂	◎					
6.40 機密性、敏感性資訊之儲存或處理是否有安全處理程序及分級標示？	6.43 機密性、敏感性資訊之儲存或處理是否有安全處理程序及分級標示？			A.10.7.3			資訊處理程序	9
6.41 是否建立資訊的處理及儲存的程序，以保護免於未經授權的揭露或誤用?	6.44 是否建立資訊的處理、處理、儲存及傳達之控制措施?	文字措詞修訂						
6.42 對應用程式、程序、資料結構及授權過程等說明之系統文件，是否有適當的存取保護措施？	6.46 包含對應用過程、程序、資料結構及授權過程等之說明的系統文件是否有適當的存取保護措施？	文字措詞修訂		A.10.7.4			系統文件之安全	3
				A.10.8		資訊交換 目標： 維護組織內及外部團體交換資訊及軟體的安全。		
刪除	6.45 對於採用語音、傳真及視訊通訊等設施進行資訊交換，是否訂有保護控制措施？	本項與6.47內容雷同，建議刪除。		A.10.8.1			資訊交換政策與程序	15
6.43 是否對於所有形式之資訊交換，訂定適當交換政策、程序及控制措施？	6.47 對於資訊及軟體之交換是否訂有適當的交換政策、程序及控制措施？	文字措詞修訂						

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
6.44 是否對高度機敏性資訊在傳輸或儲存中使用加密技術？	6.48 對高度機敏性的資訊在傳輸或儲存中是否使用加密技術？	文字措詞修訂						
6.45 是否訂定組織與任何外部團體間，交換資訊與軟體之協議？	6.49 組織與任何外部團體間資訊與軟體的交換，是否訂有交換協議，以保護經由使用所有形式之通信設施的資訊交換？	參考CNS/ISO/IEC 27002 10.8.2條文內容修訂。	◎	A.10.8.2			交換協議	11
6.46 重要電腦資訊、媒體（含報表）之運送，是否有安全保護措施及完整監控記錄（含收送人、時間及內容）？	6.50 重要電腦資訊、媒體（含報表）之運送，是否有安全保護措施並留有完整監控記錄（含收送人、時間及內容）？	文字措詞修訂	◎	A.10.8.3			輸送中的實體媒體	5
6.47 是否訂定適當控制措施，保護含有資訊之媒體，在組織實體邊界外傳送時，不受未經授權的存取、誤用或毀損？	6.51 是否制定適當之控制措施，以保護含有資訊的媒體在組織實體邊界外傳送時，不受未經授權的存取、誤用或毀損？	文字措詞修訂	◎					
6.48 採行電子交換之資訊，是否視資訊安全等級，採行識別碼與通行碼管制、電子資訊加密或電子簽章認證等保護措施，確保資訊的機密性、完整性、可用性及符合其他法律要求？	6.52 採行電子交換之資訊是否視資訊安全等級採行識別碼通行碼管制、電子訊加密或電子簽章認證等保護措施，以確保資訊的可用性、完整性、機密性及其他法律考量？	文字措詞修訂		A.10.8.4			電子傳訊	6
6.49 涉及敏感性資訊及機密文件之營運資訊系統，是否提供適當之存取控制與保護？	6.53 涉及敏感營運資訊及機密文件的營運資訊系統，是否提供適當地存取控制與保護？	文字措詞修訂		A.10.8.5			營運資訊系統	10
				A.10.9		電子商務服務 目標： 確保電子商務服務的安全及其安全使用。		
刪除	6.55 如有電子商務服務，是否制定適當之控制措施以確保安全性及其安全的使用？	本項與6.56點內容雷同，建議刪除。		A.10.9.1			電子商務	13
6.50 是否實施適當控制措施，保護在公眾網路上傳輸且涉及電子商務之資訊，使其不受詐欺行爲、契約爭議及未經授權之揭露與修改？	6.56 是否實施適當之控制措施，以保護在公眾網路上傳輸而涉及電子商務的資訊，使不受詐欺行爲、契約爭議及未經授權的揭露與修改？	文字措詞修訂	◎					
刪除	6.54 對於線上交易或申辦的資訊，是否訂有控制措施？以確保資訊之機密性及完整性。	本項與6.57點內容雷同，建議刪除。		A.10.9.2			線上交易	6
6.51 線上交易服務，是否訂定適當控制措施，防止下列事項：(1)不完整傳輸、(2)誤選路徑、(3)未經授權之訊息修改、揭露及(4)未經授權的訊息複製或重送(replay)等發生？	6.57 如有線上交易服務，是否制定適當之控制措施以防止不完整傳輸、誤選路、未經授權的訊息修改、未經授權的揭露、未經授權的訊息複製或重演？	文字措詞修訂	◎					
6.52 對外開放供公眾取得之資訊，是否訂定保護措施，確保資訊完整性，防止未經授權之修改？	6.58 對外開放之資訊，是否訂有保護措施以確保資訊完整性，並遵循任何法律要求？	文字措詞修訂		A.10.9.3			公眾可用的資訊	4
				A.10.10		監控 目標： 偵測未經授權的資訊處理活動。		

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
6.53 是否依據法律要求，如個資法，實施適當之稽核存錄措施，以紀錄使用者活動、異常及資訊安全事故？	6.59 是否實施適當之稽核存錄措施，以紀錄使用者活動、異常及資訊安全事故，並考量法規要求？	文字措詞修訂	◎	A.10.10.1			稽核存錄	12
6.54 是否採用適切的存錄與監控設備，記錄資通訊相關活動？	6.60 是否採用適切的存錄與監視以記錄資訊安全相關行動？	文字措詞修訂		A.10.10.2			監控系統的使用	5
6.55 是否建立適當之控制措施，監控資訊處理設施之使用，及定期審查？	6.61 是否建立適當之控制措施以監視資訊處理設施的使用，並定期審查？	文字措詞修訂						
6.56 各項日誌是否有適當的保護措施，不受竄改與未經授權之存取，並針對留存之通信資訊設定適當之留存期限（例如：會計、帳務、客訴的處理、防止濫用及執法機關的要求）？	6.62 各項日誌是否有適當的保護措施，不受竄改與未經授權的存取，並針對留存之通信資料設定適當之留存期限（例如：會計、帳務、客訴的處理、防止濫用及執法機關的要求）？	文字措詞修訂		A.10.10.3			日誌資訊的保護	3
6.57 是否定期稽查各項作業日誌？	6.63 各項作業日誌是否定期稽查？	文字措詞修訂						
6.58 是否適當規劃存錄設施與日誌資訊之儲存媒體容量，避免無法記錄事故或覆蓋以往所記錄事故？	6.64 存錄設施與日誌資訊是否規劃適當之儲存媒體容量，以避免無法記錄事故或覆蓋以往所記錄事故？	文字措詞修訂						
6.59 作業日誌是否留有管理者與操作者所涉及活動之詳細過程，並定期予以審查？	6.65 是否留有詳細的管理者與操作員所涉及的過程之作業日誌，系統管理者與操作者日誌是否定期予以審查？	文字措詞修訂	◎	A.10.10.4			管理者與操作者日誌	4
刪除	6.66 資安事故日誌之紀錄內容是否包括使用者識別碼、登入登出之日期時間、電腦的識別資訊或其網址、事故描述及矯正措施等事項？	參考CNS/ISO/IEC 27002 10.8.2條文內容，建議刪除。		A.10.10.5			失誤存錄	2
6.60 是否加以存錄由使用者或系統程式所通報之資訊處理或通信系統問題，迅速處理及通報？	6.67 由使用者或系統程式所通報失誤，相關於資訊處理或通信系統的問題是否加以存錄？並明確的處理所通報之失誤的規則？	文字措詞修訂						
6.61 所有系統鐘訊是否與議定之鐘訊來源校正，以確保時間紀錄正確？	6.68 所有系統鐘訊是否定期核對校正？以確保時間紀錄正確。	文字措詞修訂		A.10.10.6			鐘訊同步	1
7.存取控制				A.11	存取控制			

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.11.1		存取控制之營運要求目標： 控制資訊的存取。		
7.1 是否根據營運與安全要求，建立、文件化及審查存取控制政策？	7.1 是否根據營運與安全要求，建立、文件化及審查存取控制政策及相關說明文件？	文字措詞修訂		A.11.1.1			存取控制政策	16
7.2是否在存取政策文件中明確陳述每個使用者或使用群組之存取控制規則與權限？	7.2 存取政策聲明中是否明確陳述每個使用者或使用群組的存取控制規則與權限？	文字措詞修訂						
7.3 資訊存取控制政策是否符合相關法律、法規命令及契約規定，如電信法、個資法等？	7.3 資訊存取控制政策是否符合個人資訊保護等相關法令與契約規定？	文字措詞修訂						
				A.11.2		使用者存取管理目標： 確保經授權使用者對資訊系統的存取及防止未經授權的存取。		
刪除	7.4 是否定期審查並移除未使用之使用者權限？	本項與7.5點內容雷同，建議刪除。		A.11.2.1			使用者註冊	10
7.4 是否對所有資訊系統與服務核准和撤銷存取，訂定適當之使用者註冊與註銷程序？	7.5 是否設定適當的正式使用者註冊與註銷註冊程序，以對所有資訊系統與服務核准和撤銷存取？	文字措詞修訂	◎					
7.5 是否於使用者變更角色、調職或離職後，立即移除或封鎖其存取權限？	7.6 是否於使用者因變更角色或調職或離職後，立即移除或封鎖其存取權限？	文字措詞修訂	◎					
7.6 是否維持所有使用者註冊服務、系統或資訊等之正式紀錄？	7.7 是否維持所有使用者註冊服務、系統或資訊等的正式紀錄。	文字措詞修訂	◎					
7.7 基於系統管理或特殊作業需要，需設定特殊權限時（如系統管理、高階管理者），是否透過正式授權過程，控制特殊權限之配置？	7.8 基於系統管理或特殊作業需要，如需設定特殊權限時（如系統管理、高階管理者），是否透過正式的授權過程來控制特權的配置？	文字措詞修訂		A.11.2.2			特權管理	6
7.8 是否維護所有配置特殊權限之授權過程和紀錄，並於完成授權過程後才授予特殊權限？	7.9 是否維護所有配置特權的授權過程和紀錄，並完成授權過程後才授予特權？	文字措詞修訂						
7.9 是否在提供使用者通行碼前，進行身份鑑別程序？	7.10 是否在提供使用者通行碼之前，進行身份確認程序？	文字措詞修訂		A.11.2.3			使用者通行碼管理	8
7.10 是否以安全之程序轉交預設之通行碼給使用者，使用者取得通行碼，確認無誤後，需回應系統管理者？	7.11 預設之通行碼是否以安全之程序轉交於使用者，使用者取得通行碼確認無誤後需回應系統管理者？	文字措詞修訂						
7.11 軟體安裝完畢後，是否立即更新廠商所預設之通行碼？	7.12 軟體安裝完畢後是否立即更新廠商所預設之通行碼？	文字措詞修訂						
7.12 是否要求使用者於聘僱任期與條件中，簽署對個人通行碼保密聲明？	7.13 是否要求使用者於聘僱條款與條件中，簽署對個人通行碼保密的聲明？	文字措詞修訂						

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
7.13 是否強制要求使用者，初次登入電腦系統後，必須立即更改預設通行碼，或一定期限內未登入，則預設通行碼將失效，必須重新申請建立？	7.14 是否強制要求使用者初次登入電腦系統後必須立即更改預設之通行碼或一定期限內未登入，則預設通行碼將失效，必須重新再申請建立？	文字措詞修訂						
7.14 是否規定通行碼不得以無保護之型式儲存於電腦系統中？	7.15 通行碼是否永不以無保護之型式儲存於電腦系統中？	文字措詞修訂						
7.15 所有使用者存取權限，是否定期檢查（建議每六個月一次、特權者每三個月一次）及任何變更(如升職、降職、調職或聘僱終止等)後審查？	7.16 所有使用者存取權限是否定期檢查（建議每六個月一次、特權者每三個月一次）以及在諸如升職、降職、調職或聘僱終止等的任何變更後審查之。	文字措詞修訂		A.11.2.4			使用者存取權限之審查	5
				A.11.3		使用者責任 目標： 防止未經授權的使用者存取、危及或竊盜資訊及資訊處理設施。		
7.16 通行碼長度是否規定須超過6個字元（建議以9個字元位或以上）？	7.17 通行碼長度是否規定須超過6個字元（建議以9位或以上）？							
7.17 通行碼是否規定需以大小寫字母、特殊符號及數字組成？	7.18 通行碼是否規定需以大小寫字母及數字組成？							
7.18 通行碼輸入錯誤，是否訂有三次以內之限制？	7.19 通行碼輸入錯誤，是否訂有三次以下之限制？	文字措詞修訂						
7.19 是否定期、依規定期限或使用次數限制，要求變更通行碼，並避免重複或循環使用舊通行碼？	7.20 是否定期或依規定期限或使用次數限制，要求變更通行碼，並避免重複或循環使用舊通行碼？	文字措詞修訂						
7.20 是否規定不得在任何自動登入過程中內含通行碼，例如：儲存在巨集或功能鍵中。	7.21 不允許在任何自動登入過程中內含通行碼，例如：儲存在巨集或功能鍵中。	文字措詞修訂						
7.21 是否規定避免使用與個人有關資訊（如生日、身分證統一編號、單位簡稱、電話號碼等）當做通行碼？	7.22 是否規定避免使用與個人有關資訊（如生日、身份證字號、單位簡稱、電話號碼等）當做通行碼？	文字措詞修訂		A.11.3.1			通行碼的使用	9
7.22 是否避免保留通行碼的紀錄（例如：紙張、軟體檔案或手持裝置），除非其能被安全地存放，且該存放方式經過核准？	7.23 是否避免保留通行碼的紀錄（例如：紙張、軟體檔案或手持裝置），除非其能被安全地存放，且該存放方式經過核准？							
7.23 應用系統是否具有作業結束後或在一定期間未操作時即自動登出之保護機制？	7.24 應用系統是否具有作業結束後或在一定期間未操作時即自動登出之保護機制？							
刪除	7.26 個人電腦及終端機不使用時是否有關機或登出或設定螢幕通行碼或其他控制措施進行保護？	本項與7.29、7.30內容重複，建議刪除。						
7.24 是否避免將輸入之通行碼以明文方式顯示在螢幕上？	7.27 是否避免將輸入之通行碼以明文方式顯示在螢幕上？							
7.25是否 對於無人看管之資訊設施有適當保護措施？	7.25 對於無人看管之資訊設施是否有適當保護措施？	文字措詞修訂		A.11.3.2			無人看管之使用者設備	3
7.26 是否訂有桌面淨空及螢幕淨空政策？	7.28 是否訂有敏感或重要的營運資訊之桌面淨空及螢幕淨空政策？	文字措詞修訂	◎					
刪除	7.29 個人電腦及終端機不使用時是否有關機、登出、設定螢幕密碼或是以其他控制措施進行保護？	本項與7.26、7.30內容重複，建議刪除。						

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
7.27 主機、伺服器、個人電腦、終端機等電腦設備於不使用、人員離座時是否即刻進行保護措施如關機、登出、設定螢幕保護密碼或是以其他控制措施進行保護？	7.30 主機、伺服器、個人電腦、終端機等電腦設備於不使用、人員離座時是否即刻進行保護措施如關機、登出、設定螢幕密碼或是以其他控制措施進行保護？	文字措詞修訂	◎	A.11.3.3			桌面淨空與螢幕淨空政策	5
7.28 下班後經辦之機密性及敏感性資訊是否妥爲收存？	7.31 下班後經辦之機密性及敏感性資訊是否妥爲收存？		◎					
7.29 是否訂定適當之控制措施，防止未經授權使用影印機和其他複製設備（例如：掃瞄器、數位相機）？	7.32 是否定有適當之控制措施，以防止影印機和其他重製技術（例如：掃瞄器、數位相機）的未經授權使用？	文字措詞修訂	◎					
7.30 敏感性或機密性資訊文件，是否立即從印表機上取走？	7.33 包含敏感或機密資訊的文件是否立即從印表機上取走？	文字措詞修訂	◎					
				A.11.4		網路存取控制 目標： 防止網路服務遭未經授權的存取。		
7.31 網路使用者（含外單位人員）是否取得正式存取授權？	7.34 網路使用者（含外單位人員）是否取得正式存取授權？			A.11.4.1			網路服務的使用政策	4
7.32 是否於登入作業完成後，顯示前一次登入日期與時間，或提供登入失敗之詳細資訊？	7.35 是否於登入作業完成後顯示前一次登入的日期與時間，或提供登入失敗的詳細資訊？	文字措詞修訂		A.11.4.2			外部連線之使用者鑑別	1
7.33 是否限制登入失敗次數超過上限時，需強制延遲一段時間或重新取得授權後才允許再登入？	7.36 是否限制登入失敗次數超過上限時需強制延遲一段時間或重新取得授權後才可再登入？	文字措詞修訂						
7.34 是否訂定網路服務存取安全政策，確保使用者係經特定授權允許存取網路與網路服務？	7.37 是否訂定網路服務存取安全政策，確保使用者存取的網路與網路服務經特定授權所允許？	文字措詞修訂						
7.35 對於外部連線使用者是否進行身份鑑別機制，如密碼技術、硬體符記或詰問/應答（challenge/response）協定等安全技術？	7.38 對於外部連線使用者是否進行身份鑑別機制，如密碼技術、硬體符記或詰問/應答（challenge/response）協定等安全技術？							
7.36 是否採用自動設備識別方法，鑑別存取敏感或機密資訊之設備，方可允許其存取行爲？	7.39 是否識別允許存取敏感或機密資訊之設備，方可允許其存取行爲？	參考CNS/ISO/IEC 27002 11.4.3條文內容修訂。		A.11.4.3			網路設備識別	1
7.37 對於遠端使用者的存取控制，是否有適當的鑑別機制？	7.40 對於遠端使用者的存取控制，是否有適當的鑑別機制？			A.11.4.4			遠端診斷與組態埠保護	1
刪除	7.41 是否使用自動識別設備，以鑑別來自特定地點或設備之連線？	本項與7.39修訂後之內容重複，建議刪除。						
7.38 如需採用遠端診斷作業方式，是否訂定診斷埠之存取作業規範（如用金鑰管理及人員身份查驗或稽核等機制）？	7.42 如需採用遠端診斷作業方式，是否有訂定診斷埠的存取作業規範（如用金鑰管理及人員身份查驗或稽核等機制）？	文字措詞修訂						
7.39 無線網路之存取及應用，是否訂有嚴謹之鑑別、加密方式及頻率選擇等控制措施？	7.43 無線網路之存取及應用，是否訂有嚴謹的鑑別、加密方式及頻率選擇等控制措施？	文字措詞修訂						
7.40 是否依據網路服務需要，區隔出獨立邏輯網域（如組織內部網路或外部網路），每個網域皆有定義的安全邊界，及通訊閘道管制過濾網域間資料之存取（如網路防火牆）？	7.44 是否依據網路服務需要區隔出獨立的邏輯網域（如組織內部網路或外部網路），每個網域皆有定義的安全周界並有通訊閘道管制過濾網域間資料訊的存取（如網路防火牆）？	文字措詞修訂		A.11.4.5			網路區隔	1

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
刪除	7.45 是否設有檢測連線的來源位址與目的位址網路路由之控管措施？	參考CNS/ISO/IEC 27002 11.4.6條文內容，建議刪除。 描述之功能與7.44內容雷同。		A.11.4.6			網路連線控制	4
7.41 是否針對電子郵件、單雙向檔案傳輸、互動式存取或應用系統之存取時段作必要之限制？	7.46 是否針對電子郵件、單雙向檔案傳輸、互動式（或應用系統）存取與存取時段作必要之安全控制措施？	文字措詞修訂						
7.42 是否實施網路路徑控制，以確保電腦連線及資訊流，不會破壞營運應用程式之存取控制政策？		參考CNS/ISO/IEC 27002 11.4.7條文內容新增。		A.11.4.7			網路選路徑控制	1
				A.11.4.8			電信服務商之識別與鑑別 Telecommunications carrier identification and authentication by users.	1
				A.11.5		作業系統存取控制目標： 防止作業系統遭未經授權的存取。		
7.43 是否提供登入程序最小限之系統輔助訊息，避免提供未經授權使用者任何不必要協助？	7.47 登入程序，是否僅提供適當輔助訊息？	文字措詞修訂		A.11.5.1			安全之登入程序	9
7.44 是否依據系統機敏度，限制登入失敗次數之上限，並於登入失敗後中斷連線？	7.48 是否依據系統之機敏度，限制登入失敗次數的上限，並於登入失敗後中斷連線？	文字措詞修訂						
7.45 是否對於異常登入程序，留有紀錄及定期檢視？	7.49 對於異常登入程序，是否留有紀錄，並有專人定期檢視？	文字措詞修訂						
7.46 系統登入或存取重要資訊時，是否對連線過程提供加密之程序與措施？	7.50 系統登入或存取重要資訊時，是否提供對連線過程加密之程序與措施？	文字措詞修訂						
7.47 使用者是否採用具有唯一性之識別符號（使用者ID）？	7.51 使用者是否均有唯一的識別符（使用者ID）？	文字措詞修訂		A.11.5.2			使用者識別與鑑別	1
7.48 重要系統使用者，是否採用適切之身分鑑別技術，例如：一次性密碼、智慧卡、符記或生物特徵？	7.52 重要系統使用者除採一般識別符外，是否採用適切的替代身份鑑別技術？例如：密碼方法、智慧卡、符記或生物量測方法。	文字措詞修訂						
7.49 是否以保護的形式儲存和傳送通行碼，並告知申請者？通行碼檔案是否和應用系統資料分開存放？	7.53 是否以保護（例如加密或雜湊）的形式儲存和傳送通行碼，並告知申請者？	參考CNS/ISO/IEC 27002 11.5.3條文內容增訂。		A.11.5.3			通行碼管理系統	9

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
7.50 使用系統公用程式是否進行授權管制（如最低實務需求的授權）及身分鑑別程序？需要職務區隔時，是否有管制措施不讓具備系統應用程式存取權限的使用者，取得系統公用程式之權限？	7.54 使用系統公用程式是否作授權管制（如最低實務需求的授權）及身份鑑別程序？	參考CNS/ISO/IEC 27002 11.5.4條文內容增訂。		A.11.5.4			系統公用程式的使用	9
7.51 是否設定網路會談結束或超過定義的無動作時限後，即中斷連線或關閉設備？	7.55 是否限制網路會談結束或過定義的不動作時限後，即予中斷連線或關閉設備？	文字措詞修訂		A.11.5.5			會談逾時	1
7.52 對風險高之應用系統，是否限制連線時間，如連線時間限制在正常辦公時間內？	7.56 對風險高的應用系統是否設定連線時間限制？如連線時間限制在正常辦公時間內。	文字措詞修訂		A.11.5.6			連線時間的限制	3
				A.11.6		應用系統與資訊存取控制 目標： 防止應用系統中的資訊遭未經授權的存取。		
刪除	7.57 對風險高的應用系統是否限於有實際需要時連線？	參考CNS/ISO/IEC 27002 11.6.1條文內容，建議刪除。		A.11.6.1			資訊存取限制	4
7.53 是否訂定使用者及支援人員，對應用系統存取權限之管制措施？	7.58 是否訂有使用者對應用系統資訊存取之權限管制措施？	文字措詞修訂						
7.54 處理機密及敏感性資訊，是否採用專屬（隔離）電腦作業環境？	7.59 機密及敏感性資訊的處理是否採用專屬（隔離）的電腦作業環境	文字措詞修訂	◎	A.11.6.2			敏感性系統的隔離	2
				A.11.7		行動計算與遠距工作 目標： 確保使用行動運算與遠距工作設施時之資訊安全。		
7.55 是否訂定行動運算及通信設備之管理政策（如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求）？	7.60 是否訂定行動式之電腦及通信設備之管理政策（如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求）？	文字措詞修訂	◎	A.11.7.1			行動運算與通信	2
7.56 遠距工作是否得到管理階層授權（如活動政策、計畫及流程等）和施以必要之保護措施？	7.61 遠距工作是否得到管理階層授權（如活動政策、計畫及流程等）和施以必要之保護措施？			A.11.7.2			遠距工作	19
7.57 遠距工作活動結束後，是否撤銷相關授權與存取權限及歸還管制設備？	7.62 遠距工作活動結束後，是否進行相關授權、存取權限之撤銷並管制設備歸還？	文字措詞修訂						
8.資訊系統獲取、開發及維護				A.12	資訊系統獲取、開發及維護			

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.12.1		資訊系統之安全要求 目標： 確保安全是整體資訊系統的一部分。		
8.1 在規劃應用系統需求時，是否將安全需求納入分析及規格文件中？	8.1 應用系統在規劃需求時是否將安全要求納入分析及規格？	文字措詞修訂	◎	A.12.1.1			安全需求之分析與規格	1
				A.12.2		應用系統之正確處理 目標： 防止應用系統中資訊的錯誤、遺失、未經授權的修改或誤用。		
8.2 是否檢查輸入資料，確認其正確性及適切性？	8.2 輸入資訊是否作檢查，以確認其正確且適切性？	文字措詞修訂		A.12.2.1			輸入資料確認	7
8.3 是否針對輸入錯誤，設計及實作回應程序？	8.3 是否針對輸入錯誤，設計並實作回應程序？	文字措詞修訂						
8.4 應用程式內部處理是否加入確認查核（validation check），偵測可能經由處理錯誤或故意行爲之任何資訊毀損，並提供適當程式從失效中復原，確保資料之正確處理？	8.4 應用程式內部處理是否加入確認查核（validation check），以偵測經由處理錯誤或故意行爲之任何資訊毀損？	文字措詞修訂		A.12.2.2			內部處理的控制措施	12
8.5 應用系統是否使用密碼技術，鑑別與保護其訊息之完整性？	8.5 應用系統是否使用密碼技術，以鑑別與保護訊息的完整性？	文字措詞修訂		A.12.2.3			訊息完整性	1
8.6 輸出資訊是否具合理性查核及一致性控制計數（reconciliation control count），確保所有資料都已合理處理？	8.6 輸出資訊是否具合理性查核及一致性控制計數（reconciliation control count）以確保所有資料都已合理處理？	文字措詞修訂		A.12.2.4			輸出資料確認	6
8.7 是否設計與實作輸出確認測試與回應之程序？	8.7 是否設計與實作出對輸出確認測試作回應的程序？	文字措詞修訂						
8.8 是否設計並實作資料輸出確認過程之活動日誌，並定義所有涉及資料輸出過程人員之責任？	8.8 是否設計並實作資料輸出確認過程活動的日誌，並定義所有涉及資料輸出過程人員的責任？	文字措詞修訂						
				A.12.3		密碼控制措施 目標： 藉由密碼方式以保護資訊的機密性、鑑別性或完整性。		
8.9 是否基於風險評鑑結果，識別所需的保護等級，設計所需加解密演算法之型式、強度及品質？	8.10 是否基於風險評鑑，考量所需加密演算法的型式、強度及品質，宜識別所需的保護等級？	文字措詞修訂		A.12.3.1			使用密碼控制措施的政策	7
8.10 是否基於風險評鑑結果管理密碼金鑰，並發展適當之控制措施？	8.11 密碼金鑰管理是否基於風險評鑑，並發展適當之控制措施？	文字措詞修訂		A.12.3.2			金鑰管理	11

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.12.4		系統檔案之安全目標： 確保系統檔案的安全。		
8.11 作業系統升級前，是否考量營運要求及該版本之安全性？	8.12 作業系統升級前是否作變更營運要求及版本安全性評估？	文字措詞修訂		A.12.4.1			作業軟體之控制	8
8.12 處理作業系統軟體更新之人員，是否經管理階層授權？	8.9 作業系統軟體更新是否需經管理階層授權之人員處理？	文字措詞修訂						
8.13 是否限定由經過訓練合格之管理人員，才可執行應用程式可執行碼更新作業？	8.13 應用程式可執行碼更新作業是否限定由授權的管理人員才可執行？	文字措詞修訂						
8.14 是否使用組態控制系統，以保持對所有已實作的軟體與系統文件之控制，且維護所有變更紀錄？	8.14 是否維持將所有變更紀錄且妥善維持？	文字措詞修訂						
8.15 是否避免以真實資訊進行測試作業？	8.15 測試作業是否避免以真實資訊進行？	文字措詞修訂		A.12.4.2			系統測試資料之保護	4
8.16 存取程式原始碼（program source code），是否訂有適當之控制措施，並留存稽核日誌？	8.16 程式原始碼（program source code）之存取，是否訂有適當之控制措施？	文字措詞修訂		A.12.4.3			程式源碼之存取控制	7
刪除	8.17 所有程式原始碼之存取行爲，是否留有稽核日誌？	本項內容與8.16整併，建議刪除。						
				A.12.5		開發及支援處理之安全 目標： 維持應用系統軟體及資訊的安全。		
8.17 是否建立變更應用系統之管制程序？	8.18 是否建立應用系統之變更管制程序？	文字措詞修訂		A.12.5.1			變更控制程序	11
8.18 應用系統變更後，是否立即更新系統文件？	8.19 系統變更後是否立即更新系統文件？	文字措詞修訂						
8.19 作業系統變更後，是否對應用系統作技術性審查？	8.20 作業系統變更後，是否對應用系統作技術性審查？			A.12.5.2			作業系統變更後的應用系統技	4
8.20 作業系統變更後，是否主動公告異動範圍、時間及可能的影響？	8.21 系統變更後，是否主動公告異動範圍、時間、可能的影響？	文字措詞修訂						

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
8.21 作業系統變更後，是否檢查其相關控管措施與程序仍然有效？	8.22 系統變更後檢查其相關控管措施與程序是否仍然有效？	文字措詞修訂		A.12.5.2			術審查	4
刪除	8.24 系統安裝後是否管制程式碼？	參考CNS/ISO/IEC 27002 12.5.2條文內容，建議刪除。						
8.22 是否僅限於必要的範圍，變更套裝軟體之，並嚴格管制所有變更？		參考CNS/ISO/IEC 27002 12.5.3條文內容，建議新增。	◎	A.12.5.3			套裝軟體變更的限制	4
8.23 是否檢查組織內可能之隱匿通道(covert channel)，降低資訊洩漏的風險？		參考CNS/ISO/IEC 27002 12.5.4條文內容，建議新增。		A.12.5.4			資料洩漏	5
8.24 委外開發之系統上線前，是否偵測有無惡意程式存在？	8.23 委外開發之系統上線前是否偵測有無惡意程式？	文字措詞修訂		A.12.5.5			委外軟體開發	6
8.25 委外開發合約中，是否規範著作權之歸屬？	8.25 委外開發合約中是否規範著作權之歸屬？	文字措詞修訂						
8.26 訂約時，是否簽訂安全履行條款與相關罰則？	8.26 訂約時是否簽訂安全履行條款與相關罰則？	文字措詞修訂						
				A.12.6		技術脆弱性管理 目標： 降低利用已公佈技術弱點所導致的風險。		
8.27 是否及時取得使用中通訊傳播系統之技術脆弱性資訊，並定期執行各項系統漏洞修補程式？	8.27 是否定期執行各項系統漏洞修補程式？	文字措詞修訂		A.12.6.1			技術脆弱性控制	10
8.28 進行系統修補前，是否先作系統影響評估與測試，再採取必要措施？	8.28 進行系統修補前是否先作系統影響評估與測試，如風險評估後，再採取必要措施？	文字措詞修訂						
9.資訊安全事故管理				A.13	資訊安全事故管理			
				A.13.1		通報資訊安全之事件及弱點 目標： 確保與資訊系統相關的資訊安全事件及弱點，能夠及時傳達並矯正。		

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
9.1 是否建立資安事故（含安全漏洞、系統弱點、病毒、非法入侵及系統異常）之正式通報應變程序？	9.1 是否建立資安事故（含安全漏洞、系統弱點、病毒、非法入侵及系統異常）之正式的事故通報與提報程序？	文字措詞修訂	◎	A.13.1.1			通報資訊安全事件	4
9.2 事故回應小組是否建立單一聯繫窗口，授權在處理事故時採取立即之決定，並與外部團體（例如：執法機關、政府緊急應變中心、客戶、商業夥伴）建立聯繫管道？	9.2 是否訂有資訊安全事故建立通報程序，並於事故回應小組中建立單一聯繫窗口以評估、回應與從事故中學習？事故回應小組是否被授權在處理事故時採取立即之決定？事故回應小組應與外部團體（例如：執法機關、政府緊急應變中心、客戶、商業夥伴）建立一定之聯繫管道。	文字措詞修訂	◎					
9.3 資訊安全事故處理過程，是否留有完整記錄，如有必要，應經由直接發送電子郵件及/或網站首頁，及時回報事故給相關客戶？	9.3 資訊安全事故處理的過程是否均留有完整記錄？如有必要，應經由直接發送的電子郵件及/或網站首頁及時回報事故予相關客戶。	文字措詞修訂	◎					
9.4 是否建立資訊安全事故通報之聯絡點，並確保全組織都知道該聯絡點，隨時可聯繫，能夠有充分與及時的回應？	9.4 是否建立資訊安全事故通報的聯絡點，確保全組織都知道該聯絡點，隨時可聯繫，並能夠有充分與及時的回應？	文字措詞修訂	◎					
9.5 機關員工及外部使用者是否知悉資安事故通報及處理程序並依規定辦理?	9.5 機關員工及外部使用者是否知悉資安事故通報及處理程序並依規定辦理?		◎	A.13.1.2			通報安全弱點	1
9.6 是否要求資訊系統與服務的所有員工、承包商及第三方使用者，注意並通報任何觀察到或可疑的系統或服務之安全弱點？	9.6 是否要求資訊系統與服務的所有員工、承包商及第三方使用者，注意並通報系統或服務之任何觀察到或可疑的安全弱點？	文字措詞修訂	◎					
				A.13.2		資訊安全事故之管理及改進 目標： 確保資訊安全事故的管理採用一致及有效的作法。		
9.7 是否依不同型式之資訊安全事故，建立資安事故管理責任及應變程序？	9.7 是否依不同型式的資訊安全事故，建立資安事故管理責任及應變程序？	文字措詞修訂	◎	A.13.2.1			責任與程序	4
刪除	9.12 是否建立資安事故之通報及事故回應與提報處理程序的管理責任與職掌定義？	本項與9.7內容雷同，建議刪除。						
9.8 是否建立資安事件或事故等事後管理會議，以協助單位能從資安事件及事故中學習？	9.13 是否建立資安事故或事故等事後管理會議，以協助單位能從資安事故、事故中學習？	文字措詞修訂	◎					
9.9 是否擬定營運中斷後之各項風險處理優先順序或處理準則（含處理順序說明、最低營運水準定義）？	9.14 是否擬定營運中斷後之各風險之處理優先順序或處理準則（含處理順序說明、最低營運水準定義）？	文字措詞修訂	◎					
9.10 是否建立資安事故管理機制，如記錄事故型式、處理方法、處理成本及矯正預防措施？	9.8 是否建立資安事故管理機制，如記錄事故型式、處理方法、處理成本及矯正預防措施？		◎	A.13.2.2			從資訊安全事故中學習	1
9.11 是否已建立及使用各項指標，以協助偵測安全事故，並預防安全事故？	9.9 是否已建立及使用各項指標，以協助偵測安全事故，並預防安全事故？		◎					

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
9.12 已發生之資訊安全事故，是否在安全政策審查過程中納入考量？	9.10 已發生之資訊安全事故是否在安全政策審查過程中納入考量？	文字措詞修訂	◎					
9.13 資安事故中相關證據資料是否有適當保護措施，以符合證據能力之要求，作爲問題分析及法律必要依據？	9.11 資安事故中相關證據資料是否有適當保護措施?以作爲問題分析及法律必要依據。	文字措詞修訂		A.13.2.3			證據的收集	4
10.營運持續管理				A.14	營運持續管理			
				A.14.1		營運持續管理之資訊安全觀點 目標： 爲防範營運活動中斷，保護重要營運過程不受重大資訊系統失效或災害的影響，並確保及時重新開始(resumption)。		
10.1 是否發展與實作營運持續計畫，以因應組織營運持續所需的資訊安全要求？	10.1 是否發展與實作營運持續計畫，以確保能及時再續必要的運作？	參考CNS/ISO/IEC 27002 14.1.1條文內容修訂。		A.14.1.1			資訊安全納入營運持續管理過程	10
10.2 是否針對所有營運過程，可能造成營運中斷之機率及衝擊進行風險評鑑？	10.2 是否針對所有的營運過程，對可能造成營運中斷之機率及衝擊進行風險評鑑？	文字措詞修訂						

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
刪除	10.3 是否識別關鍵營運過程及排定優先順序？	本項內容與10.2雷同，建議刪除。		A.14.1.2			營運持續與風險評鑑	1
10.3 是否識別營運持續過程中之關鍵資通訊設備及資訊處理設施？	10.4 是否識別營運持續過程中之關鍵重信設備與資訊設施?	文字措詞修訂						
10.4 營運持續計畫是否以人員安全爲優先，並保護資通訊設備和組織財產？	10.5 營運持續計畫是否以人員安全爲優先，並保護資訊處理設施和組織財產？	文字措詞修訂		A.14.1.3			發展與實作包括資訊安全的持續計畫	7
刪除	10.6 營運持續計畫是否符合風險評鑑結果？	本項內容與10.2雷同，建議刪除。						
10.5 是否訂定營運持續計畫（含啓動條件、參與人員、緊急程序、後撤程序、回復程序、維護時程、教育訓練、職責說明、所須資源、往來單位之應變規劃及合約適當性等）？	10.7 是否擬訂營運持續管理計畫（含啓動條件、參與人員、緊急程序、後撤程序、回復程序、維護時程、教育訓練、職責說明、所須資源、往來單位之應變規劃及合約適當性等）？	文字措詞修訂						
10.6 是否維持營運持續計畫之單一框架， 以確保所有計畫有一致性， 持續一致地因應資訊安全要求， 並識別測試與維護的優先順序？		參考CNS/ISO/IEC 27002 14.1.4條文內容，建議新增。		A.14.1.4			營運持續計畫框架	9
刪除	10.8 是否制訂資訊安全緊急應變處理程序？有否定期演練及測試？	本項與10.10點內容雷同，建議刪除。		A.14.1.5			營運持續計畫的測試、維護及重新評鑑	6
10.7 營運持續計畫（含緊急應變處理程序）是否配合業務、組織及人員之變更而更新？	10.9 營運持續計畫（含緊急應變處理程序）是否配合業務、組織及人員之變更而更新？							
10.8 營運持續計畫是否定期完整測試、演練並予更新維護?	10.10 營運持續計畫是否定期完整測試、演練並予更新維護?							
11.遵循性				A.15	遵循性			
				A.15.1		符合法規要求 目標： 避免違反任何法律、法規命令、行政規則或契約義務及任何安全要求。		
11.1 是否確保所有通訊系統與組織均不違反任何法律、法規命令、行政規則、契約義務及相關安全要求？	11.1 是否確保所有資訊系統與組織均不違反任何法律、法令、法規或契約義務，以及任何安全要求？	文字措詞修訂		A.15.1.1			識別適用之法條	1
11.2 軟體取得（含自行開發、委外開發、購置或租用）等可能涉及智慧財產權規定，是否符合法律、法規命令及契約的要求？	11.1 軟體取得（含自行開發、委外開發、購置或租用）等可能涉及智慧財產權規定或合約要求是否可遵循法律、法規及契約的要求？	序號與前條重複，文字措詞修訂		A.15.1.2			智慧財產權	13
11.3 是否公布智慧財產權遵循政策，定義軟體與資訊產品的合法使用，並告知違反政策人員將遭懲處？	11.2 是否公布智慧財產權遵循政策，定義軟體與資訊產品的合法使用，並通知違反政策人員將遭懲處？	文字措詞修訂						

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
11.4 是否維護使用版權、原版碟片、手冊等所有權之證明和證據，並定期檢核是否只安裝經授權之軟體與有使用版權之產品？	11.3 是否維護使用版權、原版碟片、手冊等所有權的證明和證據，並定期檢核是否只安裝經授權軟體與有使用版權的產品？	文字措詞修訂						
11.5 組織重要紀錄（如資料庫紀錄、系統日誌、操作日誌、稽核日誌）是否依安全等級加以保護及儲存（如檔案加密或數位簽章）？	11.4 組織重要紀錄（如資料庫紀錄、系統日誌、操作日誌、稽核日誌）是否依安全等級加以保護儲存（如檔案加密或數位簽章）？	文字措詞修訂		A.15.1.3			組織紀錄的保護	4
11.6 稽核後是否產生稽核報告，並追踪改善情形（包括稽核發現之摘要、稽核區域、缺失說明及改進建議等）？	11.10 稽核後是否產生稽核報告並追踪改善情形（包括稽核發現的摘要、稽核區域、缺失說明及改進建議等）？	文字措詞修訂						
11.7 組織中對於所經管或處理之資訊，涉及個人隱私及個人資料之保護是否有適當之保護機制？	11.5 組織中對於所經管或處理之資訊，涉有個人隱私及個人資料之保護是否有妥適之保護機制？	文字措詞修訂		A.15.1.4			個人資訊的資料保護與隱私	1
11.8 是否發展和實作符合法律、法規及若適用的契約條文所要求的資料保護與隱私政策？	11.6 是否發展和實作符合法律、法規及若適用的契約條文所要求的資料保護與隱私政策？							
11.9 是否依據個人資料保護法擬定個人資料檔案安全維護計畫及業務終止個人資料處理方法？	11.8 是否指派專人負責有關個人資料保護法規之蒐集、公告、實施作爲？	依據個人資料保護法規定修訂						
11.10 是否有監視設備或其他可偵測未經授權使用之設備，防止資訊設施被不當使用？	11.7 是否有監視設備或其他可偵測未經授權使用的設備，以防止資訊設施被不當使用？	文字措詞修訂		A.15.1.5			防止資訊處理設施的誤用	1
11.11 管理人員是否定期審查其責任範圍內之資訊處理設施與其安全政策、標準及符合其他相關安全要求？	11.9 管理人員是否定期審查其責任範圍內的資訊處理設施與其安全政策、標準及其他任何安全要求的遵循性？	文字措詞修訂						
				A.15.1.6			密碼控制措施的規定	4
				A.15.1.7			Non-disclosure of communications	10
				A.15.1.8			Essential communications	18
				A.15.1.9			Legality of emergency actions	1
				A.15.2		符合安全政策、標準及技術規範 目標： 確保系統符合組織的安全政策及標準。		
11.12 組織訂定之安全程序，是否確保相關人員能正確執行？	11.11 組織所訂所有安全程序，是否確保相關人員能正確執行？	文字措詞修訂		A.15.2.1			安全政策與標準的符合	4
11.13 資訊系統是否定期進行安全技術符合性檢查（如滲透測試或系統弱點檢測）？	11.12 資訊系統是否定期進行安全技術符合性的檢查（如滲透測試或系統弱點檢測）？	文字措詞修訂						
11.14 技術遵循性之查核人員是否經過訓練，並作事前工作分配？	11.13 技術的遵循性查核人員是否經過訓練，並作事前工作分配？	文字措詞修訂						

附件6　通訊傳播事業資通安全管理內部稽核表(修訂對照)

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	資安管理內部稽核表 (檢查項目)	修訂說明	最小限安全控制措施 (C級)	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
11.15 技術遵循性檢查是否由合格資安技術單位執行？	11.14 技術遵循性檢查是否由合格資安技術單位執行？			A.15.2.2			技術符合之查核	1
11.16 技術遵循性查核時之存取行爲，是否作監控，並適當保存紀錄？	11.18 技術遵循性查核時的存取行爲是否作監控與並適當保存紀錄？	文字措詞修訂						
11.17 技術遵循性查核結果是否文件化？	11.19 技術遵循性查核結果是否文件化？							
				A.15.3		資訊系統稽核考量目標： 使資訊系統稽核處理的有效性最大化，並使其產生或受到之干擾最小化。		
11.18 是否訂定資訊安全內部稽核計畫（含稽核目標、範圍、時間、程序、人員）？	11.17 是否訂有資訊安全內部稽核計畫（含稽核目標、範圍、時間、程序、人員）？	文字措詞修訂		A.15.3.1			資訊系統稽核控制	9
11.19 是否定期辦理資訊安全內部稽核？	11.15 是否定期辦理資訊安全內部稽核？							
11.20 內部稽核範圍是否含括資通系統、供應商、資產負責人、使用者和管理階層？	11.16 內部稽核範圍是否涵括資訊系統、供應商、資訊資產負責人、使用者和管理階層？	文字措詞修訂						
11.21 是否有保護資訊系統稽核工具之存取，防止可能誤用或破解之措施？		參考CNS/ISO/IEC 27002 15.3.2 條文內容，建議新增。		A.15.3.2			資訊系統稽核工具的保護	1
277	289		49	合計	11	40	146	803
圖例：	安全領域	安全目標	控制措施/ 實作指引	27011新增 控制措施	27011 補充措施	未納入 控制措施		

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
1.資訊安全政策				A.5	安全政策			
				A.5.1		資訊安全政策 目標： 依據營運要求及相關法律與法規，管理階層提供資訊安全之指示與支持。		
1.1 是否依據相關法律、法規及營運要求，訂定組織資訊安全政策？				A.5.1.1			資訊安全政策之文件	6
1.2 是否考量組織之整體業務活動及其相關風險，訂定資訊安全政策？								
1.3 是否識別違反資訊安全政策之後果及訂定處理程序？								
1.4 是否由管理階層核准資訊安全政策文件，正式發布且轉知所有員工與各相關外部團體？								
1.5 資訊安全政策文件是否包括資訊安全之定義、整體目標、範圍、實施內容、執行組織、權責分工、員工責任、事故通報處理流程？								
1.6 是否依據資訊安全政策，訂定原則、標準及對組織特別重要之法規要求說明文件及資料（如法律、法規命令、行政規則、契約、安全教育、訓練、認知、營運持續管理、作業程序、資訊安全控管文件、使用者應遵守的安全規則）？								
1.7 資訊安全政策是否就一般和特定責任之權責（包括通報資訊安全事故）加以定義？。								
1.8 是否對支援資訊安全政策的文件建立補述文件？例如：針對特定資訊系統的更詳盡安全政策和程序，或使用者宜遵守的安全規則。								
1.9 資訊安全政策是否由具有發展、審查及評估等核准權限之管理者，依規劃期間或有重大變更時，作必要之審查及調整？				A.5.1.2			資訊安全政策之審查	12
1.10 是否妥善維護資訊安全管理政策之審查紀錄與訂定管理審查程序，包括審查時程及週期?								
1.11 是否定期對組織人員及資訊設備進行安全評估，以確定其遵守資訊安全政策及相關規定？								
1.12 是否指定專人或專責部門進行資訊安全政策的維護及檢討？								

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
2.資訊安全之組織				A.6	資訊安全之組織			
				A.6.1		內部組織 目標：管理組織內之資訊安全。		
2.1管理階層是否在組織內藉由清楚的指示、明確的指派及確認資訊安全責任， 主動地展現承諾以支持安全？				A.6.1.1			管理階層對資訊安全之承諾	8
2.2 是否指派擁有權責之管理階層或成立跨部門組織負責推動、協調及監督資訊安全管理事項？				A.6.1.2			資訊安全協調~~工作~~	7
2.3 是否指定專人或專責部門，負責辦理下列資訊安全管理工作事項(1)資安政策、計畫、措施之研議，(2)風險評鑑、資訊分類、系統安全控管措施，(3)資料及資訊系統之使用管理及保護，(4)資安認知訓練及資安稽核？								
刪除與2.3點內容合併								
2.4 資訊安全責任的配置是否依據資訊安全政策，並明確地識別需保護之個別資產與執行特定安全~~作業~~過程的責任，並加以文件化？				A.6.1.3			資訊安全責任之配置	3
2.5 是否依據員工之職務~~內容~~，訂定員工資訊安全作業程序、權責規範或授權層級並予以文件化？（含經管使用設備及作業須知）				A.6.1.4			資訊處理設施之授權過程	3
2.6 是否訂定各項資訊處理設施之用途及使用授權，及~~其~~安全之作業程序？								
刪除								
2.7 是否識別並定期審查組織對於資訊保護之機密性或保密協議之要求？	1.1通訊事業對保密協議之內容，是否包含：對於通訊之有無、對象、時間及內容等，以確保不得有不當揭露之情事發生？ (註：僅適用於電信事業)	1.1 是否訂定並定期審視保密及防止不當揭露組織需保護資訊之機密性協議（例如通訊資訊中的實體、內容、來源、目的地、日期時間）？	文字措詞修訂	A.6.1.5			機密性協議	10
2.8 是否訂定當發生資安事故時，如何及時與主管機關聯繫並通報之適當程序或規定？	1.2 組織是否訂定執法機關或研究機構請求提供資訊時之控管程序，確認此申請係符合法規命令之合法程序？	1.2 組織提供執法機關所請求之資訊時，是否訂定控管程序以確認此申請依據國家法規之合法過程與程序？	文字措詞修訂	A.6.1.6			與權責機關之聯繫	2
2.9 是否~~訂定~~與各特殊利益團體、專家安全論壇及專業協會維持適當聯繫？				A.6.1.7			與特殊利益團體之聯繫	6

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
2.10 獨立審查組織對資訊安全管理之作法與其實作（例如：各項資訊安全的控制目標、控制措施、政策、過程及程序），是否定期召開管理審查會議？當資安作業環境發生重大變更時，亦依上述作法與實作，召開管理審查會議？				A.6.1.8			資訊安全之獨立審查	1
				A.6.2		外部團體 目標： 維持外部團體存取、處理、通信或管理之組織資訊及資訊處理設施之安全。		
2.11 因營運需要開放給外部團體（含其他機關、往來業者、維護廠商、委外承包商、聘僱人員及一般民眾）使用之資訊，是否執行風險評鑑與實作安全控制措施？並於契約或規定中包含雙方權利、義務、資料保護、資訊保密、服務標的水準、智慧財產權、事故發生處理與違約處理等條款？				A.6.2.1			識別與外部團體相關之風險	19
2.12 是否對不開放外部團體存取的資訊進行必要的控制措施？								
2.13 因營運需要開放給外部組織或人員存取之資訊，其存取權限是否定期審查？								
2.14 因營運需要開放給外部團體（含其他機關、往來業者、維護廠商、委外承包商、聘僱人員及一般民眾等）使用之資訊，於開放使用之前，是否闡明所有已識別之安全要求？	1.3 提供客戶服務前，是否訂定清楚之協議內容，要求不得毀損或減低通訊服務之能力？		參考ISO/IEC 27011 6.2.2內容增訂	A.6.2.2			處理客戶事務之安全說明	11

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
2.15 委外契約中有關安全需求內容，是否包含法律要求（如個人資料保護法）、雙方有關人員權責、安全控管措施、作業程序、事故通報程序、服務水準、對委外廠商稽核權等資訊安全責任與事宜，並得依實際需要適時修改安全控管措施及作業程序等？	1.4 提供第三方服務廠商存取權限之前，是否訂定清楚之協議內容，包含提供服務所需之相關安全政策與應注意事項，並確保沒有誤解之情形存在？		參考ISO/IEC 27011 6.2.3內容增訂	A.6.2.3			第三方協議中之安全說明	22

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
3.資產管理				A.7	資產管理			
				A.7.1		資產責任 目標： 達成及維持組織資產之適切保護。		
3.1 是否明確識別所有資產，並製作與維持所有重要資產的清冊？	2.1 是否明確定義組織的電信機線設備，與其他組織相連結或相關之部份的管理責任，並加以文件化？	2.1 是否明確界定組織的電信設施與其他組織相連結或相關之部份的管理責任，並具體和明確的文件化？	文字措詞修訂	A.7.1.1			資產清冊	6
3.2 是否有明確之定義，如何分辨何種資產是重要資產，再依據該定義作資產盤點，並建立與維護重要資產清冊？								
3.3 現有之重要資產清冊是否包含災難回復所需之資訊，如：資產型態/格式/位置/備份資訊/使用版本/業務價值？								
3.4 資產清冊是否定期審查，確保資產處於適切狀態？								
3.5 是否識別所有資訊資產之擁有者，並指派其依適切控制措施維護資訊資產之責任？				A.7.1.2			資產之擁有權	2
3.6 是否識別及實作所有與資訊處理設施相關（含電子郵件、網路使用及行動設備等）之使用規則，並加以文件化？				A.7.1.3			資產可被接受之使用	2
				A.7.2		資訊分類 目標： 確保資訊得到適切之保護等級。		
3.7 是否依據資訊對於組織的價值、法律要求、敏感性及重要性加以分類？	2.2 除一般、敏感及關鍵資訊之分類外，通訊事業是否對於通訊之有無、對象、時間及內容等，加以標示，並確保資訊存取之可歸責性？(註：僅適用於電信事業)		參考ISO/IEC 27011 7.2.1內容增訂	A.7.2.1			分類指導綱要	1
3.8 是否依據組織採用的分類法，訂定適當之資訊標示與處理程序？				A.7.2.2			資訊標示與處理	1

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
3.9 是否對於機密性資訊、敏感性之手稿資訊、影印公文之廢紙及已過保存期限之公文，於棄置前予以銷毀？								
刪除								

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
4.人力資源安全				A.8	人力資源安全			
				A.8.1		聘僱前 目標： 確保員工、承包商及第三方使用者瞭解其責任， 並勝任其所被賦予的角色，以降低竊盜、詐欺或設施誤用的風險。		
4.1 是否依照組織的資訊安全政策，訂定正式文件，規範所有員工、承包商或第三方使用者之安全角色與責任？	3.1 是否詳細檢查員工、承包商及第三方使用者職務上被授權能夠存取之必要服務：如：客戶個人資料或客戶通話內容等，並納入相關安全責任之中？	3.1 是否詳細檢查職務上能夠授權存取之必要服務：例如：客戶個人資料或是客戶通話內容等，並納入相關安全責任之中？	文字措詞修訂	A.8.1.1			角色與責任	5
	3.2 對於人員進用，是否考量相關電信證照或具備適當的電信知識和技能？	3.2 對於人員進用，是否考量相關電信證照或具備適當的電信知識和技能？	文字措詞修訂					
4.2 是否明確定義所有聘僱之應徵者、承包商及第三方使用者背景查證檢核之限制與程序，確保符合隱私權、個人資料保護及/或聘僱勞工保護相關法令之要求？	3.3 對所有聘僱之應徵者、承包商及第三方使用者的之進用或委派，是否作適當之背景查驗工作，例如：工作職務涉及客戶個人資料或是通訊內容之存取者？	3.3 對所有聘僱之應徵者、承包者及第三方使用者的之進用或委派，是否作適當之背景查驗工作，例如：工作職務涉及客戶個人資料或是通訊內容之存取者？	文字措詞修訂	A.8.1.2			篩選	5
4.3 被賦予機敏資訊存取權的所有員工、承包商及第三方使用者，是否在被允許存取資訊處理設施之前，簽署適當之機密性或保密協議？	3.4 聘請第三方機構前，是否明確定義和溝通其安全角色和職責？	3.4 聘請第三方機構之前，是否明確界定和溝通其安全角色和職責？		A.8.1.3			聘僱任期與條件	7
	3.5 對於委外承包商或第三方使用者，是否在合約中加入安全角色與職責的要求？	3.5 對於委外承包商或是第三方使用者，是否在合約中加入安全角色與職責的要						
	3.6是否要求組織內任何人從事電信服務時，應保護職務上所知悉之營業秘密？	3.6 組織內任何人從事電信服務時，是否要求應保護職務上所知悉之營業秘密？	文字措詞修訂					
	3.7 組織是否依據相關法規命令，訂定防止不當揭露之責任？	3.7 組織是否依據相關法規命令，訂定防止不當揭露之責任？						

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.8.2		聘僱期間 目標： 確保員工、承包商及第三方使用者認知資訊安全的威脅與關切事項、其責任與義務， 並有能力在日常工作中支持組織安全政策與降低人爲錯誤的風險。		
刪除				A.8.2.1			管理階層責任	6
刪除								
刪除								
4.4 管理階層是否有要求員工、承包商及第三方使用者，依照組織已訂定的政策與程序執行安全事宜？								
4.5 對所有員工、承包者及第三方使用者工作職務有關之安全程序及資訊處理設施，是否提供正確使用之認知、教育與訓練？				A.8.2.2			資訊安全認知、教育及訓練	1
刪除								
4.6 是否訂定員工違反組織安全政策與程序之懲處規定？				A.8.2.3			懲處過程	1
				A.8.3		聘僱終止或變更目標： 確保員工、承包商及第三方使用者依規定離職或變更聘僱。		
4.7 是否在與員工、承包商或第三方使用者所訂之契約內規定，在聘僱終止後，與職務有關之責任仍然是有效的？				A.8.3.1			終止責任	1

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
4.8 所有員工、承包商及第三方使用者離職或聘雇終止時，是否依規定繳回其任職期間保管之資訊資產？（包含所有的軟體、公司文件、設備、行動裝置、信用卡、存取卡、軟體、手冊及儲存於電子媒體的資訊等所有其他組織資產）				A.8.3.2			資產之歸還	1
4.9 所有員工、承包商及第三方使用者之聘僱、契約或協議終止時，或因變更而調整時，是否對資訊及資訊處理設施之存取權限迅速予以移除？				A.8.3.3			存取權限之移除	3

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
5.實體及環境安全				A.9	實體及環境安全			
				A.9.1		安全區域 目標： 防止組織的場所及資訊遭未經授權的實體存取、損害及干擾。		
5.1 是否適當使用安全邊界（如圍牆、入口閘門或人員駐守的接待櫃檯等屏障），保護含有資訊與資訊處理設施的區域？	刪除	4.1 電信營運中心是否有適當的實體入侵偵測系統？	本項內容與資安管理內部稽核表5.1內容雷同，建議刪除	A.9.1.1			實體安全周界	7
5.2 組織管理之資訊處理設施（如通訊服務設施），在實體上是否與第三方管理（如：客戶代管設備）之資訊處理設施區隔？	4.1 有權責人員是否於安全邊界發生異常狀況時，可立即處理？	4.2 實體邊界發生異常狀況時，是否有權責人員可立即解決？						
刪除	4.2 通訊系統之機房控制中心與操作室是否有適當強度之門禁管制措施（strong entry controls）？	4.3 控制中心與操作室是否有適當強度的進出控制措施（strong entry controls）？		A.9.1.2			實體進入控制措施	5
5.3 具有關鍵或敏感的資訊處理設施之安全區域，是否對於授權進出人員作必要之限制及監督其活動？	刪除	4.4 是否針對訪客的探訪紀錄進行適當保護？（訪客進入及離開時間、訪客身份等。）	本項內容與資安管理內部稽核表5.4內容雷同，建議刪除					
刪除	刪除	4.5 接待人員是否檢查訪客是否攜帶危險物品進入及帶走未經授權的物品？	本項內容與資安管理內部稽核表5.4內容雷同，建議刪除					
5.4 安全區域之進出權限是否定期審查並更新，並於必要時廢止？								
5.5 辦公處所是否實施必要之保護措施？				A.9.1.3			辦公室、房間及設施之保全	4
5.6 是否檢查及評估重要資通訊設備設置地點，鄰近場所之任何安全威脅，如火災、灰塵、水災、震動、化學效應、電力供應、電磁輻射、民間暴動及其他天然或人為災害等可能對設備之危害？				A.9.1.4			防範外部與環境之威脅	3
5.7 是否設計並實施適當的控制措施，以保護敏感資訊處理設施之地點及內部人員通訊錄？								
刪除								

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
5.8 是否嚴禁在電腦機房內使用未經核准之電器或其他物品？				A.9.1.5			在安全區域內工作	4
5.9 備援設備及備份媒體存放位置，是否與主要場地保持安全距離？								
5.10 安全區域是否與易燃物或危險物料保持安全距離，並不宜儲存大量的物資？								
5.11 是否設計並實施適當之控制措施，監督安全區域內之工作，並確保其需知原則？								
5.12 是否訂定未經授權前，禁止拍照、錄影、錄音和其他記錄性設備之規定，如行動裝置上的照相機？								
5.13 無人使用之安全區域是否上鎖並定期檢查？								
5.14 對於收發、裝卸區及其他未經授權人員可進入之作業場所，是否有適當之進出控制措施，並應與資訊處理設施隔離，以避免未經授權的存取？				A.9.1.6			公共進出、收發及裝卸區	6
	4.3 電信事業維運中心是否設置於適當地點（如避免易遭水災、風災、地震影響，或臨近強烈電磁及儲存危險物之場所）？	4.6 通信中心（communication centers）是否選擇在適當地點?（避免選擇在易受水災、風災影響，與臨近強烈電磁及儲存危險物的場所）	文字措詞修訂	A.9.1.7			維運中心之安全 Securing communication centres	8
	4.4 電信事業維運中心是否裝設自動火災警報系統？	4.7 通信中心是否裝設自動火災警報系統？	文字措詞修訂 本項內容與資安管理內部稽核表5.8內容雷同，建議5.8條刪除					
	4.5 電信事業維運中心是否爲抗震建物？樓層地板是否有足夠之承載能力？	4.8 通信中心是否爲抗震建物？樓層地板是否有足夠的承載能力？	文字措詞修訂					
	4.6 電信事業維運中心是否依據消防法規，使用防火建材？	4.9 通信中心是否盡可能使用防火建材？	文字措詞修訂					
	刪除	4.10 通信中心之設計是否盡可能避免火災蔓延？	本項內容與4.9條內容雷同，建議刪除					
	4.7 通訊設備機房，是否選擇於適當地點，具備防範風災、水災、地震及火災之能力，並配備適當之偵測設備，防止未經授權之入侵？	4.11 電信設備機房（telecommunications equipment room）或實體隔離的操作區（如：行動通信基地臺mobile base station）是否有足夠的安全防護？	文字措詞修訂	A.9.1.8			設備機房之安全 Securing telecommunications equipment room	15

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
	4.8 無人看管之隔離操作區，如：行動電話中繼臺，是否具備以下安全措施： (1)自動消防設備、(2)遠端監控及自動告警系統，包含設備失效、電力失效、火警及溫濕度監控、(3)適當之實體安全維護設施等？		本項內容參考ISO/IEC 27011 9.1.9條文內容，建議增訂。	A.9.1.9			隔離操作區之實體安全 Securing physically isolated operation areas	4
				A.9.2		設備安全 目標： 防止資產的遺失、損害、遭竊或洩漏及組織活動的中斷。		
5.15 是否明確訂定資通訊設備之控制措施（包括場外使用之設備，及財產之攜出），以降低資料未經授權存取、遺失及損壞之風險？				A.9.2.1			設備安置與保護	9
5.16 處理敏感資料的資通訊設備或資訊處理設施是否予特別保護並評估其有效性？	4.9 不同客戶之代管設備是否加以分隔，並實施適當保護措施？	4.12 不同客戶之代管設備是否實體分隔，並實行適當之保護措施？						
5.17 是否採取適當控制措施，降低潛在實體威脅，如：竊盜、火災、爆裂物、煙害、水災（或水源供應停止）、閃電、溫度、濕度、灰塵、振動、化學效應、電力供應干擾、通信干擾、電磁輻射及蓄意破壞等？								
5.18 電腦作業區（含機房）是否落實執行禁止抽煙及飲食？								
5.19 是否具備環境監控機制，掌握資通訊設備及資訊處理設施之溫度及溼度狀況？								
5.20 是否對於支援性公共設施，如電源供應、水源供應、污水處理、暖氣/通風及空調，設計適當之保護措施，並施行之，確保不受公共設施失效所導致之中斷？	4.10 關鍵設施是否有不斷電系統或是足夠之備援電力保護？	4.13 關鍵設施是否有不斷電系統以及足夠電力保護？	文字措詞修訂	A.9.2.2			支援設施	1
5.21 備援電源是否定期檢查並測試，確保能在斷電期間正常運作？								
5.22 電信機線設備（telecommunications lines）、網路佈纜（network cabling）及電源纜線，是否設計適當之安全保護措施，並施行之？				A.9.2.3			佈纜的安全	6
5.23 通信纜線（communications cables）及電源纜線是否接地並隔離，防止互相干擾？								

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
5.24 設備是否定期且正確的維護保養，確保其可用性及完整性？				A.9.2.4			設備維護	5
5.25 各項設備是否依據供應商建議的間隔與保養手冊，定期檢查並維護？								
5.26 設備之維護與修理，是否由授權之維護人員執行？								
5.27 是否妥適保存所有可疑、實際之系統錯誤資訊，及所有預防性、矯正性之維護紀錄？								
5.28 設備送場外維修，對於儲存在設備內資訊是否訂有安全保護措施？								
5.29 攜出場所外之設備和媒體，是否訂有安全保護措施？				A.9.2.5			場所外設備之安全	4
5.30 行動裝置（設備）是否訂有嚴謹保護措施（如使用授權管理、設通行碼、檔案加密、專人看管）？								
5.31 設備汰除前，是否將機密性、敏感性資料及有版權的軟體予以移除或實施安全覆寫？				A.9.2.6			設備汰除或再使用之安全	1
5.32 含有敏感性資訊之設備汰除後，是否根據風險評鑑決定實體銷毀與否？								
5.33 資訊資產如須攜出場外使用，是否經事前授權，並於攜出場外與歸還時，進行安全查核及紀錄？				A.9.2.7			財產的攜出	4
				A.9.3		其他團體之安全管控 Security under the control of other party		
	4.11 通訊系統放置於其他組織處之設備，是否有足夠安全防護，且有定義清楚的邊界與介面，可以輕易加以隔離？	4.14 電信事業放置於其它場所的設備是否有足夠的安全防護，？	文字措詞修訂	A.9.3.1			位於其他服務供應商處之設備 Equipment sited in other carrier's premises	3
	4.12 放置於使用者端設備，是否具備遠端監控功能，必要時，可以輕易加以隔離？		本項內容參考ISO/IEC 27011 9.3.2條文內容，建議增訂。	A.9.3.2			位於使用者端之設備 Equipment sited in user premises	3
	4.13 是否持續監控與其它通信服務互連狀態，並有適當之控制措施，檢查與其它通訊服務互連是否正常？發生問題時，是否有方法可以矯正？	4.15 是否持續監控與其它通信服務互連的狀態？是否有適當的控制措施檢查與其它通訊服務互連是否正常？發生問題時，是否有方法可以檢查？	文字措詞修訂	A.9.3.3			互連之通訊服務 Interconnected telecommunications	1

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
	4.14 其它通信服務之互連是否已妥善定義邊界與介面？是否已定義用戶發生斷線時，如何處理之協議或合約？	4.16 其它通信服務互連是否已妥善定義範圍與介面？是否已定義一旦用戶發生斷線時如何處置的協議或合約？	文字措詞修訂				services	
6.通訊及作業管理				A.10	通訊及作業管理			

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.10.1		作業程序與責任目標： 確保正確與安全地操作資訊處理設施。		
6.1 資訊處理設施與資通訊設備相關之各項作業程序及活動是否文件化、並適當維護？如電腦開機與關機程序、備份、設備維護、資訊的處理與處理、異常情況之處理、緊急聯絡資訊、重新啓動及復原程序、稽核存底與日誌資訊之維護、電腦機房與郵件處理管理，以及生命財產安全（safey）等。	5.1 通訊系統操作程序是否包含事故、緊急或危機處理程序？	5.1 是否具體定義啓動災害情況、緊急情況或危機之處理程序的條件？	文字措詞修訂	A.10.1.1			作業程序文件化	8
6.2 資訊處理設施與資通訊設備之變更，是否有正式核准之程序，並向相關人員通報變更細節？	5.2 是否建立資訊處理設施與資通訊設備變更之管理程序？管理程序之紀錄是否包括設施之安裝、更改位置及移除？	5.2 是否建立資訊處理設施與系統變更之管理程序？管理程序之紀錄是否包括設施之安裝、改位置及移除？	文字措詞修訂	A.10.1.2			變更管理	6
6.3 資訊處理設施與資通訊設備之變更，是否詳實紀錄，並重新進行風險評鑑？								
6.4 資訊處理設施與資通訊設備之變更，是否備有後撤(fallback)程序，包括不成功的變更、意外事故的中止及復原之程序與責任？								
6.5 對於安全要求較高的業務，是否區隔其職務與責任領域？				A.10.1.3			職務的區隔	1
6.6 業務資訊資產之使用、資料建檔、系統操作、網路管理、行政管理、系統發展維護、變更管理、安全管理等工作，是否授權由不同的人員執行？								
6.7 是否分隔開發、測試及運作之設施、系統、軟體？	5.3 系統開發、測試及正式運作，是否區隔在不同的作業環境處理？	5.3 系統開發、測試及正式運作是否盡可能區隔在不同的作業環境處理？	文字措詞修訂	A.10.1.4			開發、測試及運作設施的分隔	6
6.8 運作測試系統是否使用不同的使用者剖繪（profile），且功能選單需顯示適切的識別訊息，降低錯誤之風險？	5.4 如採用敏感資訊進行測試，是否採取適當措施，避免程序或程式錯誤，導致不可預期之洩漏？	5.4 是否避免以真實之資訊進行系統開發與測試？	文字措詞修訂					

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.10.2		第三方服務交付管理 目標： 執行與維持適切之資訊安全等級服務交付，並與第三方服務交付協議一致。		
6.9 是否與第三方服務交付廠商簽訂適當之資訊安全協定，並納入契約條款，包含安全控制措施、服務定義及交付等級，並賦予相關安全管理責任？				A.10.2.1			服務交付	1
6.10 是否規劃必要轉換（資訊、資訊處理設施及其他任何需要移動者）之安全控制措施，並確保轉換期間安全的維護？								
6.11 是否定期對第三方所提供之服務、報告及紀錄等進行適當之監視與審查，並定期執行稽核？				A.10.2.2			第三方服務的監視與審查	5
6.12 第三方提供之服務如有任何異動時，是否重新進行風險評鑑？				A.10.2.3			第三方服務變更之管理	2
				A.10.3		系統規劃與驗收 目標： 使系統失效的風險最小化。		
6.13 資訊處理設施及資通訊設備設置前，是否進行容量規劃及預留安全容量，並於正式運作時，持續監控其容量狀態？				A.10.3.1			容量管理	1
6.14 是否建立新資訊系統、系統升級或新版本之驗收準則，在新資訊系統、系統升級及新版本正式驗收後，才可移轉上線？				A.10.3.2			系統驗收	10
				A.10.4		防範惡意碼與行動碼 目標： 保護軟體及資訊的完整性。		

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
6.15 是否全面使用防毒軟體，並即時更新病毒掃描引擎及病毒碼？				A.10.4.1			防範惡意程式的控制措施	8
6.16 電腦系統及資料儲存媒體是否定期進行惡意程式病毒及後門程式掃描？								
6.17 是否訂定正式政策，禁止使用未經授權的軟體？								
6.18 是否對支援重要營運程序之系統軟體與資料，執行定期審查？若出現任何未經核准的檔案或未經授權的增補修補程式，應進行正式調查。								
6.19 是否訂定使用電子郵件附件及下載之檔案前，檢查有無惡意程式軟體（含病毒、木馬或後門等程式）之程序？								
6.20 是否定義處理電腦病毒、木馬等惡意程式之管理程序與責任，並訓練員工如何通報惡意程式攻擊，及復原程序？								
6.21 是否準備遭惡意程式攻擊後復原之營運持續計畫，並包括所有必要之資料與軟體備份及復原準備工作？								
	5.5 安裝可攜碼（mobile code）是否作必要之授權處理或限制使用？是否考慮內嵌可攜碼之中介軟體（middleware）之限制使用？	5.5 行動碼（mobile code）的安裝是否作必要之授權處理或限制使用？內嵌行動碼之中介軟體（middleware）是否有考慮其限制使用？	文字措詞修訂	A.10.4.2			防範行動碼的控制措施	6
				A.10.5		備份 目標： 維持資訊及資訊處理設施的完整性與可用性。		
6.22 重要資訊及軟體是否定期作備份處理，並定義備份資訊之必要等級？				A.10.5.1			資訊備份	8
6.23 備份複本是否定期回復測試，並將回覆程序文件化，確保備份複本之可用性及有效性？								
6.24 重要及機敏資訊之備份程度及頻率，是否反應組織的營運要求？								
6.25 備份資訊是否儲存於遠端地點？距離須足以避免主要場地發生災難時遭波及？								

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
6.26 備份資訊是否給予適切等級之實體與環境保護，並與主要場域使用一致之標準？								
6.27 主要場域採用之控制措施是否延伸至涵蓋備份作業場域？								
6.28 是否定期檢查及測試復原程序，確保有效性，且能夠在復原程序分配之時間內完成復原運作？								
				A.10.6		網路安全管理 目標： 確保網路資訊及支援基礎建設進行保護。		
刪除				A.10.6.1			網路控制措施	5
6.29 是否訂定網路及網路遠端設備之使用權責及程序？								
6.30 是否使用網路安全防禦設備，並適當的隔離外部網際網路與組織內部網路？								
6.31 組織建立之網路控制措施，是否能反應資訊之機密性、完整性與可用性要求？								
6.32 對於機敏性資訊之傳輸過程，是否採取資訊加密等保護措施？								
6.33 是否訂定確保網路服務連線品質及可用性之保護措施，提供最佳服務？	5.6 是否訂定網路服務供應商及使用者之服務協議，內容包含使用範圍、相關權責及程序？	5.6 是否訂定網路服務提供者及使用者之服務及使用範圍、相關權責及程序，並納入服務協議中？在服務提供前公告，並適切的維護與管理通信服務？		A.10.6.2			網路服務的安全	3
6.34 是否定期檢討網路安全控管事項之執行？								
6.35 是否定期檢測網路運作環境之安全漏洞？								
6.36 是否使用適當之網路安全解決方案？如防火牆、入侵偵測系統？防火牆存取政策（security policy）設定是否適當？								
	5.7 是否針對不同營業項目，提供客戶適當之安全水準，且於服務協議中描述提供之安全功能、服務水準及管理需求，並辦理認知活動，提醒客戶防範垃圾郵件、網路犯罪及電腦病毒等危害？		本項內容參考ISO/IEC 27011 10.6.3條文內容，建議增訂	A.10.6.3			電信服務交付之安全管理 Security management of telecommunications services delivery.	10

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
	5.8 是否訂定相關政策，防範垃圾郵件，並建置適切控管措施，建立一個合適的、令人期待的電子郵件通信環境？	5.7 是否訂定相關政策以對應垃圾郵件並建置適切之控管措施？建立一個合適的、令人期待的電子郵件通信環境。	文字措詞修訂	A.10.6.4			垃圾郵件之反應 Response to spam	1
	5.9 是否訂定相關政策，防範阻斷服務（DoS）或分散式阻斷服務（DDoS）攻擊，並建置適切控管措施，建立一個合適的、令人期待的通訊環境？	5.8 是否訂定相關政策以對應阻斷服務（DoS）或分散式阻斷服務攻擊（DDoS）並建置適切之控管措施？建立一個合適的、令人期待的電信環境。	文字措詞修訂	A.10.6.5			DoS/DDoS攻擊之反應 Response to DoS/DDoS attacks	3
	5.10 是否具備經由IP位置、通訊埠與通訊協定等個別過濾通訊或限制通訊頻寬之機制，適當的保護易遭受網路攻擊之網路設施，如伺服器、路由器等？	5.9 是否適當的保護網路設施，例如網路攻擊下的伺服器、路由器等？應具備經由IP位置、通訊埠與通訊協定等個別過濾通訊或限制通訊頻寬的機制。	文字措詞修訂					
	5.11 是否具備偵測偽造來源地址（IP spoofing）之能力？	5.10 是否具備偵測偽造來源地址（IP spoofing）的能力？	文字措詞修訂					
	5.12 是否運用嚴格之密碼控制措施及/或高強度鑑別（strong authentication）功能，防範來源造假（source impersonation）？	5.11 是否運用嚴格的密碼控制措施及/或高強度憑證（strong authentication）的功能以防範來源造假（source impersonation）？	文字措詞修訂					
	5.13 是否事先經由定期收集與量測有關於災難、意外事件、社會現象等導致電信設備失效與網路壅塞之相關資訊，並彙集關鍵知識？	5.12 是否事先經由定期的收集與量測有關於災難、意外事件、社會現象等導致電信設備失效與網路壅塞之相關資訊並彙集關鍵知識？	文字措詞修訂					
	5.14 資通訊設備是否具備偵測網路壅塞及避免網路壅塞時通訊集中之機制？	5.13 通訊設備是否具備偵測網路壅塞並避免網路壅塞時通訊集中之機制？	文字措詞修訂					
	5.15 是否訂定作業程序，預先收集可能造成網路雍塞或是預期事件之資訊？	5.14 是否制訂維運規範以收集可能造成網路雍塞之災難及計畫中事件的資訊？	文字措詞修訂					

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
	5.16 是否建置分散式處理中心，採用輔助設備及適當之組態，提升系統峰值處理能力，防範潛在系統崩潰或是災難之發生？	5.15 是否將暫時的設備總處理能能力經由量測納入改善考量？經由量測以改進潛在之營運中斷與災難時分散式處理中心與支援性設備的建置，並在必要時考量適切的配置變更。	文字措詞修訂					
	5.17 是否能鑑別及給予必要的通訊優先權，協助災難發生後之交通維護、緊急通訊、電力供應或維持社會秩序？	5.16 是否能鑑別並給予必要的通訊優先權以預防或減輕災難時交通維護、通訊、電力供應或維持社會秩序？	文字措詞修訂					
				A.10.7		儲存媒體之處理目標： 防止資產被未經授權的揭露、修改、移除或破壞，及中斷營運活動。		
6.37 是否建立各種可攜式媒體之操作管理程序，防止文件、電腦媒體（例如：磁帶、磁碟）、輸入或輸出資料及系統文件，遭受未經授權的揭露、修改、移除及破壞？				A.10.7.1			可攜式媒體的管理	6
刪除								
6.38 含有敏感性資訊之媒體是否以正式程序加以安全地汰除，例如：焚化或絞碎，或清除資料後由組織內其他應用系統使用？				A.10.7.2			媒體的汰除	5
刪除								
6.39 具機密性或敏感性資訊之媒體是否有安全之保存和報廢程序？								
6.40 機密性、敏感性資訊之儲存或處理是否有安全處理程序及分級標示？				A.10.7.3			資訊處理程序	9
6.41 是否建立資訊的處理及儲存的程序，以保護免於未經授權的揭露或誤用?								

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
6.42 對應用程式、程序、資料結構及授權過程等說明之系統文件，是否有適當的存取保護措施？				A.10.7.4			系統文件之安全	3
				A.10.8		資訊交換 目標： 維護組織內及外部團體交換資訊及軟體的安全。		
刪除				A.10.8.1			資訊交換政策與程序	15
6.43 是否對於所有形式之資訊交換，訂定適當交換政策、程序及控制措施？								
6.44 是否對高度機敏性資訊在傳輸或儲存中使用加密技術？								
6.45 是否訂定組織與任何外部團體間，交換資訊與軟體之協議？				A.10.8.2			交換協議	11
6.46 重要電腦資訊、媒體（含報表）之運送，是否有安全保護措施及完整監控記錄（含收送人、時間及內容）？				A.10.8.3			輸送中的實體媒體	5
6.47 是否訂定適當控制措施，保護含有資訊之媒體，在組織實體邊界外傳送時，不受未經授權的存取、誤用或毀損？								
6.48 採行電子交換之資訊，是否視資訊安全等級，採行識別碼與通行碼管制、電子資訊加密或電子簽章認證等保護措施，確保資訊的機密性、完整性、可用性及符合其他法律要求？				A.10.8.4			電子傳訊	6
6.49 涉及敏感性資訊及機密文件之營運資訊系統，是否提供適當之存取控制與保護？				A.10.8.5			營運資訊系統	10
				A.10.9		電子商務服務 目標： 確保電子商務服務的安全及其安全使用。		
刪除								

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
6.50 是否實施適當控制措施，保護在公眾網路上傳輸且涉及電子商務之資訊，使其不受詐欺行為、契約爭議及未經授權之揭露與修改？				A.10.9.1			電子商務	13
刪除				A.10.9.2			線上交易	6
6.51 線上交易服務，是否訂定適當控制措施，防止下列事項：(1)不完整傳輸、(2)誤選路徑、(3)未經授權之訊息修改、揭露及(4)未經授權的訊息複製或重送(replay)等發生？								
6.52 對外開放供公眾取得之資訊，是否訂定保護措施，確保資訊完整性，防止未經授權之修改？				A.10.9.3			公眾可用的資訊	4
				A.10.10		監控 目標： 偵測未經授權的資訊處理活動。		
6.53 是否依據法律要求，如個資法，實施適當之稽核存錄措施，以紀錄使用者活動、異常及資訊安全事故？	5.18 個人資料檔案之留存期限，是否遵守相關法規命令？	5.17 個人資料之留存時限是否依照權責單位之規定？	文字措詞修訂	A.10.10.1			稽核存錄	12
6.54 是否採用適切的存錄與監控設備，記錄資通訊相關活動？				A.10.10.2			監控系統的使用	5
6.55 是否建立適當之控制措施，監控資訊處理設施之使用，及定期審查？								
6.56 各項日誌是否有適當的保護措施，不受竄改與未經授權之存取，並針對留存之通信資訊設定適當之留存期限（例如：會計、帳務、客訴的處理、防止濫用及執法機關的要求）？				A.10.10.3			日誌資訊的保護	3
6.57 是否定期稽查各項作業日誌？								
6.58 是否適當規劃存錄設施與日誌資訊之儲存媒體容量，避免無法記錄事故或覆蓋以往所記錄事故？								
6.59 作業日誌是否留有管理者與操作者所涉及活動之詳細過程，並定期予以審查？				A.10.10.4			管理者與操作者日誌	4

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
刪除				A.10.10.5			失誤存錄	2
6.60 是否加以存錄由使用者或系統程式所通報之資訊處理或通信系統問題，迅速處理及通報？								
6.61 所有系統鐘訊是否與議定之鐘訊來源校正，以確保時間紀錄正確？				A.10.10.6			鐘訊同步	1
7.存取控制				A.11	存取控制			

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.11.1		存取控制之營運要求目標： 控制資訊的存取。		
7.1 是否根據營運與安全要求，建立、文件化及審查存取控制政策？	6.1 通訊事業是否對於用戶端設備，訂定適切之存取控制規則（例如：控制的要求應基於資訊擁有者而非設備擁有者；採原則禁止、例外開放之規則）？	6.1 對於用戶端設備，電信事業是否策定適切的存取控制規則（例如：控制的要求應基於資訊擁有者而非設備擁有者；採原則禁止、例外開放之規則）？	文字措詞修訂	A.11.1.1			存取控制政策	16
7.2是否在存取政策文件中明確陳述每個使用者或使用群組之存取控制規則與權限？	刪除	6.2 是否將網路運作及電腦運作之使用權責予以區隔？	本項內容參考ISO/IEC 27011 11.1.1條文內容，建議刪除					
7.3 資訊存取控制政策是否符合相關法律、法規命令及契約規定，如電信法、個資法等？								
				A.11.2		使用者存取管理目標： 確保經授權使用者對資訊系統的存取及防止未經授權的存取。		
刪除				A.11.2.1			使用者註冊	10
7.4 是否對所有資訊系統與服務核准和撤銷存取，訂定適當之使用者註冊與註銷程序？								
7.5 是否於使用者變更角色、調職或離職後，立即移除或封鎖其存取權限？								
7.6 是否維持所有使用者註冊服務、系統或資訊等之正式紀錄？								
7.7 基於系統管理或特殊作業需要，需設定特殊權限時（如系統管理、高階管理者），是否透過正式授權過程，控制特殊權限之配置？				A.11.2.2			特權管理	6
7.8 是否維護所有配置特殊權限之授權過程和紀錄，並於完成授權過程後才授予特殊權限？								
7.9 是否在提供使用者通行碼前，進行身份鑑別程序？				A.11.2.3			使用者通行碼管理	8
7.10 是否以安全之程序轉交預設之通行碼給使用者，使用者取得通行碼，確認無誤後，需回應系統管理者？								
7.11 軟體安裝完畢後，是否立即更新廠商所預設之通行碼？								

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
7.12 是否要求使用者於聘僱任期與條件中，簽署對個人通行碼保密聲明？								
7.13 是否強制要求使用者，初次登入電腦系統後，必須立即更改預設通行碼，或一定期限內未登入，則預設通行碼將失效，必須重新申請建立？								
7.14 是否規定通行碼不得以無保護之型式儲存於電腦系統中？								
7.15 所有使用者存取權限，是否定期檢查（建議每六個月一次、特權者每三個月一次）及任何變更(如升職、降職、調職或聘僱終止等)後審查？				A.11.2.4			使用者存取權限之審查	5
				A.11.3		使用者責任 目標： 防止未經授權的使用者存取、危及或竊盜資訊及資訊處理設施。		
7.16 通行碼長度是否規定須超過6個字元（建議以9個字元位或以上）？								
7.17 通行碼是否規定需以大小寫字母、特殊符號及數字組成？								
7.18 通行碼輸入錯誤，是否訂有三次以內之限制？								
7.19 是否定期、依規定期限或使用次數限制，要求變更通行碼，並避免重複或循環使用舊通行碼？								
7.20 是否規定不得在任何自動登入過程中內含通行碼，例如：儲存在巨集或功能鍵中。								
7.21 是否規定避免使用與個人有關資訊（如生日、身分證統一編號、單位簡稱、電話號碼等）當做通行碼？				A.11.3.1			通行碼的使用	9
7.22 是否避免保留通行碼的紀錄（例如：紙張、軟體檔案或手持裝置）， 除非其能被安全地存放，且該存放方式經過核准？								
7.23 應用系統是否具有作業結束後或在一定期間未操作時即自動登出之保護機制？								
刪除								
7.24 是否避免將輸入之通行碼以明文方式顯示在螢幕上？								
7.25是否 對於無人看管之資訊設施有適當保護措施？				A.11.3.2			無人看管之使用者設備	3

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
7.26 是否訂有桌面淨空及螢幕淨空政策？				A.11.3.3			桌面淨空與螢幕淨空政策	5
刪除								
7.27 主機、伺服器、個人電腦、終端機等電腦設備於不使用、人員離座時是否即刻進行保護措施如關機、登出、設定螢幕保護密碼或是以其他控制措施進行保護？								
7.28 下班後經辦之機密性及敏感性資訊是否妥爲收存？								
7.29 是否訂定適當之控制措施，防止未經授權使用影印機和其他複製設備（例如：掃瞄器、數位相機）？								
7.30 敏感性或機密性資訊文件，是否立即從印表機上取走？								
				A.11.4		網路存取控制 目標： 防止網路服務遭未經授權的存取。		
7.31 網路使用者（含外單位人員）是否取得正式存取授權？				A.11.4.1			網路服務的使用政策	4
7.32 是否於登入作業完成後，顯示前一次登入日期與時間，或提供登入失敗之詳細資訊？				A.11.4.2			外部連線之使用者鑑別	1
7.33 是否限制登入失敗次數超過上限時，需強制延遲一段時間或重新取得授權後才允許再登入？								
7.34 是否訂定網路服務存取安全政策，確保使用者係經特定授權允許存取網路與網路服務？								
7.35 對於外部連線使用者是否進行身份鑑別機制，如密碼技術、硬體符記或詰問/應答（challenge/response）協定等安全技術？								
7.36 是否採用自動設備識別方法，鑑別存取敏感或機密資訊之設備，方可允許其存取行爲？				A.11.4.3			網路設備識別	1
7.37 對於遠端使用者的存取控制，是否有適當的鑑別機制？								
刪除								

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
7.38 如需採用遠端診斷作業方式，是否訂定診斷埠之存取作業規範（如用金鑰管理及人員身份查驗或稽核等機制）？				A.11.4.4			遠端診斷與組態埠保護	1
7.39 無線網路之存取及應用，是否訂有嚴謹之鑑別、加密方式及頻率選擇等控制措施？								
7.40 是否依據網路服務需要，區隔出獨立邏輯網域（如組織內部網路或外部網路），每個網域皆有定義的安全邊界，及通訊閘道管制過濾網域間資料之存取（如網路防火牆）？				A.11.4.5			網路區隔	1
刪除				A.11.4.6			網路連線控制	4
7.41 是否針對電子郵件、單雙向檔案傳輸、互動式存取或應用系統之存取時段作必要之限制？								
7.42 是否實施網路路徑控制，以確保電腦連線及資訊流，不會破壞營運應用程式之存取控制政策？				A.11.4.7			網路選路徑控制	1
	6.2 是否提供使用者能有效辨識與認可正確之電信服務營運商（如用戶無法證實時，應有的警示措施）的適切的控制措施？	6.3 是否有適切的控制機制，提供使用者能有效的辨識與認可正確的電信服務（如用戶無法證實時，應有的警示措施）？	文字措詞修訂	A.11.4.8			電信服務商之識別與鑑別 Telecommunications carrier identification and authentication by users.	1
				A.11.5		作業系統存取控制目標： 防止作業系統遭未經授權的存取。		
7.43 是否提供登入程序最小限之系統輔助訊息，避免提供未經授權使用者任何不必要協助？				A.11.5.1			安全之登入程序	9
7.44 是否依據系統機敏度，限制登入失敗次數之上限，並於登入失敗後中斷連線？								

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
7.45 是否對於異常登入程序，留有紀錄及定期檢視？								
7.46 系統登入或存取重要資訊時，是否對連線過程提供加密之程序與措施？								
7.47 使用者是否採用具有唯一性之識別符號（使用者ID）？				A.11.5.2			使用者識別與鑑別	1
7.48 重要系統使用者，是否採用適切之身分鑑別技術，例如：一次性密碼、智慧卡、符記或生物特徵？								
7.49 是否以保護的形式儲存和傳送通行碼，並告知申請者？通行碼檔案是否和應用系統資料分開存放？				A.11.5.3			通行碼管理系統	9
7.50 使用系統公用程式是否進行授權管制（如最低實務需求的授權）及身分鑑別程序？需要職務區隔時，是否有管制措施不讓具備系統應用程式存取權限的使用者，取得系統公用程式之權限？				A.11.5.4			系統公用程式的使用	9
7.51 是否設定網路會談結束或超過定義的無動作時限後，即中斷連線或關閉設備？				A.11.5.5			會談逾時	1
7.52 對風險高之應用系統，是否限制連線時間，如連線時間限制在正常辦公時間內？				A.11.5.6			連線時間的限制	3
				A.11.6		應用系統與資訊存取控制 目標： 防止應用系統中的資訊遭未經授權的存取。		
刪除				A.11.6.1			資訊存取限制	4
7.53 是否訂定使用者及支援人員，對應用系統存取權限之管制措施？								
7.54 處理機密及敏感性資訊，是否採用專屬（隔離）電腦作業環境？				A.11.6.2			敏感性系統的隔離	2

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.11.7		行動計算與遠距工作 目標： 確保使用行動運算與遠距工作設施時之資訊安全。		
7.55 是否訂定行動運算及通信設備之管理政策（如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求）？				A.11.7.1			行動運算與通信	2
7.56 遠距工作是否得到管理階層授權（如活動政策、計畫及流程等）和施以必要之保護措施？				A.11.7.2			遠距工作	19
7.57 遠距工作活動結束後，是否撤銷相關授權與存取權限及歸還管制設備？								
8.資訊系統獲取、開發及維護				A.12	資訊系統獲取、開發及維護			

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.12.1		資訊系統之安全要求 目標： 確保安全是整體資訊系統的一部分。		
8.1 在規劃應用系統需求時，是否將安全需求納入分析及規格文件中？				A.12.1.1			安全需求之分析與規格	1
				A.12.2		應用系統之正確處理 目標： 防止應用系統中資訊的錯誤、遺失、未經授權的修改或誤用。		
8.2 是否檢查輸入資料，確認其正確性及適切性？				A.12.2.1			輸入資料確認	7
8.3 是否針對輸入錯誤，設計及實作回應程序？								
8.4 應用程式內部處理是否加入確認查核（validation check），偵測可能經由處理錯誤或故意行爲之任何資訊毀損，並提供適當程式從失效中復原，確保資料之正確處理？				A.12.2.2			內部處理的控制措施	12
8.5 應用系統是否使用密碼技術，鑑別與保護其訊息之完整性？				A.12.2.3			訊息完整性	1
8.6 輸出資訊是否具合理性查核及一致性控制計數（reconciliation control count），確保所有資料都已合理處理？				A.12.2.4			輸出資料確認	6
8.7 是否設計與實作輸出確認測試與回應之程序？								
8.8 是否設計並實作資料輸出確認過程之活動日誌，並定義所有涉及資料輸出過程人員之責任？								
				A.12.3		密碼控制措施 目標： 藉由密碼方式以保護資訊的機密性、鑑別性或完整性。		
8.9 是否基於風險評鑑結果，識別所需的保護等級，設計所需加解密演算法之型式、強度及品質？				A.12.3.1			使用密碼控制措施的政策	7

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
8.10 是否基於風險評鑑結果管理密碼金鑰，並發展適當之控制措施？				A.12.3.2			金鑰管理	11
				A.12.4		系統檔案之安全 目標： 確保系統檔案的安全。		
8.11 作業系統升級前，是否考量營運要求及該版本之安全性？	刪除	7.1 更新作業軟體、應用軟體、程式庫之人員，是否由經過適當訓練之管理員執行，並經過適當之管理授權？	本項內容與資安管理內部稽核表8.9、8.13條文內容雷同，建議刪除。	A.12.4.1			作業軟體之控制	8
8.12 處理作業系統軟體更新之人員，是否經管理階層授權？	7.1 操作系統環境中，應只能保持一套經批准之程式碼，不能有發展中程式碼與安裝編譯器程式？	7.2 操作系統之環境中應只能保持一套經批准之程式碼，不能有發展中之程式碼與安裝有編譯器程式？						
8.13 是否限定由經過訓練合格之管理人員，才可執行應用程式可執行碼更新作業？	刪除	7.3 是否採用型態管理控制系統來保持所有建置之軟體與文件一致？	本項內容與資安管理內部稽核表8.14條文內容雷同，建議刪除。					
8.14 是否使用組態控制系統，以保持對所有已實作的軟體與系統文件之控制，且維護所有變更紀錄？	7.2 所有資訊系統變更實作前，是否均有適當之回復策略？	7.4 所有資訊系統變更實作前，是否均有適當之回復策略？						
	7.3 是否針對所有運作中程式原始碼之更新及維護，留存稽核日誌？	7.5 是否針對所有運作中程式原始碼之更新維護稽核日誌？	文字措詞修訂					
	7.4 是否針對屬敏感性系統（如交換器設備等）之作業系統軟體或應用軟體，實施涵蓋所有路徑之完整測試？	7.6 是否針對屬敏感性系統（如交換器設備等）之作業系統軟體或應用軟體，實施涵蓋所有路徑之完整測試？						
	7.5 是否針對屬敏感性系統之應用軟體，至少保留前三代版本相關備份？	7.7 是否針對屬敏感性系統之應用軟體，至少保留前三代版本相關備份。	文字措詞修訂					
8.15 是否避免以真實資訊進行測試作業？				A.12.4.2			系統測試資料之保護	4
8.16 存取程式原始碼（program source code），是否訂有適當之控制措施，並留存稽核日誌？				A.12.4.3			程式源碼之存取控制	7
刪除								
				A.12.5		開發及支援處理之安全 目標： 維持應用系統軟體及資訊的安全。		

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
8.17 是否建立變更應用系統之管制程序？				A.12.5.1			變更控制程序	11
8.18 應用系統變更後，是否立即更新系統文件？								
8.19 作業系統變更後，是否對應用系統作技術性審查？				A.12.5.2			作業系統變更後的應用系統技術審查	4
8.20 作業系統變更後，是否主動公告異動範圍、時間及可能的影響？								
8.21 作業系統變更後，是否檢查其相關控管措施與程序仍然有效？								
刪除								
8.22 是否僅限於必要的範圍，變更套裝軟體之，並嚴格管制所有變更？				A.12.5.3			套裝軟體變更的限制	4
8.23 是否檢查組織內可能之隱匿通道(covert channel)，降低資訊洩漏的風險？				A.12.5.4			資料洩漏	5
8.24 委外開發之系統上線前，是否偵測有無惡意程式存在？				A.12.5.5			委外軟體開發	6
8.25 委外開發合約中，是否規範著作權之歸屬？								
8.26 訂約時，是否簽訂安全履行條款與相關罰則？								
				A.12.6		技術脆弱性管理 目標： 降低利用已公佈技術弱點所導致的風險。		
8.27 是否及時取得使用中通訊傳播系統之技術脆弱性資訊，並定期執行各項系統漏洞修補程式？				A.12.6.1			技術脆弱性控制	10
8.28 進行系統修補前，是否先作系統影響評估與測試，再採取必要措施？								
9.資訊安全事故管理				A.13	資訊安全事故管理			
				A.13.1		通報資訊安全之事件及弱點 目標： 確保與資訊系統相關的資訊安全事件及弱點，能夠及時傳達並矯正。		

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
9.1 是否建立資安事故（含安全漏洞、系統弱點、病毒、非法入侵及系統異常）之正式通報應變程序？				A.13.1.1			通報資訊安全事件	4
9.2 事故回應小組是否建立單一聯繫窗口，授權在處理事故時採取立即之決定，並與外部團體（例如：執法機關、政府緊急應變中心、客戶、商業夥伴）建立聯繫管道？								
9.3 資訊安全事故處理過程，是否留有完整記錄，如有必要，應經由直接發送電子郵件及/或網站首頁，及時回報事故給相關客戶？								
9.4 是否建立資訊安全事故通報之聯絡點，並確保全組織都知道該聯絡點，隨時可聯繫，能夠有充分與及時的回應？								
9.5 機關員工及外部使用者是否知悉資安事故通報及處理程序並依規定辦理?				A.13.1.2			通報安全弱點	1
9.6 是否要求資訊系統與服務的所有員工、承包商及第三方使用者，注意並通報任何觀察到或可疑的系統或服務之安全弱點？								
				A.13.2		資訊安全事故之管理及改進 目標： 確保資訊安全事故的管理採用一致及有效的作法。		
9.7 是否依不同型式之資訊安全事故，建立資安事故管理責任及應變程序？	8.1 是否建立資安事故之通報及事故回應與提報處理程序的管理責任與職掌定義？	8.1 是否建立資安事件之通報及事故回應與提報處理程序的管理責任與職掌定義？		A.13.2.1			責任與程序	4
刪除								
9.8 是否建立資安事件或事故等事後管理會議，以協助單位能從資安事件及事故中學習？	8.2 是否建立資安事件或事故等事後管理會議，以協助單位能從資安事件、事故中學習？	8.2 是否建立資安事件或事故等事後管理會議，以協助單位能從資安事件、事故中學習？						
9.9 是否擬定營運中斷後之各項風險處理優先順序或處理準則（含處理順序說明、最低營運水準定義）？								

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
9.10 是否建立資安事故管理機制，如記錄事故型式、處理方法、處理成本及矯正預防措施？				A.13.2.2			從資訊安全事故中學習	1
9.11 是否已建立及使用各項指標，以協助偵測安全事故，並預防安全事故？								
9.12 已發生之資訊安全事故，是否在安全政策審查過程中納入考量？								
9.13 資安事故中相關證據資料是否有適當保護措施，以符合證據能力之要求，作爲問題分析及法律必要依據？				A.13.2.3			證據的收集	4
10.營運持續管理				A.14	營運持續管理			
				A.14.1		營運持續管理之資訊安全觀點 目標： 爲防範營運活動中斷，保護重要營運過程不受重大資訊系統失效或災害的影響，並確保及時重新開始(resumption)。		
10.1 是否發展與實作營運持續計畫，以因應組織營運持續所需的資訊安全要求？	8.3 是否訂定營運中斷後之各風險之處理優先順序或處理準則？	8.3 是否擬定營運中斷後之各風險之處理優先順序或處理準則？	文字措詞修訂	A.14.1.1			資訊安全納入營運持續管理過程	10
10.2 是否針對所有營運過程，可能造成營運中斷之機率及衝擊進行風險評鑑？								

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
刪除				A.14.1.2			營運持續與風險評鑑	1
10.3 是否識別營運持續過程中之關鍵資通訊設備及資訊處理設施？								
10.4 營運持續計畫是否以人員安全爲優先，並保護資通訊設備和組織財產？				A.14.1.3			發展與實作包括資訊安全的持續計畫	7
刪除								
10.5 是否訂定營運持續計畫（含啓動條件、參與人員、緊急程序、後撤程序、回復程序、維護時程、教育訓練、職責說明、所須資源、往來單位之應變規劃及合約適當性等）？								
10.6 是否維持營運持續計畫之單一框架， 以確保所有計畫有一致性， 持續一致地因應資訊安全要求， 並識別測試與維護的優先順序？				A.14.1.4			營運持續計畫框架	9
刪除				A.14.1.5			營運持續計畫的測試、維護及重新評鑑	6
10.7 營運持續計畫（含緊急應變處理程序）是否配合業務、組織及人員之變更而更新？								
10.8 營運持續計畫是否定期完整測試、演練並予更新維護?								
11.遵循性				A.15	遵循性			
				A.15.1		符合法規要求 目標： 避免違反任何法律、法規命令、行政規則或契約義務及任何安全要求。		
11.1 是否確保所有通訊系統與組織均不違反任何法律、法規命令、行政規則、契約義務及相關安全要求？				A.15.1.1			識別適用之法條	1
11.2 軟體取得（含自行開發、委外開發、購置或租用）等可能涉及智慧財產權規定，是否符合法律、法規命令及契約的要求？								

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
11.3 是否公布智慧財產權遵循政策，定義軟體與資訊產品的合法使用，並告知違反政策人員將遭懲處？				A.15.1.2			智慧財產權	13

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
11.4 是否維護使用版權、原版碟片、手冊等所有權之證明和證據，並定期檢核是否只安裝經授權之軟體與有使用版權之產品？								
11.5 組織重要紀錄（如資料庫紀錄、系統日誌、操作日誌、稽核日誌）是否依安全等級加以保護及儲存（如檔案加密或數位簽章）？				A.15.1.3			組織紀錄的保護	4
11.6 稽核後是否產生稽核報告，並追踪改善情形（包括稽核發現之摘要、稽核區域、缺失說明及改進建議等）？								
11.7 組織中對於所經管或處理之資訊，涉及個人隱私及個人資料之保護是否有適當之保護機制？				A.15.1.4			個人資訊的資料保護與隱私	1
11.8 是否發展和實作符合法律、法規及若適用的契約條文所要求的資料保護與隱私政策？								
11.9 是否依據個人資料保護法擬定個人資料檔案安全維護計畫及業務終止個人資料處理方法？								
11.10 是否有監視設備或其他可偵測未經授權使用之設備，防止資訊設施被不當使用？				A.15.1.5			防止資訊處理設施的誤用	1
11.11 管理人員是否定期審查其責任範圍內之資訊處理設施與其安全政策、標準及符合其他相關安全要求？								
				A.15.1.6			密碼控制措施的規定	4
				A.15.1.7			Non-disclosure of communications	10
				A.15.1.8			Essential communications	18
				A.15.1.9			Legality of emergency actions	1
				A.15.2		符合安全政策、標準及技術規範 目標： 確保系統符合組織的安全政策及標準。		
11.12 組織訂定之安全程序，是否確保相關人員能正確執行？				A.15.2.1			安全政策與標準的符合	4

附件7　通訊事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 電信事業增項控制措施 (A級) （修訂建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
11.13 資訊系統是否定期進行安全技術符合性檢查（如滲透測試或系統弱點檢測）？				A.15.2.2			技術符合之查核	1
11.14 技術遵循性之查核人員是否經過訓練，並作事前工作分配？								
11.15 技術遵循性檢查是否由合格資安技術單位執行？								
11.16 技術遵循性查核時之存取行爲，是否作監控，並適當保存紀錄？								
11.17 技術遵循性查核結果是否文件化？								
				A.15.3		資訊系統稽核考量目標： 使資訊系統稽核處理的有效性最大化，並使其產生或受到之干擾最小化。		
11.18 是否訂定資訊安全內部稽核計畫（含稽核目標、範圍、時間、程序、人員）？				A.15.3.1			資訊系統稽核控制	9
11.19 是否定期辦理資訊安全內部稽核？								
11.20 內部稽核範圍是否含括資通系統、供應商、資產負責人、使用者和管理階層？								
11.21 是否有保護資訊系統稽核工具之存取，防止可能誤用或破解之措施？				A.15.3.2			資訊系統稽核工具的保護	1
277	55	56		合計	11	40	146	803
圖例：	安全領域	安全目標	控制措施/ 實作指引	27011新增 控制措施	27011 補充措施	未納入 控制措施		

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
1.資訊安全政策				A.5	安全政策			
				A.5.1		資訊安全政策 目標： 依據營運要求及相關法律與法規，管理階層提供資訊安全之指示與支持。		
1.1 是否依據相關法律、法規及營運要求，訂定組織資訊安全政策？				A.5.1.1			資訊安全政策之文件	6
1.2 是否考量組織之整體業務活動及其相關風險，訂定資訊安全政策？								
1.3 是否識別違反資訊安全政策之後果及訂定處理程序？								
1.4 是否由管理階層核准資訊安全政策文件，正式發布且轉知所有員工與各相關外部團體？								
1.5 資訊安全政策文件是否包括資訊安全之定義、整體目標、範圍、實施內容、執行組織、權責分工、員工責任、事故通報處理流程？								
1.6 是否依據資訊安全政策，訂定原則、標準及對組織特別重要之法規要求說明文件及資料（如法律、法規命令、行政規則、契約、安全教育、訓練、認知、營運持續管理、作業程序、資訊安全控管文件、使用者應遵守的安全規則）？								
1.7 資訊安全政策是否就一般和特定責任之權責（包括通報資訊安全事故）加以定義？。								
1.8 是否對支援資訊安全政策的文件建立補述文件？例如：針對特定資訊系統的更詳盡安全政策和程序，或使用者宜遵守的安全規則。								
1.9 資訊安全政策是否由具有發展、審查及評估等核准權限之管理者，依規劃期間或有重大變更時，作必要之審查及調整？				A.5.1.2			資訊安全政策之審查	12
1.10 是否妥善維護資訊安全管理政策之審查紀錄與訂定管理審查程序，包括審查時程及週期?								
1.11 是否定期對組織人員及資訊設備進行安全評估，以確定其遵守資訊安全政策及相關規定？								
1.12 是否指定專人或專責部門進行資訊安全政策的維護及檢討？								

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
2.資訊安全之組織				A.6	資訊安全之組織			
				A.6.1		內部組織 目標：管理組織內之資訊安全。		
2.1管理階層是否在組織內藉由清楚的指示、明確的指派及確認資訊安全責任， 主動地展現承諾以支持安全？				A.6.1.1			管理階層對資訊安全之承諾	8
2.2 是否指派擁有權責之管理階層或成立跨部門組織負責推動、協調及監督資訊安全管理事項？				A.6.1.2			資訊安全協調~~工作~~	7
2.3 是否指定專人或專責部門，負責辦理下列資訊安全管理工作事項(1)資安政策、計畫、措施之研議，(2)風險評鑑、資訊分類、系統安全控管措施，(3)資料及資訊系統之使用管理及保護，(4)資安認知訓練及資安稽核？								
刪除與2.3點內容合併								
2.4 資訊安全責任的配置是否依據資訊安全政策，並明確地識別需保護之個別資產與執行特定安全~~作業~~過程的責任，並加以文件化？				A.6.1.3			資訊安全責任之配置	3
2.5 是否依據員工之職務~~內容~~，訂定員工資訊安全作業程序、權責規範或授權層級並予以文件化？（含經管使用設備及作業須知）				A.6.1.4			資訊處理設施之授權過程	3
2.6 是否訂定各項資訊處理設施之用途及使用授權，及~~其~~安全之作業程序？								
刪除								
2.7 是否識別並定期審查組織對於資訊保護之機密性或保密協議之要求？		1.1 是否訂定並定期審視保密及防止不當揭露組織需保護資訊之機密性協議（例如通訊資訊中的實體、內容、來源、目的地、日期時間）？	文字措詞修訂	A.6.1.5			機密性協議	10
2.8 是否訂定當發生資安事故時，如何及時與主管機關聯繫並通報之適當程序或規定？		1.2 組織提供執法機關所請求之資訊時，是否訂定控管程序以確認此申請依據國家法規之合法過程與程序？	文字措詞修訂	A.6.1.6			與權責機關之聯繫	2
2.9 是否~~訂定~~與各特殊利益團體、專家安全論壇及專業協會維持適當聯繫？				A.6.1.7			與特殊利益團體之聯繫	6

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
2.10 獨立審查組織對資訊安全管理之作法與其實作（例如：各項資訊安全的控制目標、控制措施、政策、過程及程序），是否定期召開管理審查會議？當資安作業環境發生重大變更時，亦依上述作法與實作，召開管理審查會議？				A.6.1.8			資訊安全之獨立審查	1
				A.6.2		外部團體 目標： 維持外部團體存取、處理、通信或管理之組織資訊及資訊處理設施之安全。		
2.11 因營運需要開放給外部團體（含其他機關、往來業者、維護廠商、委外承包商、聘僱人員及一般民眾）使用之資訊，是否執行風險評鑑與實作安全控制措施？並於契約或規定中包含雙方權利、義務、資料保護、資訊保密、服務標的水準、智慧財產權、事故發生處理與違約處理等條款？				A.6.2.1			識別與外部團體相關之風險	19
2.12 是否對不開放外部團體存取的資訊進行必要的控制措施？								
2.13 因營運需要開放給外部組織或人員存取之資訊，其存取權限是否定期審查？								
2.14 因營運需要開放給外部團體（含其他機關、往來業者、維護廠商、委外承包商、聘僱人員及一般民眾等）使用之資訊，於開放使用之前，是否闡明所有已識別之安全要求？			參考ISO/IEC 27011 6.2.2內容增訂	A.6.2.2			處理客戶事務之安全說明	11

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
2.15 委外契約中有關安全需求內容，是否包含法律要求（如個人資料保護法）、雙方有關人員權責、安全控管措施、作業程序、事故通報程序、服務水準、對委外廠商稽核權等資訊安全責任與事宜，並得依實際需要適時修改安全控管措施及作業程序等？	1.4 提供第三方服務廠商存取權限之前，是否訂定清楚之協議內容，包含提供服務所需之相關安全政策與應注意事項，並確保沒有誤解之情形存在？		參考ISO/IEC 27011 6.2.3內容增訂	A.6.2.3			第三方協議中之安全說明	22

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
3.資產管理				A.7	資產管理			
				A.7.1		資產責任 目標： 達成及維持組織資產之適切保護。		
3.1 是否明確識別所有資產，並製作與維持所有重要資產的清冊？	2.1 是否明確定義組織的廣播電視系統，與其他組織相連結或相關之部份的管理責任，並加以文件化？	2.1 是否明確界定組織的電信設施與其他組織相連結或相關之部份的管理責任，並具體和明確的文件化？	文字措詞修訂	A.7.1.1			資產清冊	6
3.2 是否有明確之定義，如何分辨何種資產是重要資產，再依據該定義作資產盤點，並建立與維護重要資產清冊？								
3.3 現有之重要資產清冊是否包含災難回復所需之資訊，如：資產型態/格式/位置/備份資訊/使用版本/業務價值？								
3.4 資產清冊是否定期審查，確保資產處於適切狀態？								
3.5 是否識別所有資訊資產之擁有者，並指派其依適切控制措施維護資訊資產之責任？				A.7.1.2			資產之擁有權	2
3.6 是否識別及實作所有與資訊處理設施相關（含電子郵件、網路使用及行動設備等）之使用規則，並加以文件化？				A.7.1.3			資產可被接受之使用	2
				A.7.2		資訊分類 目標： 確保資訊得到適切之保護等級。		
3.7 是否依據資訊對於組織的價值、法律要求、敏感性及重要性加以分類？			參考ISO/IEC 27011 7.2.1內容增訂	A.7.2.1			分類指導綱要	1
3.8 是否依據組織採用的分類法，訂定適當之資訊標示與處理程序？				A.7.2.2			資訊標示與處理	1

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
3.9 是否對於機密性資訊、敏感性之手稿資訊、影印公文之廢紙及已過保存期限之公文，於棄置前予以銷毀？								
刪除								

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
4.人力資源安全				A.8	人力資源安全			
				A.8.1		聘僱前 目標： 確保員工、承包商及第三方使用者瞭解其責任， 並勝任其所被賦予的角色，以降低竊盜、詐欺或設施誤用的風險。		
4.1 是否依照組織的資訊安全政策，訂定正式文件，規範所有員工、承包商或第三方使用者之安全角色與責任？	3.1 是否詳細檢查員工、承包商及第三方使用者職務上被授權能夠存取之必要服務：如：客戶個人資料，並納入相關安全責任之中？	3.1 是否詳細檢查職務上能夠授權存取之必要服務：例如：客戶個人資料或是客戶通話內容等，並納入相關安全責任之中？	文字措詞修訂	A.8.1.1			角色與責任	5
	3.2 對於人員進用，是否考量相關傳播證照或具備適當的傳播知識和技能？	3.2 對於人員進用，是否考量相關電信證照或具備適當的電信知識和技能？	文字措詞修訂					
4.2 是否明確定義所有聘僱之應徵者、承包商及第三方使用者背景查證檢核之限制與程序，確保符合隱私權、個人資料保護及/或聘僱勞工保護相關法令之要求？	3.3 對所有聘僱之應徵者、承包商及第三方使用者的之進用或委派，是否作適當之背景查驗工作，例如：工作職務涉及客戶個人資料或是傳播內容之存取者？	3.3 對所有聘僱之應徵者、承包者及第三方使用者的之進用或委派，是否作適當之背景查驗工作，例如：工作職務涉及客戶個人資料或是通訊內容之存取者？	文字措詞修訂	A.8.1.2			篩選	5
4.3 被賦予機敏資訊存取權的所有員工、承包商及第三方使用者，是否在被允許存取資訊處理設施之前，簽署適當之機密性或保密協議？	3.4 聘請第三方機構前，是否明確定義和溝通其安全角色和職責？	3.4 聘請第三方機構之前，是否明確界定和溝通其安全角色和職責？		A.8.1.3			聘僱任期與條件	7
	3.5 對於委外承包商或第三方使用者，是否在合約中加入安全角色與職責的要求？	3.5 對於委外承包商或是第三方使用者，是否在合約中加入安全角色與職責的要						
	3.6是否要求組織內任何人從事傳播服務時，應保護職務上所知悉之營業秘密？	3.6 組織內任何人從事電信服務時，是否要求應保護職務上所知悉之營業秘密？	文字措詞修訂					
	3.7 組織是否依據相關法規命令，訂定防止不當揭露之責任？	3.7 組織是否依據相關法規命令，訂定防止不當揭露之責任？						

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.8.2		聘僱期間 目標： 確保員工、承包商及第三方使用者認知資訊安全的威脅與關切事項、其責任與義務， 並有能力在日常工作中支持組織安全政策與降低人爲錯誤的風險。		
刪除				A.8.2.1			管理階層責任	6
刪除								
刪除								
4.4 管理階層是否有要求員工、承包商及第三方使用者，依照組織已訂定的政策與程序執行安全事宜？								
4.5 對所有員工、承包者及第三方使用者工作職務有關之安全程序及資訊處理設施，是否提供正確使用之認知、教育與訓練？				A.8.2.2			資訊安全認知、教育及訓練	1
刪除								
4.6 是否訂定員工違反組織安全政策與程序之懲處規定？				A.8.2.3			懲處過程	1
				A.8.3		聘僱終止或變更目標： 確保員工、承包商及第三方使用者依規定離職或變更聘僱。		
4.7 是否在與員工、承包商或第三方使用者所訂之契約內規定，在聘僱終止後，與職務有關之責任仍然是有效的？				A.8.3.1			終止責任	1

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
4.8 所有員工、承包商及第三方使用者離職或聘雇終止時，是否依規定繳回其任職期間保管之資訊資產？（包含所有的軟體、公司文件、設備、行動裝置、信用卡、存取卡、軟體、手冊及儲存於電子媒體的資訊等所有其他組織資產）				A.8.3.2			資產之歸還	1
4.9 所有員工、承包商及第三方使用者之聘僱、契約或協議終止時，或因變更而調整時，是否對資訊及資訊處理設施之存取權限迅速予以移除？				A.8.3.3			存取權限之移除	3

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
5.實體及環境安全				A.9	實體及環境安全			
				A.9.1		安全區域 目標： 防止組織的場所及資訊遭未經授權的實體存取、損害及干擾。		
5.1 是否適當使用安全邊界（如圍牆、入口閘門或人員駐守的接待櫃檯等屏障），保護含有資訊與資訊處理設施的區域？		4.1 電信營運中心是否有適當的實體入侵偵測系統？	本項內容與資安管理內部稽核表5.1內容雷同，建議刪除	A.9.1.1			實體安全周界	7
5.2 組織管理之資訊處理設施（如通訊服務設施），在實體上是否與第三方管理（如：客戶代管設備）之資訊處理設施區隔？	4.1 有權責人員是否於安全邊界發生異常狀況時，可立即處理？	4.2 實體邊界發生異常狀況時，是否有權責人員可立即解決？						
刪除	4.2 傳播系統之機房控制中心與操作室是否有適當強度之門禁管制措施（strong entry controls）？	4.3 控制中心與操作室是否有適當強度的進出控制措施（strong entry controls）？		A.9.1.2			實體進入控制措施	5
5.3 具有關鍵或敏感的資訊處理設施之安全區域，是否對於授權進出人員作必要之限制及監督其活動？		4.4 是否針對訪客的探訪紀錄進行適當保護？（訪客進入及離開時間、訪客身份等。）	本項內容與資安管理內部稽核表5.4內容雷同，建議刪除					
刪除		4.5 接待人員是否檢查訪客是否攜帶危險物品進入及帶走未經授權的物品？	本項內容與資安管理內部稽核表5.4內容雷同，建議刪除					
5.4 安全區域之進出權限是否定期審查並更新，並於必要時廢止？								
5.5 辦公處所是否實施必要之保護措施？				A.9.1.3			辦公室、房間及設施之保全	4
5.6 是否檢查及評估重要資通訊設備設置地點，鄰近場所之任何安全威脅，如火災、灰塵、水災、震動、化學效應、電力供應、電磁幅射、民間暴動及其他天然或人為災害等可能對設備之危害？				A.9.1.4			防範外部與環境之威脅	3
5.7 是否設計並實施適當的控制措施，以保護敏感資訊處理設施之地點及內部人員通訊錄？								
刪除								

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
5.8 是否嚴禁在電腦機房內使用未經核准之電器或其他物品？				A.9.1.5			在安全區域內工作	4
5.9 備援設備及備份媒體存放位置，是否與主要場地保持安全距離？								
5.10 安全區域是否與易燃物或危險物料保持安全距離，並不宜儲存大量的物資？								
5.11 是否設計並實施適當之控制措施，監督安全區域內之工作，並確保其需知原則？								
5.12 是否訂定未經授權前，禁止拍照、錄影、錄音和其他記錄性設備之規定，如行動裝置上的照相機？								
5.13 無人使用之安全區域是否上鎖並定期檢查？								
5.14 對於收發、裝卸區及其他未經授權人員可進入之作業場所，是否有適當之進出控制措施，並應與資訊處理設施隔離，以避免未經授權的存取？				A.9.1.6			公共進出、收發及裝卸區	6
	4.3 傳播事業維運中心是否設置於適當地點（如避免易遭水災、風災、地震影響，或臨近強烈電磁及儲存危險物之場所）？	4.6 通信中心（communication centers）是否選擇在適當地點?（避免選擇在易受水災、風災影響，與臨近強烈電磁及儲存危險物的場所）	文字措詞修訂	A.9.1.7			維運中心之安全 Securing communication centres	8
	4.4 傳播事業維運中心是否裝設自動火災警報系統？	4.7 通信中心是否裝設自動火災警報系統？	文字措詞修訂 本項內容與資安管理內部稽核表5.8內容雷同，建議5.8條刪除					
	4.5 傳播事業維運中心是否爲抗震建物？樓層地板是否有足夠之承載能力？	4.8 通信中心是否爲抗震建物？樓層地板是否有足夠的承載能力？	文字措詞修訂					
	4.6 傳播事業維運中心是否依據消防法規，使用防火建材？	4.9 通信中心是否盡可能使用防火建材？	文字措詞修訂					
		4.10 通信中心之設計是否盡可能避免火災蔓延？	本項內容與4.9條內容雷同，建議刪除					
	4.7 傳播設備機房，是否選擇於適當地點，具備防範風災、水災、地震及火災之能力，並配備適當之偵測設備，防止未經授權之入侵？	4.11 電信設備機房（telecommunications equipment room）或實體隔離的操作區（如：行動通信基地臺mobile base station）是否有足夠的安全防護？	文字措詞修訂	A.9.1.8			設備機房之安全 Securing telecommunications equipment room	15

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
	4.8 無人看管之隔離操作區，如：廣播電視中繼臺等，是否具備以下安全措施： (1)自動消防設備、(2)遠端監控及自動告警系統，包含設備失效、電力失效、火警及溫濕度監控、(3)適當之實體安全維護設施等？		本項內容參考ISO/IEC 27011 9.1.9條文內容，建議增訂。	A.9.1.9			隔離操作區之實體安全 Securing physically isolated operation areas	4
				A.9.2		設備安全 目標： 防止資產的遺失、損害、遭竊或洩漏及組織活動的中斷。		
5.15 是否明確訂定資通訊設備之控制措施（包括場外使用之設備，及財產之攜出），以降低資料未經授權存取、遺失及損壞之風險？				A.9.2.1			設備安置與保護	9
5.16 處理敏感資料的資通訊設備或資訊處理設施是否予特別保護並評估其有效性？		4.12 不同客戶之代管設備是否實體分隔，並實行適當之保護措施？						
5.17 是否採取適當控制措施，降低潛在實體威脅，如：竊盜、火災、爆裂物、煙害、水災（或水源供應停止）、閃電、溫度、濕度、灰塵、振動、化學效應、電力供應干擾、通信干擾、電磁輻射及蓄意破壞等？								
5.18 電腦作業區（含機房）是否落實執行禁止抽煙及飲食？								
5.19 是否具備環境監控機制，掌握資通訊設備及資訊處理設施之溫度及溼度狀況？								
5.20 是否對於支援性公共設施，如電源供應、水源供應、污水處理、暖氣/通風及空調，設計適當之保護措施，並施行之，確保不受公共設施失效所導致之中斷？	4.10 關鍵設施是否有不斷電系統或是足夠之備援電力保護？	4.13 關鍵設施是否有不斷電系統以及足夠電力保護？	文字措詞修訂	A.9.2.2			支援設施	1
5.21 備援電源是否定期檢查並測試，確保能在斷電期間正常運作？								
5.22 電信機線設備（telecommunications lines）、網路佈纜（network cabling）及電源纜線，是否設計適當之安全保護措施，並施行之？				A.9.2.3			佈纜的安全	6
5.23 通信纜線（communications cables）及電源纜線是否接地並隔離，防止互相干擾？								

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
5.24 設備是否定期且正確的維護保養，確保其可用性及完整性？				A.9.2.4			設備維護	5
5.25 各項設備是否依據供應商建議的間隔與保養手冊，定期檢查並維護？								
5.26 設備之維護與修理，是否由授權之維護人員執行？								
5.27 是否妥適保存所有可疑、實際之系統錯誤資訊，及所有預防性、矯正性之維護紀錄？								
5.28 設備送場外維修，對於儲存在設備內資訊是否訂有安全保護措施？								
5.29 攜出場所外之設備和媒體，是否訂有安全保護措施？				A.9.2.5			場所外設備之安全	4
5.30 行動裝置（設備）是否訂有嚴謹保護措施（如使用授權管理、設通行碼、檔案加密、專人看管）？								
5.31 設備汰除前，是否將機密性、敏感性資料及有版權的軟體予以移除或實施安全覆寫？				A.9.2.6			設備汰除或再使用之安全	1
5.32 含有敏感性資訊之設備汰除後，是否根據風險評鑑決定實體銷毀與否？								
5.33 資訊資產如須攜出場外使用，是否經事前授權，並於攜出場外與歸還時，進行安全查核及紀錄？				A.9.2.7			財產的攜出	4
				A.9.3		其他團體之安全管控 Security under the control of other party		
	4.11 傳播系統放置於其他組織處之設備，是否有足夠安全防護，且有定義清楚的邊界與介面，可以輕易加以隔離？	4.14 電信事業放置於其它場所的設備是否有足夠的安全防護，？	文字措詞修訂	A.9.3.1			位於其他服務供應商處之設備 Equipment sited in other carrier's premises	3
	4.12 放置於使用者端設備，是否具備遠端監控功能，必要時，可以輕易加以隔離？		本項內容參考ISO/IEC 27011 9.3.2條文內容，建議增訂。	A.9.3.2			位於使用者端之設備 Equipment sited in user premises	3
	4.13 是否持續監控與其它通信服務互連狀態，並有適當之控制措施，檢查與其它通訊服務互連是否正常？發生問題時，是否有方法可以矯正？	4.15 是否持續監控與其它通信服務互連的狀態？是否有適當的控制措施檢查與其它通訊服務互連是否正常？發生問題時，是否有方法可以檢查？	文字措詞修訂	A.9.3.3			互連之通訊服務 Interconnected telecommunications	1

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
	4.14 其它通信服務之互連是否已妥善定義邊界與介面？是否已定義用戶發生斷線時，如何處理之協議或合約？	4.16 其它通信服務互連是否已妥善定義範圍與介面？是否已定義一旦用戶發生斷線時如何處置的協議或合約？	文字措詞修訂				services	
6.通訊及作業管理				A.10	通訊及作業管理			

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.10.1		作業程序與責任目標： 確保正確與安全地操作資訊處理設施。		
6.1 資訊處理設施與資通訊設備相關之各項作業程序及活動是否文件化、並適當維護？如電腦開機與關機程序、備份、設備維護、資訊的處理與處理、異常情況之處理、緊急聯絡資訊、重新啓動及復原程序、稽核存底與日誌資訊之維護、電腦機房與郵件處理管理，以及生命財產安全（safey）等。	5.1 傳播系統操作程序是否包含事故、緊急或危機處理程序？	5.1 是否具體定義啓動災害情況、緊急情況或危機之處理程序的條件？	文字措詞修訂	A.10.1.1			作業程序文件化	8
6.2 資訊處理設施與資通訊設備之變更，是否有正式核准之程序，並向相關人員通報變更細節？	5.2 是否建立資訊處理設施與資通訊設備變更之管理程序？管理程序之紀錄是否包括設施之安裝、更改位置及移除？	5.2 是否建立資訊處理設施與系統變更之管理程序？管理程序之紀錄是否包括設施之安裝、改位置及移除？	文字措詞修訂	A.10.1.2			變更管理	6
6.3 資訊處理設施與資通訊設備之變更，是否詳實紀錄，並重新進行風險評鑑？								
6.4 資訊處理設施與資通訊設備之變更，是否備有後撤(fallback)程序，包括不成功的變更、意外事故的中止及復原之程序與責任？								
6.5 對於安全要求較高的業務，是否區隔其職務與責任領域？				A.10.1.3			職務的區隔	1
6.6 業務資訊資產之使用、資料建檔、系統操作、網路管理、行政管理、系統發展維護、變更管理、安全管理等工作，是否授權由不同的人員執行？								
6.7 是否分隔開發、測試及運作之設施、系統、軟體？	5.3 系統開發、測試及正式運作，是否區隔在不同的作業環境處理？	5.3 系統開發、測試及正式運作是否盡可能區隔在不同的作業環境處理？	文字措詞修訂	A.10.1.4			開發、測試及運作設施的分隔	6
6.8 運作測試系統是否使用不同的使用者剖繪（profile），且功能選單需顯示適切的識別訊息，降低錯誤之風險？	5.4 如採用敏感資訊進行測試，是否採取適當措施，避免程序或程式錯誤，導致不可預期之洩漏？	5.4 是否避免以真實之資訊進行系統開發與測試？	文字措詞修訂					

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.10.2		第三方服務交付管理 目標： 執行與維持適切之資訊安全等級服務交付，並與第三方服務交付協議一致。		
6.9 是否與第三方服務交付廠商簽訂適當之資訊安全協定，並納入契約條款，包含安全控制措施、服務定義及交付等級，並賦予相關安全管理責任？				A.10.2.1			服務交付	1
6.10 是否規劃必要轉換（資訊、資訊處理設施及其他任何需要移動者）之安全控制措施，並確保轉換期間安全的維護？								
6.11 是否定期對第三方所提供之服務、報告及紀錄等進行適當之監視與審查，並定期執行稽核？				A.10.2.2			第三方服務的監視與審查	5
6.12 第三方提供之服務如有任何異動時，是否重新進行風險評鑑？				A.10.2.3			第三方服務變更之管理	2
				A.10.3		系統規劃與驗收 目標： 使系統失效的風險最小化。		
6.13 資訊處理設施及資通訊設備設置前，是否進行容量規劃及預留安全容量，並於正式運作時，持續監控其容量狀態？				A.10.3.1			容量管理	1
6.14 是否建立新資訊系統、系統升級或新版本之驗收準則，在新資訊系統、系統升級及新版本正式驗收後，才可移轉上線？				A.10.3.2			系統驗收	10
				A.10.4		防範惡意碼與行動碼 目標： 保護軟體及資訊的完整性。		

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
6.15 是否全面使用防毒軟體，並即時更新病毒掃描引擎及病毒碼？				A.10.4.1			防範惡意程式的控制措施	8
6.16 電腦系統及資料儲存媒體是否定期進行惡意程式病毒及後門程式掃描？								
6.17 是否訂定正式政策，禁止使用未經授權的軟體？								
6.18 是否對支援重要營運程序之系統軟體與資料，執行定期審查？若出現任何未經核准的檔案或未經授權的增補修補程式，應進行正式調查。								
6.19 是否訂定使用電子郵件附件及下載之檔案前，檢查有無惡意程式軟體（含病毒、木馬或後門等程式）之程序？								
6.20 是否定義處理電腦病毒、木馬等惡意程式之管理程序與責任，並訓練員工如何通報惡意程式攻擊，及復原程序？								
6.21 是否準備遭惡意程式攻擊後復原之營運持續計畫，並包括所有必要之資料與軟體備份及復原準備工作？								
	5.5 安裝可攜碼（mobile code）是否作必要之授權處理或限制使用？是否考慮內嵌可攜碼之中介軟體（middleware）之限制使用？	5.5 行動碼（mobile code）的安裝是否作必要之授權處理或限制使用？內嵌行動碼之中介軟體（middleware）是否有考慮其限制使用？	文字措詞修訂	A.10.4.2			防範行動碼的控制措施	6
				A.10.5		備份 目標： 維持資訊及資訊處理設施的完整性與可用性。		
6.22 重要資訊及軟體是否定期作備份處理，並定義備份資訊之必要等級？				A.10.5.1			資訊備份	8
6.23 備份複本是否定期回復測試，並將回覆程序文件化，確保備份複本之可用性及有效性？								
6.24 重要及機敏資訊之備份程度及頻率，是否反應組織的營運要求？								
6.25 備份資訊是否儲存於遠端地點？距離須足以避免主要場地發生災難時遭波及？								

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
6.26 備份資訊是否給予適切等級之實體與環境保護，並與主要場域使用一致之標準？								
6.27 主要場域採用之控制措施是否延伸至涵蓋備份作業場域？								
6.28 是否定期檢查及測試復原程序，確保有效性，且能夠在復原程序分配之時間內完成復原運作？								
				A.10.6		網路安全管理 目標： 確保網路資訊及支援基礎建設進行保護。		
刪除				A.10.6.1			網路控制措施	5
6.29 是否訂定網路及網路遠端設備之使用權責及程序？								
6.30 是否使用網路安全防禦設備，並適當的隔離外部網際網路與組織內部網路？								
6.31 組織建立之網路控制措施，是否能反應資訊之機密性、完整性與可用性要求？								
6.32 對於機敏性資訊之傳輸過程，是否採取資訊加密等保護措施？								
6.33 是否訂定確保網路服務連線品質及可用性之保護措施，提供最佳服務？		5.6 是否訂定網路服務提供者及使用者之服務及使用範圍、相關權責及程序，並納入服務協議中？在服務提供前公告，並適切的維護與管理通信服務？		A.10.6.2			網路服務的安全	3
6.34 是否定期檢討網路安全控管事項之執行？								
6.35 是否定期檢測網路運作環境之安全漏洞？								
6.36 是否使用適當之網路安全解決方案？如防火牆、入侵偵測系統？防火牆存取政策（security policy）設定是否適當？								
			本項內容參考ISO/IEC 27011 10.6.3條文內容，建議增訂	A.10.6.3			電信服務交付之安全管理 Security management of telecommunications services delivery.	10

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
		5.7 是否訂定相關政策以對應垃圾郵件並建置適切之控管措施？建立一個合適的、令人期待的電子郵件通信環境。	文字措詞修訂	A.10.6.4			垃圾郵件之反應 Response to spam	1
	5.9 是否訂定相關政策，防範阻斷服務（DoS）或分散式阻斷服務（DDoS）攻擊，並建置適切控管措施，建立一個合適的、令人期待的傳播環境？	5.8 是否訂定相關政策以對應阻斷服務（DoS）或分散式阻斷服務攻擊（DDoS）並建置適切之控管措施？建立一個合適的、令人期待的電信環境。	文字措詞修訂					
	5.10 是否具備經由IP位置、通訊埠與通訊協定等個別過濾通訊或限制通訊頻寬之機制，適當的保護易遭受網路攻擊之網路設施，如伺服器、路由器等？	5.9 是否適當的保護網路設施，例如網路攻擊下的伺服器、路由器等？應具備經由IP位置、通訊埠與通訊協定等個別過濾通訊或限制通訊頻寬的機制。	文字措詞修訂					
		5.10 是否具備偵測偽造來源地址（IP spoofing）的能力？	文字措詞修訂					
		5.11 是否運用嚴格的密碼控制措施及/或高強度憑證（strong authentication）的功能以防範來源造假（source impersonation）？	文字措詞修訂					
		5.12 是否事先經由定期的收集與量測有關於災難、意外事件、社會現象等導致電信設備失效與網路壅塞之相關資訊並彙集關鍵知識？	文字措詞修訂					
		5.13 通訊設備是否具備偵測網路壅塞並避免網路壅塞時通訊集中之機制？	文字措詞修訂	A.10.6.5			DoS/DDoS攻擊之反應 Response to DoS/DDoS attacks	3
	5.15 是否訂定作業程序，預先收集可能造成廣播中斷或是預期事件之資訊？	5.14 是否制訂維運規範以收集可能造成網路雍塞之災難及計畫中事件的資訊？	文字措詞修訂					

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
	5.16 是否建置分散式處理中心，採用輔助設備及適當之組態，提升系統傳播能力，防範潛在系統崩潰或是災難之發生？	5.15 是否將暫時的設備總處理能能力經由量測納入改善考量？經由量測以改進潛在之營運中斷與災難時分散式處理中心與支援性設備的建置，並在必要時考量適切的配置變更。	文字措詞修訂					
		5.16 是否能鑑別並給予必要的通訊優先權以預防或減輕災難時交通維護、通訊、電力供應或維持社會秩序？	文字措詞修訂					
				A.10.7		儲存媒體之處理目標： 防止資產被未經授權的揭露、修改、移除或破壞，及中斷營運活動。		
6.37 是否建立各種可攜式媒體之操作管理程序，防止文件、電腦媒體（例如：磁帶、磁碟）、輸入或輸出資料及系統文件，遭受未經授權的揭露、修改、移除及破壞？				A.10.7.1			可攜式媒體的管理	6
刪除								
6.38 含有敏感性資訊之媒體是否以正式程序加以安全地汰除，例如：焚化或絞碎，或清除資料後由組織內其他應用系統使用？				A.10.7.2			媒體的汰除	5
刪除								
6.39 具機密性或敏感性資訊之媒體是否有安全之保存和報廢程序？								
6.40 機密性、敏感性資訊之儲存或處理是否有安全處理程序及分級標示？				A.10.7.3			資訊處理程序	9
6.41 是否建立資訊的處理及儲存的程序，以保護免於未經授權的揭露或誤用?								

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
6.42 對應用程式、程序、資料結構及授權過程等說明之系統文件，是否有適當的存取保護措施？				A.10.7.4			系統文件之安全	3
				A.10.8		資訊交換 目標： 維護組織內及外部團體交換資訊及軟體的安全。		
刪除				A.10.8.1			資訊交換政策與程序	15
6.43 是否對於所有形式之資訊交換，訂定適當交換政策、程序及控制措施？								
6.44 是否對高度機敏性資訊在傳輸或儲存中使用加密技術？								
6.45 是否訂定組織與任何外部團體間，交換資訊與軟體之協議？				A.10.8.2			交換協議	11
6.46 重要電腦資訊、媒體（含報表）之運送，是否有安全保護措施及完整監控記錄（含收送人、時間及內容）？				A.10.8.3			輸送中的實體媒體	5
6.47 是否訂定適當控制措施，保護含有資訊之媒體，在組織實體邊界外傳送時，不受未經授權的存取、誤用或毀損？								
6.48 採行電子交換之資訊，是否視資訊安全等級，採行識別碼與通行碼管制、電子資訊加密或電子簽章認證等保護措施，確保資訊的機密性、完整性、可用性及符合其他法律要求？				A.10.8.4			電子傳訊	6
6.49 涉及敏感性資訊及機密文件之營運資訊系統，是否提供適當之存取控制與保護？				A.10.8.5			營運資訊系統	10
				A.10.9		電子商務服務 目標： 確保電子商務服務的安全及其安全使用。		
刪除								

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
6.50 是否實施適當控制措施，保護在公眾網路上傳輸且涉及電子商務之資訊，使其不受詐欺行為、契約爭議及未經授權之揭露與修改？				A.10.9.1			電子商務	13
刪除				A.10.9.2			線上交易	6
6.51 線上交易服務，是否訂定適當控制措施，防止下列事項：(1)不完整傳輸、(2)誤選路徑、(3)未經授權之訊息修改、揭露及(4)未經授權的訊息複製或重送(replay)等發生？								
6.52 對外開放供公眾取得之資訊，是否訂定保護措施，確保資訊完整性，防止未經授權之修改？				A.10.9.3			公眾可用的資訊	4
				A.10.10		監控 目標： 偵測未經授權的資訊處理活動。		
6.53 是否依據法律要求，如個資法，實施適當之稽核存錄措施，以紀錄使用者活動、異常及資訊安全事故？	5.18 個人資料檔案之留存期限，是否遵守相關法規命令？	5.17 個人資料之留存時限是否依照權責單位之規定？	文字措詞修訂	A.10.10.1			稽核存錄	12
6.54 是否採用適切的存錄與監控設備，記錄資通訊相關活動？				A.10.10.2			監控系統的使用	5
6.55 是否建立適當之控制措施，監控資訊處理設施之使用，及定期審查？								
6.56 各項日誌是否有適當的保護措施，不受竄改與未經授權之存取，並針對留存之通信資訊設定適當之留存期限（例如：會計、帳務、客訴的處理、防止濫用及執法機關的要求）？				A.10.10.3			日誌資訊的保護	3
6.57 是否定期稽查各項作業日誌？								
6.58 是否適當規劃存錄設施與日誌資訊之儲存媒體容量，避免無法記錄事故或覆蓋以往所記錄事故？								
6.59 作業日誌是否留有管理者與操作者所涉及活動之詳細過程，並定期予以審查？				A.10.10.4			管理者與操作者日誌	4

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
刪除				A.10.10.5			失誤存錄	2
6.60 是否加以存錄由使用者或系統程式所通報之資訊處理或通信系統問題，迅速處理及通報？								
6.61 所有系統鐘訊是否與議定之鐘訊來源校正，以確保時間紀錄正確？				A.10.10.6			鐘訊同步	1
7.存取控制				A.11	存取控制			

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.11.1		存取控制之營運要求目標： 控制資訊的存取。		
7.1 是否根據營運與安全要求，建立、文件化及審查存取控制政策？		6.1 對於用戶端設備，電信事業是否策定適切的存取控制規則（例如：控制的要求應基於資訊擁有者而非設備擁有者；採原則禁止、例外開放之規則）？	文字措詞修訂	A.11.1.1			存取控制政策	16
7.2是否在存取政策文件中明確陳述每個使用者或使用群組之存取控制規則與權限？		6.2 是否將網路運作及電腦運作之使用權責予以區隔？	本項內容參考ISO/IEC 27011 11.1.1條文內容，建議刪除					
7.3 資訊存取控制政策是否符合相關法律、法規命令及契約規定，如電信法、個資法等？								
				A.11.2		使用者存取管理目標： 確保經授權使用者對資訊系統的存取及防止未經授權的存取。		
刪除				A.11.2.1			使用者註冊	10
7.4 是否對所有資訊系統與服務核准和撤銷存取，訂定適當之使用者註冊與註銷程序？								
7.5 是否於使用者變更角色、調職或離職後，立即移除或封鎖其存取權限？								
7.6 是否維持所有使用者註冊服務、系統或資訊等之正式紀錄？								
7.7 基於系統管理或特殊作業需要，需設定特殊權限時（如系統管理、高階管理者），是否透過正式授權過程，控制特殊權限之配置？				A.11.2.2			特權管理	6
7.8 是否維護所有配置特殊權限之授權過程和紀錄，並於完成授權過程後才授予特殊權限？								
7.9 是否在提供使用者通行碼前，進行身份鑑別程序？				A.11.2.3			使用者通行碼管理	8
7.10 是否以安全之程序轉交預設之通行碼給使用者，使用者取得通行碼，確認無誤後，需回應系統管理者？								
7.11 軟體安裝完畢後，是否立即更新廠商所預設之通行碼？								

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
7.12 是否要求使用者於聘僱任期與條件中，簽署對個人通行碼保密聲明？								
7.13 是否強制要求使用者，初次登入電腦系統後，必須立即更改預設通行碼，或一定期限內未登入，則預設通行碼將失效，必須重新申請建立？								
7.14 是否規定通行碼不得以無保護之型式儲存於電腦系統中？								
7.15 所有使用者存取權限，是否定期檢查（建議每六個月一次、特權者每三個月一次）及任何變更(如升職、降職、調職或聘僱終止等)後審查？				A.11.2.4			使用者存取權限之審查	5
				A.11.3		使用者責任 目標： 防止未經授權的使用者存取、危及或竊盜資訊及資訊處理設施。		
7.16 通行碼長度是否規定須超過6個字元（建議以9個字元位或以上）？				A.11.3.1			通行碼的使用	9
7.17 通行碼是否規定需以大小寫字母、特殊符號及數字組成？								
7.18 通行碼輸入錯誤，是否訂有三次以內之限制？								
7.19 是否定期、依規定期限或使用次數限制，要求變更通行碼，並避免重複或循環使用舊通行碼？								
7.20 是否規定不得在任何自動登入過程中內含通行碼，例如：儲存在巨集或功能鍵中。								
7.21 是否規定避免使用與個人有關資訊（如生日、身分證統一編號、單位簡稱、電話號碼等）當做通行碼？								
7.22 是否避免保留通行碼的紀錄（例如：紙張、軟體檔案或手持裝置）， 除非其能被安全地存放，且該存放方式經過核准？								
7.23 應用系統是否具有作業結束後或在一定期間未操作時即自動登出之保護機制？								
刪除								
7.24 是否避免將輸入之通行碼以明文方式顯示在螢幕上？								
7.25是否 對於無人看管之資訊設施有適當保護措施？				A.11.3.2			無人看管之使用者設備	3

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
7.26 是否訂有桌面淨空及螢幕淨空政策？				A.11.3.3			桌面淨空與螢幕淨空政策	5
刪除								
7.27 主機、伺服器、個人電腦、終端機等電腦設備於不使用、人員離座時是否即刻進行保護措施如關機、登出、設定螢幕保護密碼或是以其他控制措施進行保護？								
7.28 下班後經辦之機密性及敏感性資訊是否妥爲收存？								
7.29 是否訂定適當之控制措施，防止未經授權使用影印機和其他複製設備（例如：掃瞄器、數位相機）？								
7.30 敏感性或機密性資訊文件，是否立即從印表機上取走？								
				A.11.4		網路存取控制 目標： 防止網路服務遭未經授權的存取。		
7.31 網路使用者（含外單位人員）是否取得正式存取授權？				A.11.4.1			網路服務的使用政策	4
7.32 是否於登入作業完成後，顯示前一次登入日期與時間，或提供登入失敗之詳細資訊？				A.11.4.2			外部連線之使用者鑑別	1
7.33 是否限制登入失敗次數超過上限時，需強制延遲一段時間或重新取得授權後才允許再登入？								
7.34 是否訂定網路服務存取安全政策，確保使用者係經特定授權允許存取網路與網路服務？								
7.35 對於外部連線使用者是否進行身份鑑別機制，如密碼技術、硬體符記或詰問/應答（challenge/response）協定等安全技術？								
7.36 是否採用自動設備識別方法，鑑別存取敏感或機密資訊之設備，方可允許其存取行爲？				A.11.4.3			網路設備識別	1
7.37 對於遠端使用者的存取控制，是否有適當的鑑別機制？								
刪除								

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
7.38 如需採用遠端診斷作業方式，是否訂定診斷埠之存取作業規範（如用金鑰管理及人員身份查驗或稽核等機制）？				A.11.4.4			遠端診斷與組態埠保護	1
7.39 無線網路之存取及應用，是否訂有嚴謹之鑑別、加密方式及頻率選擇等控制措施？								
7.40 是否依據網路服務需要，區隔出獨立邏輯網域（如組織內部網路或外部網路），每個網域皆有定義的安全邊界，及通訊閘道管制過濾網域間資料之存取（如網路防火牆）？				A.11.4.5			網路區隔	1
刪除				A.11.4.6			網路連線控制	4
7.41 是否針對電子郵件、單雙向檔案傳輸、互動式存取或應用系統之存取時段作必要之限制？								
7.42 是否實施網路路徑控制，以確保電腦連線及資訊流，不會破壞營運應用程式之存取控制政策？				A.11.4.7			網路選路徑控制	1
		6.3 是否有適切的控制機制，提供使用者能有效的辨識與認可正確的電信服務（如用戶無法證實時，應有的警示措施）？	文字措詞修訂	A.11.4.8			電信服務商之識別與鑑別 Telecommunications carrier identification and authentication by users.	1
				A.11.5		作業系統存取控制目標： 防止作業系統遭未經授權的存取。		
7.43 是否提供登入程序最小限之系統輔助訊息，避免提供未經授權使用者任何不必要協助？				A.11.5.1			安全之登入程序	9
7.44 是否依據系統機敏度，限制登入失敗次數之上限，並於登入失敗後中斷連線？								

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
7.45 是否對於異常登入程序，留有紀錄及定期檢視？								
7.46 系統登入或存取重要資訊時，是否對連線過程提供加密之程序與措施？								
7.47 使用者是否採用具有唯一性之識別符號（使用者ID）？				A.11.5.2			使用者識別與鑑別	1
7.48 重要系統使用者，是否採用適切之身分鑑別技術，例如：一次性密碼、智慧卡、符記或生物特徵？								
7.49 是否以保護的形式儲存和傳送通行碼，並告知申請者？通行碼檔案是否和應用系統資料分開存放？				A.11.5.3			通行碼管理系統	9
7.50 使用系統公用程式是否進行授權管制（如最低實務需求的授權）及身分鑑別程序？需要職務區隔時，是否有管制措施不讓具備系統應用程式存取權限的使用者，取得系統公用程式之權限？				A.11.5.4			系統公用程式的使用	9
7.51 是否設定網路會談結束或超過定義的無動作時限後，即中斷連線或關閉設備？				A.11.5.5			會談逾時	1
7.52 對風險高之應用系統，是否限制連線時間，如連線時間限制在正常辦公時間內？				A.11.5.6			連線時間的限制	3
				A.11.6		應用系統與資訊存取控制 目標： 防止應用系統中的資訊遭未經授權的存取。		
刪除				A.11.6.1			資訊存取限制	4
7.53 是否訂定使用者及支援人員，對應用系統存取權限之管制措施？								
7.54 處理機密及敏感性資訊，是否採用專屬（隔離）電腦作業環境？				A.11.6.2			敏感性系統的隔離	2

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.11.7		行動計算與遠距工作 目標： 確保使用行動運算與遠距工作設施時之資訊安全。		
7.55 是否訂定行動運算及通信設備之管理政策（如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求）？				A.11.7.1			行動運算與通信	2
7.56 遠距工作是否得到管理階層授權（如活動政策、計畫及流程等）和施以必要之保護措施？				A.11.7.2			遠距工作	19
7.57 遠距工作活動結束後，是否撤銷相關授權與存取權限及歸還管制設備？								
8.資訊系統獲取、開發及維護				A.12	資訊系統獲取、開發及維護			

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
				A.12.1		資訊系統之安全要求 目標： 確保安全是整體資訊系統的一部分。		
8.1 在規劃應用系統需求時，是否將安全需求納入分析及規格文件中？				A.12.1.1			安全需求之分析與規格	1
				A.12.2		應用系統之正確處理 目標： 防止應用系統中資訊的錯誤、遺失、未經授權的修改或誤用。		
8.2 是否檢查輸入資料，確認其正確性及適切性？				A.12.2.1			輸入資料確認	7
8.3 是否針對輸入錯誤，設計及實作回應程序？								
8.4 應用程式內部處理是否加入確認查核（validation check），偵測可能經由處理錯誤或故意行爲之任何資訊毀損，並提供適當程式從失效中復原，確保資料之正確處理？				A.12.2.2			內部處理的控制措施	12
8.5 應用系統是否使用密碼技術，鑑別與保護其訊息之完整性？				A.12.2.3			訊息完整性	1
8.6 輸出資訊是否具合理性查核及一致性控制計數（reconciliation control count），確保所有資料都已合理處理？				A.12.2.4			輸出資料確認	6
8.7 是否設計與實作輸出確認測試與回應之程序？								
8.8 是否設計並實作資料輸出確認過程之活動日誌，並定義所有涉及資料輸出過程人員之責任？								
				A.12.3		密碼控制措施 目標： 藉由密碼方式以保護資訊的機密性、鑑別性或完整性。		
8.9 是否基於風險評鑑結果，識別所需的保護等級，設計所需加解密演算法之型式、強度及品質？				A.12.3.1			使用密碼控制措施的政策	7

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
8.10 是否基於風險評鑑結果管理密碼金鑰，並發展適當之控制措施？				A.12.3.2			金鑰管理	11
				A.12.4		系統檔案之安全 目標： 確保系統檔案的安全。		
8.11 作業系統升級前，是否考量營運要求及該版本之安全性？		7.1 更新作業軟體、應用軟體、程式庫之人員，是否由經過適當訓練之管理員執行，並經過適當之管理授權？	本項內容與資安管理內部稽核表8.9、8.13條文內容雷同，建議刪除。	A.12.4.1			作業軟體之控制	8
8.12 處理作業系統軟體更新之人員，是否經管理階層授權？	7.1 操作系統環境中，應只能保持一套經批准之程式碼，不能有發展中程式碼與安裝編譯器程式？	7.2 操作系統之環境中應只能保持一套經批准之程式碼，不能有發展中之程式碼與安裝有編譯器程式？						
8.13 是否限定由經過訓練合格之管理人員，才可執行應用程式可執行碼更新作業？		7.3 是否採用型態管理控制系統來保持所有建置之軟體與文件一致？	本項內容與資安管理內部稽核表8.14條文內容雷同，建議刪除。					
8.14 是否使用組態控制系統，以保持對所有已實作的軟體與系統文件之控制，且維護所有變更紀錄？	7.2 所有資訊系統變更實作前，是否均有適當之回復策略？	7.4 所有資訊系統變更實作前，是否均有適當之回復策略？						
	7.3 是否針對所有運作中程式原始碼之更新及維護，留存稽核日誌？	7.5 是否針對所有運作中程式原始碼之更新維護稽核日誌？	文字措詞修訂					
	7.4 是否針對屬敏感性系統（如交換器設備等）之作業系統軟體或應用軟體，實施涵蓋所有路徑之完整測試？	7.6 是否針對屬敏感性系統（如交換器設備等）之作業系統軟體或應用軟體，實施涵蓋所有路徑之完整測試？						
	7.5 是否針對屬敏感性系統之應用軟體，至少保留前三代版本相關備份？	7.7 是否針對屬敏感性系統之應用軟體，至少保留前三代版本相關備份。	文字措詞修訂					
8.15 是否避免以真實資訊進行測試作業？				A.12.4.2			系統測試資料之保護	4
8.16 存取程式原始碼（program source code），是否訂有適當之控制措施，並留存稽核日誌？				A.12.4.3			程式源碼之存取控制	7
刪除								
				A.12.5		開發及支援處理之安全 目標： 維持應用系統軟體及資訊的安全。		

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
8.17 是否建立變更應用系統之管制程序？				A.12.5.1			變更控制程序	11
8.18 應用系統變更後，是否立即更新系統文件？								
8.19 作業系統變更後，是否對應用系統作技術性審查？				A.12.5.2			作業系統變更後的應用系統技術審查	4
8.20 作業系統變更後，是否主動公告異動範圍、時間及可能的影響？								
8.21 作業系統變更後，是否檢查其相關控管措施與程序仍然有效？								
刪除								
8.22 是否僅限於必要的範圍，變更套裝軟體之，並嚴格管制所有變更？				A.12.5.3			套裝軟體變更的限制	4
8.23 是否檢查組織內可能之隱匿通道(covert channel)，降低資訊洩漏的風險？				A.12.5.4			資料洩漏	5
8.24 委外開發之系統上線前，是否偵測有無惡意程式存在？				A.12.5.5			委外軟體開發	6
8.25 委外開發合約中，是否規範著作權之歸屬？								
8.26 訂約時，是否簽訂安全履行條款與相關罰則？								
				A.12.6		技術脆弱性管理 目標： 降低利用已公佈技術弱點所導致的風險。		
8.27 是否及時取得使用中通訊傳播系統之技術脆弱性資訊，並定期執行各項系統漏洞修補程式？				A.12.6.1			技術脆弱性控制	10
8.28 進行系統修補前，是否先作系統影響評估與測試，再採取必要措施？								
9.資訊安全事故管理				A.13	資訊安全事故管理			
				A.13.1		通報資訊安全之事件及弱點 目標： 確保與資訊系統相關的資訊安全事件及弱點，能夠及時傳達並矯正。		

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
9.1 是否建立資安事故（含安全漏洞、系統弱點、病毒、非法入侵及系統異常）之正式通報應變程序？				A.13.1.1			通報資訊安全事件	4
9.2 事故回應小組是否建立單一聯繫窗口，授權在處理事故時採取立即之決定，並與外部團體（例如：執法機關、政府緊急應變中心、客戶、商業夥伴）建立聯繫管道？								
9.3 資訊安全事故處理過程，是否留有完整記錄，如有必要，應經由直接發送電子郵件及/或網站首頁，及時回報事故給相關客戶？								
9.4 是否建立資訊安全事故通報之聯絡點，並確保全組織都知道該聯絡點，隨時可聯繫，能夠有充分與及時的回應？								
9.5 機關員工及外部使用者是否知悉資安事故通報及處理程序並依規定辦理?				A.13.1.2			通報安全弱點	1
9.6 是否要求資訊系統與服務的所有員工、承包商及第三方使用者，注意並通報任何觀察到或可疑的系統或服務之安全弱點？								
				A.13.2		資訊安全事故之管理及改進 目標： 確保資訊安全事故的管理採用一致及有效的作法。		
9.7 是否依不同型式之資訊安全事故，建立資安事故管理責任及應變程序？	8.1 是否建立資安事故之通報及事故回應與提報處理程序的管理責任與職掌定義？	8.1 是否建立資安事件之通報及事故回應與提報處理程序的管理責任與職掌定義？		A.13.2.1			責任與程序	4
刪除								
9.8 是否建立資安事件或事故等事後管理會議，以協助單位能從資安事件及事故中學習？	8.2 是否建立資安事件或事故等事後管理會議，以協助單位能從資安事件、事故中學習？	8.2 是否建立資安事件或事故等事後管理會議，以協助單位能從資安事件、事故中學習？						
9.9 是否擬定營運中斷後之各項風險處理優先順序或處理準則（含處理順序說明、最低營運水準定義）？								

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
9.10 是否建立資安事故管理機制，如記錄事故型式、處理方法、處理成本及矯正預防措施？				A.13.2.2			從資訊安全事故中學習	1
9.11 是否已建立及使用各項指標，以協助偵測安全事故，並預防安全事故？								
9.12 已發生之資訊安全事故，是否在安全政策審查過程中納入考量？								
9.13 資安事故中相關證據資料是否有適當保護措施，以符合證據能力之要求，作爲問題分析及法律必要依據？				A.13.2.3			證據的收集	4
10.營運持續管理				A.14	營運持續管理			
				A.14.1		營運持續管理之資訊安全觀點 目標： 爲防範營運活動中斷，保護重要營運過程不受重大資訊系統失效或災害的影響，並確保及時重新開始(resumption)。		
10.1 是否發展與實作營運持續計畫，以因應組織營運持續所需的資訊安全要求？	8.3 是否訂定營運中斷後之各風險之處理優先順序或處理準則？	8.3 是否擬定營運中斷後之各風險之處理優先順序或處理準則？	文字措詞修訂	A.14.1.1			資訊安全納入營運持續管理過程	10
10.2 是否針對所有營運過程，可能造成營運中斷之機率及衝擊進行風險評鑑？								

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
刪除				A.14.1.2			營運持續與風險評鑑	1
10.3 是否識別營運持續過程中之關鍵資通訊設備及資訊處理設施？								
10.4 營運持續計畫是否以人員安全爲優先，並保護資通訊設備和組織財產？				A.14.1.3			發展與實作包括資訊安全的持續計畫	7
刪除								
10.5 是否訂定營運持續計畫（含啓動條件、參與人員、緊急程序、後撤程序、回復程序、維護時程、教育訓練、職責說明、所須資源、往來單位之應變規劃及合約適當性等）？								
10.6 是否維持營運持續計畫之單一框架， 以確保所有計畫有一致性， 持續一致地因應資訊安全要求， 並識別測試與維護的優先順序？				A.14.1.4			營運持續計畫框架	9
刪除				A.14.1.5			營運持續計畫的測試、維護及重新評鑑	6
10.7 營運持續計畫（含緊急應變處理程序）是否配合業務、組織及人員之變更而更新？								
10.8 營運持續計畫是否定期完整測試、演練並予更新維護?								
11.遵循性				A.15	遵循性			
				A.15.1		符合法規要求 目標： 避免違反任何法律、法規命令、行政規則或契約義務及任何安全要求。		
11.1 是否確保所有通訊系統與組織均不違反任何法律、法規命令、行政規則、契約義務及相關安全要求？				A.15.1.1			識別適用之法條	1
11.2 軟體取得（含自行開發、委外開發、購置或租用）等可能涉及智慧財產權規定，是否符合法律、法規命令及契約的要求？								

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
11.3 是否公布智慧財產權遵循政策，定義軟體與資訊產品的合法使用，並告知違反政策人員將遭懲處？				A.15.1.2			智慧財產權	13

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
11.4 是否維護使用版權、原版碟片、手冊等所有權之證明和證據，並定期檢核是否只安裝經授權之軟體與有使用版權之產品？								
11.5 組織重要紀錄（如資料庫紀錄、系統日誌、操作日誌、稽核日誌）是否依安全等級加以保護及儲存（如檔案加密或數位簽章）？				A.15.1.3			組織紀錄的保護	4
11.6 稽核後是否產生稽核報告，並追踪改善情形（包括稽核發現之摘要、稽核區域、缺失說明及改進建議等）？								
11.7 組織中對於所經管或處理之資訊，涉及個人隱私及個人資料之保護是否有適當之保護機制？				A.15.1.4			個人資訊的資料保護與隱私	1
11.8 是否發展和實作符合法律、法規及若適用的契約條文所要求的資料保護與隱私政策？								
11.9 是否依據個人資料保護法擬定個人資料檔案安全維護計畫及業務終止個人資料處理方法？								
11.10 是否有監視設備或其他可偵測未經授權使用之設備，防止資訊設施被不當使用？				A.15.1.5			防止資訊處理設施的誤用	1
11.11 管理人員是否定期審查其責任範圍內之資訊處理設施與其安全政策、標準及符合其他相關安全要求？								
				A.15.1.6			密碼控制措施的規定	4
				A.15.1.7			Non-disclosure of communications	10
				A.15.1.8			Essential communications	18
				A.15.1.9			Legality of emergency actions	1
				A.15.2		符合安全政策、標準及技術規範 目標： 確保系統符合組織的安全政策及標準。		
11.12 組織訂定之安全程序，是否確保相關人員能正確執行？				A.15.2.1			安全政策與標準的符合	4

附件8　傳播事業增項稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	ISO/IEC 27011 傳播事業增項控制措施 (A級) （增項建議）	ISO/IEC 27011 增項稽核表	修訂說明	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
11.13 資訊系統是否定期進行安全技術符合性檢查（如滲透測試或系統弱點檢測）？				A.15.2.2			技術符合之查核	1
11.14 技術遵循性之查核人員是否經過訓練，並作事前工作分配？								
11.15 技術遵循性檢查是否由合格資安技術單位執行？								
11.16 技術遵循性查核時之存取行爲，是否作監控，並適當保存紀錄？								
11.17 技術遵循性查核結果是否文件化？								
				A.15.3		資訊系統稽核考量目標： 使資訊系統稽核處理的有效性最大化，並使其產生或受到之干擾最小化。		
11.18 是否訂定資訊安全內部稽核計畫（含稽核目標、範圍、時間、程序、人員）？				A.15.3.1			資訊系統稽核控制	9
11.19 是否定期辦理資訊安全內部稽核？								
11.20 內部稽核範圍是否含括資通系統、供應商、資產負責人、使用者和管理階層？								
11.21 是否有保護資訊系統稽核工具之存取，防止可能誤用或破解之措施？				A.15.3.2			資訊系統稽核工具的保護	1
277	40	56		合計	11	40	146	803
圖例：	安全領域	安全目標	控制措施/ 實作指引	27011新增 控制措施	27011 補充措施	未納入 控制措施		

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
1.資訊安全政策		A.5	安全政策			
		A.5.1		資訊安全政策 目標： 依據營運要求及相關法律與法規，管理階層提供資訊安全之指示與支持。		
1.1 是否依據相關法律、法規及營運要求，訂定組織資訊安全政策？		A.5.1.1			資訊安全政策之文件	6
1.2 是否考量組織之整體業務活動及其相關風險，訂定資訊安全政策？						
1.3 是否識別違反資訊安全政策之後果及訂定處理程序？						
1.4 是否由管理階層核准資訊安全政策文件，正式發布且轉知所有員工與各相關外部團體？						
1.5 資訊安全政策文件是否包括資訊安全之定義、整體目標、範圍、實施內容、執行組織、權責分工、員工責任、事故通報處理流程？						
1.6 是否依據資訊安全政策，訂定原則、標準及對組織特別重要之法規要求說明文件及資料（如法律、法規命令、行政規則、契約、安全教育、訓練、認知、營運持續管理、作業程序、資訊安全控管文件、使用者應遵守的安全規則）？						
1.7 資訊安全政策是否就一般和特定責任之權責（包括通報資訊安全事故）加以定義？。						
1.8 是否對支援資訊安全政策的文件建立補述文件？例如：針對特定資訊系統的更詳盡安全政策和程序，或使用者宜遵守的安全規則。						
1.9 資訊安全政策是否由具有發展、審查及評估等核准權限之管理者，依規劃期間或有重大變更時，作必要之審查及調整？		A.5.1.2			資訊安全政策之審查	12
1.10 是否妥善維護資訊安全管理政策之審查紀錄與訂定管理審查程序，包括審查時程及週期?						
1.11 是否定期對組織人員及資訊設備進行安全評估，以確定其遵守資訊安全政策及相關規定？						
1.12 是否指定專人或專責部門進行資訊安全政策的維護及檢討？						

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
2.資訊安全之組織		A.6	資訊安全之組織			
		A.6.1		內部組織 目標：管理組織內之資訊安全。		
2.1管理階層是否在組織內藉由清楚的指示、明確的指派及確認資訊安全責任， 主動地展現承諾以支持安全？		A.6.1.1			管理階層對資訊安全之承諾	8
2.2 是否指派擁有權責之管理階層或成立跨部門組織負責推動、協調及監督資訊安全管理事項？		A.6.1.2			資訊安全協調~~工作~~	7
2.3 是否指定專人或專責部門，負責辦理下列資訊安全管理工作事項(1)資安政策、計畫、措施之研議，(2)風險評鑑、資訊分類、系統安全控管措施，(3)資料及資訊系統之使用管理及保護，(4)資安認知訓練及資安稽核？						
刪除與2.3點內容合併						
2.4 資訊安全責任的配置是否依據資訊安全政策，並明確地識別需保護之個別資產與執行特定安全~~作業~~過程的責任，並加以文件化？		A.6.1.3			資訊安全責任之配置	3
2.5 是否依據員工之職務~~內容~~，訂定員工資訊安全作業程序、權責規範或授權層級並予以文件化？（含經管使用設備及作業須知）		A.6.1.4			資訊處理設施之授權過程	3
2.6 是否訂定各項資訊處理設施之用途及使用授權，及~~其~~安全之作業程序？						
刪除						
2.7 是否識別並定期審查組織對於資訊保護之機密性或保密協議之要求？		A.6.1.5			機密性協議	10
2.8 是否訂定當發生資安事故時，如何及時與主管機關聯繫並通報之適當程序或規定？		A.6.1.6			與權責機關之聯繫	2

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
2.9 是否~~訂定~~與各特殊利益團體、專家安全論壇及專業協會維持適當聯繫？		A.6.1.7			與特殊利益團體之聯繫	6
2.10 獨立審查組織對資訊安全管理之作法與其實作（例如：各項資訊安全的控制目標、控制措施、政策、過程及程序），是否定期召開管理審查會議？當資安作業環境發生重大變更時，亦依上述作法與實作，召開管理審查會議？		A.6.1.8			資訊安全之獨立審查	1
		A.6.2		外部團體 目標： 維持外部團體存取、處理、通信或管理之組織資訊及資訊處理設施之安全。		
2.11 因營運需要開放給外部團體（含其他機關、往來業者、維護廠商、委外承包商、聘僱人員及一般民眾）使用之資訊，是否執行風險評鑑與實作安全控制措施？並於契約或規定中包含雙方權利、義務、資料保護、資訊保密、服務標的水準、智慧財產權、事故發生處理與違約處理等條款？		A.6.2.1			識別與外部團體相關之風險	19
2.12 是否對不開放外部團體存取的資訊進行必要的控制措施？						
2.13 因營運需要開放給外部組織或人員存取之資訊，其存取權限是否定期審查？						
2.14 因營運需要開放給外部團體（含其他機關、往來業者、維護廠商、委外承包商、聘僱人員及一般民眾等）使用之資訊，於開放使用之前，是否闡明所有已識別之安全要求？		A.6.2.2			處理客戶事務之安全說明	11

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
2.15 委外契約中有關安全需求內容，是否包含法律要求（如個人資料保護法）、雙方有關人員權責、安全控管措施、作業程序、事故通報程序、服務水準、對委外廠商稽核權等資訊安全責任與事宜，並得依實際需要適時修改安全控管措施及作業程序等？		A.6.2.3			第三方協議中之安全說明	22

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
3.資產管理		A.7	資產管理			
		A.7.1		資產責任 目標： 達成及維持組織資產之適切保護。		
3.1 是否明確識別所有資產，並製作與維持所有重要資產的清冊？		A.7.1.1			資產清冊	6
3.2 是否有明確之定義，如何分辨何種資產是重要資產，再依據該定義作資產盤點，並建立與維護重要資產清冊？						
3.3 現有之重要資產清冊是否包含災難回復所需之資訊，如：資產型態/格式/位置/備份資訊/使用版本/業務價值？						
3.4 資產清冊是否定期審查，確保資產處於適切狀態？						
3.5 是否識別所有資訊資產之擁有者，並指派其依適切控制措施維護資訊資產之責任？		A.7.1.2			資產之擁有權	2
3.6 是否識別及實作所有與資訊處理設施相關（含電子郵件、網路使用及行動設備等）之使用規則，並加以文件化？		A.7.1.3			資產可被接受之使用	2
		A.7.2		資訊分類 目標： 確保資訊得到適切之保護等級。		
3.7 是否依據資訊對於組織的價值、法律要求、敏感性及重要性加以分類？		A.7.2.1			分類指導綱要	1

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
3.8 是否依據組織採用的分類法，訂定適當之資訊標示與處理程序？		A.7.2.2			資訊標示與處理	1
3.9 是否對於機密性資訊、敏感性之手稿資訊、影印公文之廢紙及已過保存期限之公文，於棄置前予以銷毀？						
刪除						

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
4.人力資源安全		A.8	人力資源安全			
		A.8.1		聘僱前 目標： 確保員工、承包商及第三方使用者瞭解其責任， 並勝任其所被賦予的角色，以降低竊盜、詐欺或設施誤用的風險。		
4.1 是否依照組織的資訊安全政策，訂定正式文件，規範所有員工、承包商或第三方使用者之安全角色與責任？		A.8.1.1			角色與責任	5
4.2 是否明確定義所有聘僱之應徵者、承包商及第三方使用者背景查證檢核之限制與程序，確保符合隱私權、個人資料保護及/或聘僱勞工保護相關法令之要求？		A.8.1.2			篩選	5
4.3 被賦予機敏資訊存取權的所有員工、承包商及第三方使用者，是否在被允許存取資訊處理設施之前，簽署適當之機密性或保密協議？		A.8.1.3			聘僱任期與條件	7

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
		A.8.2		聘僱期間 目標： 確保員工、承包商及第三方使用者認知資訊安全的威脅與關切事項、其責任與義務，並有能力在日常工作中支持組織安全政策與降低人為錯誤的風險。		
刪除		A.8.2.1			管理階層責任	6
刪除						
刪除						
4.4 管理階層是否有要求員工、承包商及第三方使用者，依照組織已訂定的政策與程序執行安全事宜？						
4.5 對所有員工、承包者及第三方使用者工作職務有關之安全程序及資訊處理設施，是否提供正確使用之認知、教育與訓練？		A.8.2.2			資訊安全認知、教育及訓練	1
刪除						
4.6 是否訂定員工違反組織安全政策與程序之懲處規定？		A.8.2.3			懲處過程	1
		A.8.3		聘僱終止或變更目標： 確保員工、承包商及第三方使用者依規定離職或變更聘僱。		
4.7 是否在與員工、承包商或第三方使用者所訂之契約內規定，在聘僱終止後，與職務有關之責任仍然是有效的？		A.8.3.1			終止責任	1

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
4.8 所有員工、承包商及第三方使用者離職或聘雇終止時，是否依規定繳回其任職期間保管之資訊資產？（包含所有的軟體、公司文件、設備、行動裝置、信用卡、存取卡、軟體、手冊及儲存於電子媒體的資訊等所有其他組織資產）		A.8.3.2			資產之歸還	1
4.9 所有員工、承包商及第三方使用者之聘僱、契約或協議終止時，或因變更而調整時，是否對資訊及資訊處理設施之存取權限迅速予以移除？		A.8.3.3			存取權限之移除	3

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
5.實體及環境安全		A.9	實體及環境安全			
		A.9.1		安全區域 目標： 防止組織的場所及資訊遭未經授權的實體存取、損害及干擾。		
5.1 是否適當使用安全邊界（如圍牆、入口閘門或人員駐守的接待櫃檯等屏障），保護含有資訊與資訊處理設施的區域？		A.9.1.1			實體安全周界	7
5.2 組織管理之資訊處理設施（如通訊服務設施），在實體上是否與第三方管理（如：客戶代管設備）之資訊處理設施區隔？						
刪除		A.9.1.2			實體進入控制措施	5
5.3 具有關鍵或敏感的資訊處理設施之安全區域，是否對於授權進出人員作必要之限制及監督其活動？						
刪除						
5.4 安全區域之進出權限是否定期審查並更新，並於必要時廢止？						
5.5 辦公處所是否實施必要之保護措施？		A.9.1.3			辦公室、房間及設施之保全	4
5.6 是否檢查及評估重要資通訊設備設置地點，鄰近場所之任何安全威脅，如火災、灰塵、水災、震動、化學效應、電力供應、電磁幅射、民間暴動及其他天然或人為災害等可能對設備之危害？		A.9.1.4			防範外部與環境之威脅	3
5.7 是否設計並實施適當的控制措施，以保護敏感資訊處理設施之地點及內部人員通訊錄？						

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
刪除		A.9.1.5			在安全區域內工作	4
5.8 是否嚴禁在電腦機房內使用未經核准之電器或其他物品？						
5.9 備援設備及備份媒體存放位置，是否與主要場地保持安全距離？						
5.10 安全區域是否與易燃物或危險物料保持安全距離，並不宜儲存大量的物資？						
5.11 是否設計並實施適當之控制措施，監督安全區域內之工作，並確保其需知原則？						
5.12 是否訂定未經授權前，禁止拍照、錄影、錄音和其他記錄性設備之規定，如行動裝置上的照相機？						
5.13 無人使用之安全區域是否上鎖並定期檢查？						
5.14 對於收發、裝卸區及其他未經授權人員可進入之作業場所，是否有適當之進出控制措施，並應與資訊處理設施隔離，以避免未經授權的存取？		A.9.1.6			公共進出、收發及裝卸區	6
		A.9.1.7			維運中心之安全 Securing communication centres	8

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
		A.9.1.8			設備機房之安全 Securing telecommunications equipment room	15
		A.9.1.9			隔離操作區之實體安全 Securing physically isolated operation areas	4
		A.9.2		設備安全 目標： 防止資產的遺失、損害、遭竊或洩漏及組織活動的中斷。		
5.15 是否明確訂定資通訊設備之控制措施（包括場外使用之設備，及財產之攜出），以降低資料未經授權存取、遺失及損壞之風險？		A.9.2.1			設備安置與保護	9
5.16 處理敏感資料的資通訊設備或資訊處理設施是否予特別保護並評估其有效性？						
5.17 是否採取適當控制措施，降低潛在實體威脅，如：竊盜、火災、爆裂物、煙害、水災（或水源供應停止）、閃電、溫度、濕度、灰塵、振動、化學效應、電力供應干擾、通信干擾、電磁輻射及蓄意破壞等？						
5.18 電腦作業區（含機房）是否落實執行禁止抽煙及飲食？						
5.19 是否具備環境監控機制，掌握資通訊設備及資訊處理設施之溫度及溼度狀況？						
5.20 是否對於支援性公共設施，如電源供應、水源供應、污水處理、暖氣/通風及空調，設計適當之保護措施，並施行之，確保不受公共設施失效所導致之中斷？		A.9.2.2			支援設施	1

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
5.21 備援電源是否定期檢查並測試，確保能在斷電期間正常運作？						
5.22 電信機線設備（telecommunications lines）、網路佈纜（network cabling）及電源纜線，是否設計適當之安全保護措施，並施行之？		A.9.2.3			佈纜的安全	6
5.23 通信纜線（communications cables）及電源纜線是否接地並隔離，防止互相干擾？						
5.24 設備是否定期且正確的維護保養，確保其可用性及完整性？		A.9.2.4			設備維護	5
5.25 各項設備是否依據供應商建議的間隔與保養手冊，定期檢查並維護？						
5.26 設備之維護與修理，是否由授權之維護人員執行？						
5.27 是否妥適保存所有可疑、實際之系統錯誤資訊，及所有預防性、矯正性之維護紀錄？						
5.28 設備送場外維修，對於儲存在設備內資訊是否訂有安全保護措施？						
5.29 攜出場所外之設備和媒體，是否訂有安全保護措施？		A.9.2.5			場所外設備之安全	4
5.30 行動裝置（設備）是否訂有嚴謹保護措施（如使用授權管理、設通行碼、檔案加密、專人看管）？						
5.31 設備汰除前，是否將機密性、敏感性資料及有版權的軟體予以移除或實施安全覆寫？		A.9.2.6			設備汰除或再使用之安全	1
5.32 含有敏感性資訊之設備汰除後，是否根據風險評鑑決定實體銷毀與否？						
5.33 資訊資產如須攜出場外使用，是否經事前授權，並於攜出場外與歸還時，進行安全查核及紀錄？		A.9.2.7			財產的攜出	4
		A.9.3		其他團體之安全管控 Security under the control of other party		
		A.9.3.1			位於其他服務供應商處之設備 Equipment sited in other carrier's premises	3

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
		A.9.3.2			位於使用者端之設備 Equipment sited in user premises	3
		A.9.3.3			互連之通訊服務 Interconnected telecommunications services	1
6.通訊及作業管理		A.10	通訊及作業管理			

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
		A.10.1		作業程序與責任目標： 確保正確與安全地操作資訊處理設施。		
6.1 資訊處理設施與資通訊設備相關之各項作業程序及活動是否文件化、並適當維護？如電腦開機與關機程序、備份、設備維護、資訊的處理與處理、異常情況之處理、緊急聯絡資訊、重新啓動及復原程序、稽核存底與日誌資訊之維護、電腦機房與郵件處理管理，以及生命財產安全（safey）等。		A.10.1.1			作業程序文件化	8
6.2 資訊處理設施與資通訊設備之變更，是否有正式核准之程序，並向相關人員通報變更細節？		A.10.1.2			變更管理	6
6.3 資訊處理設施與資通訊設備之變更，是否詳實紀錄，並重新進行風險評鑑？						
6.4 資訊處理設施與資通訊設備之變更，是否備有後撤(fallback)程序，包括不成功的變更、意外事故的中止及復原之程序與責任？						
6.5 對於安全要求較高的業務，是否區隔其職務與責任領域？	6.5 對於涉及個人資料蒐集、處理及利用之業務，是否區隔其職務與責任，以授與執行業務所需之最小權限爲原則？	A.10.1.3			職務的區隔	1
6.6 業務資訊資產之使用、資料建檔、系統操作、網路管理、行政管理、系統發展維護、變更管理、安全管理等工作，是否授權由不同的人員執行？	6.6 個人資料之使用、資料建檔、系統操作、網路管理、行政管理、系統發展維護、變更管理、安全管理等工作是否授權由不同的人員執行？					
6.7 是否分隔開發、測試及運作之設施、系統、軟體？						

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
6.8 運作測試系統是否使用不同的使用者剖繪（profile），且功能選單需顯示適切的識別訊息，降低錯誤之風險？		A.10.1.4			開發、測試及運作設施的分隔	6
		A.10.2		第三方服務交付管理 目標： 執行與維持適切之資訊安全等級服務交付，並與第三方服務交付協議一致。		
6.9 是否與第三方服務交付廠商簽訂適當之資訊安全協定，並納入契約條款，包含安全控制措施、服務定義及交付等級，並賦予相關安全管理責任？		A.10.2.1			服務交付	1
6.10 是否規劃必要轉換（資訊、資訊處理設施及其他任何需要移動者）之安全控制措施，並確保轉換期間安全的維護？						
6.11 是否定期對第三方所提供之服務、報告及紀錄等進行適當之監視與審查，並定期執行稽核？		A.10.2.2			第三方服務的監視與審查	5
6.12 第三方提供之服務如有任何異動時，是否重新進行風險評鑑？		A.10.2.3			第三方服務變更之管理	2
		A.10.3		系統規劃與驗收 目標： 使系統失效的風險最小化。		
6.13 資訊處理設施及資通訊設備設置前，是否進行容量規劃及預留安全容量，並於正式運作時，持續監控其容量狀態？		A.10.3.1			容量管理	1
6.14 是否建立新資訊系統、系統升級或新版本之驗收準則，在新資訊系統、系統升級及新版本正式驗收後，才可移轉上線？		A.10.3.2			系統驗收	10

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
		A.10.4		防範惡意碼與行動碼 目標： 保護軟體及資訊的完整性。		
6.15 是否全面使用防毒軟體，並即時更新病毒掃描引擎及病毒碼？	◎	A.10.4.1			防範惡意程式的控制措施	8
6.16 電腦系統及資料儲存媒體是否定期進行惡意程式病毒及後門程式掃描？	◎					
6.17 是否訂定正式政策，禁止使用未經授權的軟體？	◎					
6.18 是否對支援重要營運程序之系統軟體與資料，執行定期審查？若出現任何未經核准的檔案或未經授權的增補修補程式，應進行正式調查。	◎					
6.19 是否訂定使用電子郵件附件及下載之檔案前，檢查有無惡意程式軟體（含病毒、木馬或後門等程式）之程序？	◎					
6.20 是否定義處理電腦病毒、木馬等惡意程式之管理程序與責任，並訓練員工如何通報惡意程式攻擊，及復原程序？	◎					
6.21 是否準備遭惡意程式攻擊後復原之營運持續計畫，並包括所有必要之資料與軟體備份及復原準備工作？	◎					
		A.10.4.2			防範行動碼的控制措施	6
		A.10.5		備份 目標： 維持資訊及資訊處理設施的完整性與可用性。		
6.22 重要資訊及軟體是否定期作備份處理，並定義備份資訊之必要等級？						

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
6.23 備份複本是否定期回復測試，並將回覆程序文件化，確保備份複本之可用性及有效性？		A.10.5.1			資訊備份	8
6.24 重要及機敏資訊之備份程度及頻率，是否反應組織的營運要求？						
6.25 備份資訊是否儲存於遠端地點？距離須足以避免主要場地發生災難時遭波及？						
6.26 備份資訊是否給予適切等級之實體與環境保護，並與主要場域使用一致之標準？						
6.27 主要場域採用之控制措施是否延伸至涵蓋備份作業場域？						
6.28 是否定期檢查及測試復原程序，確保有效性，且能夠在復原程序分配之時間內完成復原運作？						
		A.10.6		網路安全管理 目標： 確保網路資訊及支援基礎建設進行保護。		
刪除		A.10.6.1			網路控制措施	5
6.29 是否訂定網路及網路遠端設備之使用權責及程序？						
6.30 是否使用網路安全防禦設備，並適當的隔離外部網際網路與組織內部網路？						
6.31 組織建立之網路控制措施，是否能反應資訊之機密性、完整性與可用性要求？						
6.32 對於機敏性資訊之傳輸過程，是否採取資訊加密等保護措施？						
6.33 是否訂定確保網路服務連線品質及可用性之保護措施，提供最佳服務？		A.10.6.2			網路服務的安全	3
6.34 是否定期檢討網路安全控管事項之執行？						
6.35 是否定期檢測網路運作環境之安全漏洞？						

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
6.36 是否使用適當之網路安全解決方案？如防火牆、入侵偵測系統？防火牆存取政策（security policy）設定是否適當？						
		A.10.6.3			電信服務交付之安全管理 Security management of telecommunications services delivery.	10
		A.10.6.4			垃圾郵件之反應 Response to spam	1

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
		A.10.6.5			DoS/DDoS攻擊之反應 Response to DoS/DDoS attacks	3
		A.10.7		儲存媒體之處理 目標： 防止資產被未經授權的揭露、修改、移除或破壞，及中斷營運活動。		
6.37 是否建立各種可攜式媒體之操作管理程序，防止文件、電腦媒體（例如：磁帶、磁碟）、輸入或輸出資料及系統文件，遭受未經授權的揭露、修改、移除及破壞？	◎	A.10.7.1			可攜式媒體的管理	6

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
刪除						
6.38 含有敏感性資訊之媒體是否以正式程序加以安全地汰除，例如：焚化或絞碎，或清除資料後由組織內其他應用系統使用？	◎	A.10.7.2			媒體的汰除	5
刪除						
6.39 具機密性或敏感性資訊之媒體是否有安全之保存和報廢程序？	◎					
6.40 機密性、敏感性資訊之儲存或處理是否有安全處理程序及分級標示？	◎	A.10.7.3			資訊處理程序	9
6.41 是否建立資訊的處理及儲存的程序，以保護免於未經授權的揭露或誤用?	◎					
6.42 對應用程式、程序、資料結構及授權過程等說明之系統文件，是否有適當的存取保護措施？		A.10.7.4			系統文件之安全	3
		A.10.8		資訊交換 目標： 維護組織內及外部團體交換資訊及軟體的安全。		
刪除		A.10.8.1			資訊交換政策與程序	15
6.43 是否對於所有形式之資訊交換，訂定適當交換政策、程序及控制措施？	◎					
6.44 是否對高度機敏性資訊在傳輸或儲存中使用加密技術？	◎					
6.45 是否訂定組織與任何外部團體間，交換資訊與軟體之協議？	◎	A.10.8.2			交換協議	11
6.46 重要電腦資訊、媒體（含報表）之運送，是否有安全保護措施及完整監控記錄（含收送人、時間及內容）？	◎	A.10.8.3			輸送中的實體媒體	5

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
6.47 是否訂定適當控制措施，保護含有資訊之媒體，在組織實體邊界外傳送時，不受未經授權的存取、誤用或毀損？	◎					
6.48 採行電子交換之資訊，是否視資訊安全等級，採行識別碼與通行碼管制、電子資訊加密或電子簽章認證等保護措施，確保資訊的機密性、完整性、可用性及符合其他法律要求？	◎	A.10.8.4			電子傳訊	6
6.49 涉及敏感性資訊及機密文件之營運資訊系統，是否提供適當之存取控制與保護？	◎	A.10.8.5			營運資訊系統	10
		A.10.9		電子商務服務 目標： 確保電子商務服務的安全及其安全使用。		
刪除		A.10.9.1			電子商務	13
6.50 是否實施適當控制措施，保護在公眾網路上傳輸且涉及電子商務之資訊，使其不受詐欺行爲、契約爭議及未經授權之揭露與修改？	◎					
刪除		A.10.9.2			線上交易	6
6.51 線上交易服務，是否訂定適當控制措施，防止下列事項：(1)不完整傳輸、(2)誤選路徑、(3)未經授權之訊息修改、揭露及(4)未經授權的訊息複製或重送(replay)等發生？	◎					
6.52 對外開放供公眾取得之資訊，是否訂定保護措施，確保資訊完整性，防止未經授權之修改？		A.10.9.3			公眾可用的資訊	4
		A.10.10		監控 目標： 偵測未經授權的資訊處理活動。		
6.53 是否依據法律要求，如個資法，實施適當之稽核存錄措施，以紀錄使用者活動、異常及資訊安全事故？	◎	A.10.10.1			稽核存錄	12

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
6.54 是否採用適切的存錄與監控設備，記錄資通訊相關活動？	◎	A.10.10.2			監控系統的使用	5
6.55 是否建立適當之控制措施，監控資訊處理設施之使用，及定期審查？	◎					
6.56 各項日誌是否有適當的保護措施，不受竄改與未經授權之存取，並針對留存之通信資訊設定適當之留存期限（例如：會計、帳務、客訴的處理、防止濫用及執法機關的要求）？	◎	A.10.10.3			日誌資訊的保護	3
6.57 是否定期稽查各項作業日誌？	◎					
6.58 是否適當規劃存錄設施與日誌資訊之儲存媒體容量，避免無法記錄事故或覆蓋以往所記錄事故？	◎					
6.59 作業日誌是否留有管理者與操作者所涉及活動之詳細過程，並定期予以審查？	◎	A.10.10.4			管理者與操作者日誌	4
刪除		A.10.10.5			失誤存錄	2
6.60 是否加以存錄由使用者或系統程式所通報之資訊處理或通信系統問題，迅速處理及通報？	◎					
6.61 所有系統鐘訊是否與議定之鐘訊來源校正，以確保時間紀錄正確？	◎	A.10.10.6			鐘訊同步	1
7.存取控制		A.11	存取控制			

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
		A.11.1		存取控制之營運要求目標： 控制資訊的存取。		
7.1 是否根據營運與安全要求，建立、文件化及審查存取控制政策？		A.11.1.1			存取控制政策	16
7.2是否在存取政策文件中明確陳述每個使用者或使用群組之存取控制規則與權限？						
7.3 資訊存取控制政策是否符合相關法律、法規命令及契約規定，如電信法、個資法等？						
		A.11.2		使用者存取管理目標： 確保經授權使用者對資訊系統的存取及防止未經授權的存取。		
刪除		A.11.2.1			使用者註冊	10
7.4 是否對所有資訊系統與服務核准和撤銷存取，訂定適當之使用者註冊與註銷程序？	◎					
7.5 是否於使用者變更角色、調職或離職後，立即移除或封鎖其存取權限？	◎					
7.6 是否維持所有使用者註冊服務、系統或資訊等之正式紀錄？	◎					
7.7 基於系統管理或特殊作業需要，需設定特殊權限時（如系統管理、高階管理者），是否透過正式授權過程，控制特殊權限之配置？	◎	A.11.2.2			特權管理	6
7.8 是否維護所有配置特殊權限之授權過程和紀錄，並於完成授權過程後才授予特殊權限？	◎					
7.9 是否在提供使用者通行碼前，進行身份鑑別程序？	◎					
7.10 是否以安全之程序轉交預設之通行碼給使用者，使用者取得通行碼，確認無誤後，需回應系統管理者？	◎					

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
7.11 軟體安裝完畢後，是否立即更新廠商所預設之通行碼？	◎	A.11.2.3			使用者通行碼管理	8
7.12 是否要求使用者於聘僱任期與條件中，簽署對個人通行碼保密聲明？	◎					
7.13 是否強制要求使用者，初次登入電腦系統後，必須立即更改預設通行碼，或一定期限內未登入，則預設通行碼將失效，必須重新申請建立？	◎					
7.14 是否規定通行碼不得以無保護之型式儲存於電腦系統中？	◎					
7.15 所有使用者存取權限，是否定期檢查（建議每六個月一次、特權者每三個月一次）及任何變更(如升職、降職、調職或聘僱終止等)後審查？	◎	A.11.2.4			使用者存取權限之審查	5
		A.11.3		使用者責任 目標： 防止未經授權的使用者存取、危及或竊盜資訊及資訊處理設施。		
7.16 通行碼長度是否規定須超過6個字元（建議以9個字元位或以上）？	◎	A.11.3.1			通行碼的使用	9
7.17 通行碼是否規定需以大小寫字母、特殊符號及數字組成？	◎					
7.18 通行碼輸入錯誤，是否訂有三次以內之限制？	◎					
7.19 是否定期、依規定期限或使用次數限制，要求變更通行碼，並避免重複或循環使用舊通行碼？	◎					
7.20 是否規定不得在任何自動登入過程中內含通行碼，例如：儲存在巨集或功能鍵中。	◎					
7.21 是否規定避免使用與個人有關資訊（如生日、身分證統一編號、單位簡稱、電話號碼等）當做通行碼？	◎					
7.22 是否避免保留通行碼的紀錄（例如：紙張、軟體檔案或手持裝置）， 除非其能被安全地存放，且該存放方式經過核准？	◎					
7.23 應用系統是否具有作業結束後或在一定期間未操作時即自動登出之保護機制？	◎					
刪除						

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
7.24 是否避免將輸入之通行碼以明文方式顯示在螢幕上？	◎					
7.25是否 對於無人看管之資訊設施有適當保護措施？		A.11.3.2			無人看管之使用者設備	3
7.26 是否訂有桌面淨空及螢幕淨空政策？	◎	A.11.3.3			桌面淨空與螢幕淨空政策	5
刪除						
7.27 主機、伺服器、個人電腦、終端機等電腦設備於不使用、人員離座時是否即刻進行保護措施如關機、登出、設定螢幕保護密碼或是以其他控制措施進行保護？	◎					
7.28 下班後經辦之機密性及敏感性資訊是否妥爲收存？	◎					
7.29 是否訂定適當之控制措施，防止未經授權使用影印機和其他複製設備（例如：掃瞄器、數位相機）？	◎					
7.30 敏感性或機密性資訊文件，是否立即從印表機上取走？	◎					
		A.11.4		網路存取控制 目標： 防止網路服務遭未經授權的存取。		
7.31 網路使用者（含外單位人員）是否取得正式存取授權？		A.11.4.1			網路服務的使用政策	4
7.32 是否於登入作業完成後，顯示前一次登入日期與時間，或提供登入失敗之詳細資訊？	◎	A.11.4.2			外部連線之使用者鑑別	1
7.33 是否限制登入失敗次數超過上限時，需強制延遲一段時間或重新取得授權後才允許再登入？	◎					
7.34 是否訂定網路服務存取安全政策，確保使用者係經特定授權允許存取網路與網路服務？	◎					
7.35 對於外部連線使用者是否進行身份鑑別機制，如密碼技術、硬體符記或詰問/應答（challenge/response）協定等安全技術？	◎					

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
7.36 是否採用自動設備識別方法，鑑別存取敏感或機密資訊之設備，方可允許其存取行為？	◎	A.11.4.3			網路設備識別	1
7.37 對於遠端使用者的存取控制，是否有適當的鑑別機制？		A.11.4.4			遠端診斷與組態埠保護	1
刪除						
7.38 如需採用遠端診斷作業方式，是否訂定診斷埠之存取作業規範（如用金鑰管理及人員身份查驗或稽核等機制）？						
7.39 無線網路之存取及應用，是否訂有嚴謹之鑑別、加密方式及頻率選擇等控制措施？						
7.40 是否依據網路服務需要，區隔出獨立邏輯網域（如組織內部網路或外部網路），每個網域皆有定義的安全邊界，及通訊閘道管制過濾網域間資料之存取（如網路防火牆）？	◎	A.11.4.5			網路區隔	1
刪除		A.11.4.6			網路連線控制	4
7.41 是否針對電子郵件、單雙向檔案傳輸、互動式存取或應用系統之存取時段作必要之限制？	◎					
7.42 是否實施網路路徑控制，以確保電腦連線及資訊流，不會破壞營運應用程式之存取控制政策？		A.11.4.7			網路選路徑控制	1
		A.11.4.8			電信服務商之識別與鑑別 Telecommunications carrier identification and authentication by users.	1
		A.11.5		作業系統存取控制 目標： 防止作業系統遭未經授權的存取。		

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
7.43 是否提供登入程序最小限之系統輔助訊息，避免提供未經授權使用者任何不必要協助？	◎	A.11.5.1			安全之登入程序	9
7.44 是否依據系統機敏度，限制登入失敗次數之上限，並於登入失敗後中斷連線？	◎					
7.45 是否對於異常登入程序，留有紀錄及定期檢視？	◎					
7.46 系統登入或存取重要資訊時，是否對連線過程提供加密之程序與措施？	◎					
7.47 使用者是否採用具有唯一性之識別符號（使用者ID）？	◎	A.11.5.2			使用者識別與鑑別	1
7.48 重要系統使用者，是否採用適切之身分鑑別技術，例如：一次性密碼、智慧卡、符記或生物特徵？	◎					
7.49 是否以保護的形式儲存和傳送通行碼，並告知申請者？通行碼檔案是否和應用系統資料分開存放？		A.11.5.3			通行碼管理系統	9
7.50 使用系統公用程式是否進行授權管制（如最低實務需求的授權）及身分鑑別程序？需要職務區隔時，是否有管制措施不讓具備系統應用程式存取權限的使用者，取得系統公用程式之權限？		A.11.5.4			系統公用程式的使用	9
7.51 是否設定網路會談結束或超過定義的無動作時限後，即中斷連線或關閉設備？	◎	A.11.5.5			會談逾時	1
7.52 對風險高之應用系統，是否限制連線時間，如連線時間限制在正常辦公時間內？	◎	A.11.5.6			連線時間的限制	3

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
		A.11.6		應用系統與資訊存取控制 目標： 防止應用系統中的資訊遭未經授權的存取。		
刪除		A.11.6.1			資訊存取限制	4
7.53 是否訂定使用者及支援人員，對應用系統存取權限之管制措施？	◎					
7.54 處理機密及敏感性資訊，是否採用專屬（隔離）電腦作業環境？	◎	A.11.6.2			敏感性系統的隔離	2
		A.11.7		行動計算與遠距工作 目標： 確保使用行動運算與遠距工作設施時之資訊安全。		
7.55 是否訂定行動運算及通信設備之管理政策（如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求）？	◎	A.11.7.1			行動運算與通信	2
7.56 遠距工作是否得到管理階層授權（如活動政策、計畫及流程等）和施以必要之保護措施？	◎	A.11.7.2			遠距工作	19
7.57 遠距工作活動結束後，是否撤銷相關授權與存取權限及歸還管制設備？	◎					
8.資訊系統獲取、開發及維護		A.12	資訊系統獲取、開發及維護			

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
		A.12.1		資訊系統之安全要求 目標： 確保安全是整體資訊系統的一部分。		
8.1 在規劃應用系統需求時，是否將安全需求納入分析及規格文件中？		A.12.1.1			安全需求之分析與規格	1
		A.12.2		應用系統之正確處理 目標： 防止應用系統中資訊的錯誤、遺失、未經授權的修改或誤用。		
8.2 是否檢查輸入資料，確認其正確性及適切性？		A.12.2.1			輸入資料確認	7
8.3 是否針對輸入錯誤，設計及實作回應程序？						
8.4 應用程式內部處理是否加入確認查核（validation check），偵測可能經由處理錯誤或故意行爲之任何資訊毀損，並提供適當程式從失效中復原，確保資料之正確處理？		A.12.2.2			內部處理的控制措施	12
8.5 應用系統是否使用密碼技術，鑑別與保護其訊息之完整性？		A.12.2.3			訊息完整性	1
8.6 輸出資訊是否具合理性查核及一致性控制計數（reconciliation control count），確保所有資料都已合理處理？		A.12.2.4			輸出資料確認	6
8.7 是否設計與實作輸出確認測試與回應之程序？						
8.8 是否設計並實作資料輸出確認過程之活動日誌，並定義所有涉及資料輸出過程人員之責任？						
		A.12.3		密碼控制措施 目標： 藉由密碼方式以保護資訊的機密性、鑑別性或完整性。		

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
8.9 是否基於風險評鑑結果，識別所需的保護等級，設計所需加解密演算法之型式、強度及品質？		A.12.3.1			使用密碼控制措施的政策	7
8.10 是否基於風險評鑑結果管理密碼金鑰，並發展適當之控制措施？		A.12.3.2			金鑰管理	11
		A.12.4		系統檔案之安全目標： 確保系統檔案的安全。		
8.11 作業系統升級前，是否考量營運要求及該版本之安全性？						
8.12 處理作業系統軟體更新之人員，是否經管理階層授權？						
8.13 是否限定由經過訓練合格之管理人員，才可執行應用程式可執行碼更新作業？						
8.14 是否使用組態控制系統，以保持對所有已實作的軟體與系統文件之控制，且維護所有變更紀錄？		A.12.4.1			作業軟體之控制	8
8.15 是否避免以真實資訊進行測試作業？		A.12.4.2			系統測試資料之保護	4
8.16 存取程式原始碼（program source code），是否訂有適當之控制措施，並留存稽核日誌？		A.12.4.3			程式源碼之存取控制	7

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
刪除		A.12.4.3			程式源碼之存取控制	7
		A.12.5		開發及支援處理之安全 目標： 維持應用系統軟體及資訊的安全。		
8.17 是否建立變更應用系統之管制程序？		A.12.5.1			變更控制程序	11
8.18 應用系統變更後，是否立即更新系統文件？						
8.19 作業系統變更後，是否對應用系統作技術性審查？		A.12.5.2			作業系統變更後的應用系統技術審查	4
8.20 作業系統變更後，是否主動公告異動範圍、時間及可能的影響？						
8.21 作業系統變更後，是否檢查其相關控管措施與程序仍然有效？						
刪除						
8.22 是否僅限於必要的範圍，變更套裝軟體之，並嚴格管制所有變更？		A.12.5.3			套裝軟體變更的限制	4
8.23 是否檢查組織內可能之隱匿通道(covert channel)，降低資訊洩漏的風險？		A.12.5.4			資料洩漏	5
8.24 委外開發之系統上線前，是否偵測有無惡意程式存在？		A.12.5.5			委外軟體開發	6
8.25 委外開發合約中，是否規範著作權之歸屬？						
8.26 訂約時，是否簽訂安全履行條款與相關罰則？						
		A.12.6		技術脆弱性管理 目標： 降低利用已公佈技術弱點所導致的風險。		
8.27 是否及時取得使用中通訊傳播系統之技術脆弱性資訊，並定期執行各項系統漏洞修補程式？		A.12.6.1			技術脆弱性控制	10
8.28 進行系統修補前，是否先作系統影響評估與測試，再採取必要措施？						

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
9.資訊安全事故管理		A.13	資訊安全 事故管理			
		A.13.1		通報資訊安全之事件及弱點 目標： 確保與資訊系統相關的資訊安全事件及弱點，能夠及時傳達並矯正。		

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
9.1 是否建立資安事故（含安全漏洞、系統弱點、病毒、非法入侵及系統異常）之正式通報應變程序？	◎	A.13.1.1			通報資訊安全事件	4
9.2 事故回應小組是否建立單一聯繫窗口，授權在處理事故時採取立即之決定，並與外部團體（例如：執法機關、政府緊急應變中心、客戶、商業夥伴）建立聯繫管道？	◎					
9.3 資訊安全事故處理過程，是否留有完整記錄，如有必要，應經由直接發送電子郵件及/或網站首頁，及時回報事故給相關客戶？	◎					
9.4 是否建立資訊安全事故通報之聯絡點，並確保全組織都知道該聯絡點，隨時可聯繫，能夠有充分與及時的回應？	◎					
9.5 機關員工及外部使用者是否知悉資安事故通報及處理程序並依規定辦理?		A.13.1.2			通報安全弱點	1
9.6 是否要求資訊系統與服務的所有員工、承包商及第三方使用者，注意並通報任何觀察到或可疑的系統或服務之安全弱點？						
		A.13.2		資訊安全事故之管理及改進 目標： 確保資訊安全事故的管理採用一致及有效的作法。		
9.7 是否依不同型式之資訊安全事故，建立資安事故管理責任及應變程序？		A.13.2.1			責任與程序	4
刪除						
9.8 是否建立資安事件或事故等事後管理會議，以協助單位能從資安事件及事故中學習？						

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
9.9 是否擬定營運中斷後之各項風險處理優先順序或處理準則（含處理順序說明、最低營運水準定義）？						
9.10 是否建立資安事故管理機制，如記錄事故型式、處理方法、處理成本及矯正預防措施？		A.13.2.2			從資訊安全事故中學習	1
9.11 是否已建立及使用各項指標，以協助偵測安全事故，並預防安全事故？						
9.12 已發生之資訊安全事故，是否在安全政策審查過程中納入考量？						
9.13 資安事故中相關證據資料是否有適當保護措施，以符合證據能力之要求，作爲問題分析及法律必要依據？		A.13.2.3			證據的收集	4
10.營運持續管理		A.14	營運持續管理			
		A.14.1		營運持續管理之資訊安全觀點 目標： 爲防範營運活動中斷，保護重要營運過程不受重大資訊系統失效或災害的影響，並確保及時重新開始(resumption)。		
10.1 是否發展與實作營運持續計畫，以因應組織營運持續所需的資訊安全要求？		A.14.1.1			資訊安全納入營運持續管理過程	10
10.2 是否針對所有營運過程，可能造成營運中斷之機率及衝擊進行風險評鑑？						

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
刪除		A.14.1.2			營運持續與風險評鑑	1
10.3 是否識別營運持續過程中之關鍵資通訊設備及資訊處理設施？						
10.4 營運持續計畫是否以人員安全爲優先，並保護資通訊設備和組織財產？		A.14.1.3			發展與實作包括資訊安全的持續計畫	7
刪除						
10.5 是否訂定營運持續計畫（含啓動條件、參與人員、緊急程序、後撤程序、回復程序、維護時程、教育訓練、職責說明、所須資源、往來單位之應變規劃及合約適當性等）？						
10.6 是否維持營運持續計畫之單一框架， 以確保所有計畫有一致性， 持續一致地因應資訊安全要求， 並識別測試與維護的優先順序？		A.14.1.4			營運持續計畫框架	9
刪除		A.14.1.5			營運持續計畫的測試、維護及重新評鑑	6
10.7 營運持續計畫（含緊急應變處理程序）是否配合業務、組織及人員之變更而更新？						
10.8 營運持續計畫是否定期完整測試、演練並予更新維護?						
11.遵循性		A.15	遵循性			
		A.15.1		符合法規要求 目標： 避免違反任何法律、法規命令、行政規則或契約義務及任何安全要求。		
11.1 是否確保所有通訊系統與組織均不違反任何法律、法規命令、行政規則、契約義務及相關安全要求？		A.15.1.1			識別適用之法條	1
11.2 軟體取得（含自行開發、委外開發、購置或租用）等可能涉及智慧財產權規定，是否符合法律、法規命令及契約的要求？						

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
11.3 是否公布智慧財產權遵循政策，定義軟體與資訊產品的合法使用，並告知違反政策人員將遭懲處？		A.15.1.2			智慧財產權	13

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
11.4 是否維護使用版權、原版碟片、手冊等所有權之證明和證據，並定期檢核是否只安裝經授權之軟體與有使用版權之產品？						
11.5 組織重要紀錄（如資料庫紀錄、系統日誌、操作日誌、稽核日誌）是否依安全等級加以保護及儲存（如檔案加密或數位簽章）？		A.15.1.3			組織紀錄的保護	4
11.6 稽核後是否產生稽核報告，並追踪改善情形（包括稽核發現之摘要、稽核區域、缺失說明及改進建議等）？						
11.7 組織中對於所經管或處理之資訊，涉及個人隱私及個人資料之保護是否有適當之保護機制？		A.15.1.4			個人資訊的資料保護與隱私	1
11.8 是否發展和實作符合法律、法規及若適用的契約條文所要求的資料保護與隱私政策？						
11.9 是否依據個人資料保護法擬定個人資料檔案安全維護計畫及業務終止個人資料處理方法？						
11.10 是否有監視設備或其他可偵測未經授權使用之設備，防止資訊設施被不當使用？		A.15.1.5			防止資訊處理設施的誤用	1
11.11 管理人員是否定期審查其責任範圍內之資訊處理設施與其安全政策、標準及符合其他相關安全要求？						
		A.15.1.6			密碼控制措施的規定	4
		A.15.1.7			Non-disclosure of communications	10
		A.15.1.8			Essential communications	18
		A.15.1.9			Legality of emergency actions	1
		A.15.2		符合安全政策、標準及技術規範 目標： 確保系統符合組織的安全政策及標準。		
11.12 組織訂定之安全程序，是否確保相關人員能正確執行？		A.15.2.1			安全政策與標準的符合	4

附件9 通訊傳播事業個資保護控制措施內部稽核表

圖例詳如：最後一頁下方

資安管理內部稽核表 (B級) (修訂建議)	個資保護 控制措施	區分	安全領域	安全目標	CNS 27002+ISO 27011 控制措施	實作指引數量
11.13 資訊系統是否定期進行安全技術符合性檢查（如滲透測試或系統弱點檢測）？	◎	A.15.2.2			技術符合之查核	1
11.14 技術遵循性之查核人員是否經過訓練，並作事前工作分配？	◎					
11.15 技術遵循性檢查是否由合格資安技術單位執行？	◎					
11.16 技術遵循性查核時之存取行爲，是否作監控，並適當保存紀錄？	◎					
11.17 技術遵循性查核結果是否文件化？	◎					
		A.15.3		資訊系統稽核考量目標： 使資訊系統稽核處理的有效性最大化，並使其產生或受到之干擾最小化。		
11.18 是否訂定資訊安全內部稽核計畫（含稽核目標、範圍、時間、程序、人員）？	◎	A.15.3.1			資訊系統稽核控制	9
11.19 是否定期辦理資訊安全內部稽核？	◎					
11.20 內部稽核範圍是否含括資通系統、供應商、資產負責人、使用者和管理階層？	◎					
11.21 是否有保護資訊系統稽核工具之存取，防止可能誤用或破解之措施？		A.15.3.2			資訊系統稽核工具的保護	1
277	90	合計	11	40	146	803
圖例：	安全領域	安全目標	控制措施/ 實作指引	27011新增 控制措施	27011 補充措施	未納入 控制措施

附件 10　　第 1 場次資通安全管理機制座談會會議紀錄

國家通訊傳播委員會

100 年度「資訊安全管理系統研究」計畫

一、會議名稱：資通安全管理機制座談會(第一類電信)

二、時間：100 年 5 月 10 日(二)10：00

三、地點：中華軟協大會議室(北市承德路二段 239 號 6 樓)

四、主席：協同計畫主持人鍾榮翰顧問　　記錄：鍾如郁

五、出席人員： 詳見簽到表

六、討論意見綜整：

1. 個資法施行細則即將訂頒實施，一旦發生個資外洩，除了損害賠償之外，行政機關很快就會行使行政檢查權，業界應有策略性的作法以為因應。
2. 重點應放在風險評鑑，除了 ISO27005 之外可能還不夠，可參考 BS25999，先做 BIA 鑑別出核心業務，核心業務需要哪些硬體、軟體來支援。再作風險評鑑，會比較完整。
3. 企業應從風險評鑑著手，首先鑑別出核心業務，接著識別出核心業務有哪些風險存在，可能會受到天災或人為損害影響，造成營運無法持續運作。識別出風險後，才能將企業的資源作有效的運用。識別的方法已非常普遍，重點在於能否落實執行。
4. 風險評鑑、風險評鑑是很重要的輸入項，但在體系的實施或系統導入的執行面，以過往的經驗來說，關注的層面主要還是在管理系統，不管是從資料保護或個資法的角度來看，檢查的環節裡針對技術面的實施並未有很落實的描述，或者在檢測的部分並未有很清楚的標準被定義出來。建議可在本次的研究中把技術面的要求作比較實質的描述。以電信業來說，電信機房是很重要的關鍵設備，套用 ISO27001 的規定，只會告訴我們實體設備應有門禁，但到底需要什麼樣的門禁？機房座落的位置應在何處？這些部分都是管理系統中未加以描述的。這些實體安全與

邏輯安全若沒有把真正的強度加進來的話，執行時不會特別關注，在檢查的時候也看不到，但最有可能出問題的卻是在這個部分。以 SONY 事件為例，是技術上的失能，是系統本身安全機制強度不夠，發生的是系統性的崩潰。企業無法承受的是系統化的錯誤，系統化的錯誤大多來自於技術失能，但目前大部分的規範或標準，在技術上的描述都不夠深入、明確，讓業者只能自行摸索，這部分仍有改善的空間。

5. 臺灣推動 ISMS 的進程，目的事業主管機關扮演很重要的角色，若目的事業主管機關有所要求，業者自然會配合。以衛生署為例，去年度補助醫院導入 ISMS，許多醫院即陸續通過 ISMS 的認證。就執行面的有效性來看，第一類電信業者會考慮得比較周全，不像某些政府機關是為了通過而通過。政府機關目前的作法，建議先針對資訊系統做分類分級，篩選出重要的資訊系統，找出系統間的關聯，接著作風險評鑑，再進行風險處理。

6. 符合標準並不能免除法律責任。

7. 企業或機關導入 ISMS 的動機多來自於主管機關的要求，若只有外部的力量，通常會做得心不甘情不願，多半選擇最小範圍導入，敷衍了事。若能演化為內部的力量，逐漸形成企業文化，將能發揮最大成效。

8. 國內導入 ISMS 最常見的狀況：多侷限在 IT 單位，核心作業流程都未納入。組織內真正重要的核心業務是否被界定出來？還是只做自己想做的部分？為何大部分的機關或企業只選擇某一範圍執行導入，最主要的原因仍是預算考量與需投入的資源多寡，造成機關或企業卻步。建議仍應從全組織的觀點做整體資安的考量，才會較有成效。

9. 企業內部單位組織太多，初期計畫全面實施導入，無論是否為核心業務均導入 ISMS，但經評估後發現全公司導入是做不到的。採取的策略是：有上級主管機關或業務要求的優先執行導入，至少先符合法令的要求。近兩年 NCC 提出資安管理規範後，業界也意識到導入 ISMS 為趨勢，除了外部的要求之外，內部也有自省，並不只是單純由於 NCC 的要求。由前端的訂單系統、帳務系統逐步實施。去年 NCC 加入 ISO27011

的要求之後，針對電信網路的部分也開始執行 ISMS 的導入。相關資源的獲得，來自總公司的要求、與其他同業的比較或主管的想法，或者接觸到某些活動(例如 CIIP)後，意識到有此需求。以政策角度，每年初會訂定相關指標，檢視業務執行是否達到水準。

10. 資通安全管理要點納入 ISO27011 後，稽查表訂定要考慮到臺灣的現況，全面移植國外的制度不見得適用。在個資議題開始發酵後，通過 ISO27000 系列的認證不代表個資的防護 OK，應如何確認個資防護符合規定？建議可參考 NIST SP800-122 這份文件，可提供個資安全維護作為策略性的明確作法，清楚列出個資保護的控制措施。
11. 導入 ISMS 並非因為主管機關的要求，而是意識到重要性而主動進行，分期逐步擴大範圍。尤其在社會期待與主管機關的壓力下，特別注重資通安全。衛生署編列預算補助署立醫院通過 ISMS，電信產業是否也能獲得主管機關的補助？
12. 如何證明 ISMS 的有效性量測，目前朝向由 CIA 的面向來考量，納入個資保護的所有流程，包含業務、IT 都納入，防止個資被竊取與不當使用。並且由防禦系統與偵測系統中獲得數據，避免人為統計干擾結果。
13. 外商投資的公司，總公司已有 ISO 相關辦法，但並未移植到臺灣分公司，臺灣分公司只有機房，網管中心或是客戶資料都存在總公司，NCC 要求臺灣分公司進行 ISO 機制的認證、資安管理或安全機制，執行上會有困難。若 NCC 有所要求，希望待電信法修正通過後，取得法律授權，在有法源依據、明確法規、明確施行細則及罰則的情況下，並正式行文，外商總公司即會配合辦理。目前外商公司的態度則是觀望中。
14. 瓦斯公司僅因為瓦斯幹管中埋了光纖，被列為第一類電信業者，電纜出租用戶數很少，若主管機關持續要求全面導入 ISMS，在無法負荷的情況下，可能考慮放棄此業務。
15. 資通安全等級的自我評估，如何確認評估符合事實？因評估構面不夠廣、法令適用不夠完善，建議適度調整。
16. ISO27011 驗證的相關疑義，有必要形成共同見解，建議適時釐清，以

符合產業的需求。

17. 業者所提報的自評資料，NCC 並未有適時的意見回饋，目前業者只能根據自我認知的作業方式，自行摸索。建議後續可透過座談方式，提供更多資訊，以利業者配合。

18. 主管機關訂定績效的量測指標時必須很小心，數據若不能利用系統自動化統計，人工計算需耗費太多工時，反而沒有績效。ISO27004、ISO27005 強調控制措施的有效性不是由單一的措施來看，是由安全目標的角度綜整出一個指標。

19. 建議 NCC 不需訂定可用率的指標，只需要求業者提供安全、可靠的服務，市場自然會淘汰無法達到的業者。

20. 針對 SCOPE，NCC 是否有明確範圍？基地台是否包括在內？另有關驗證天數，ISO27001 是根據 ISO27006 作驗證天數的換算，目前與 NCC、TAF 達的共識是將所有驗證天數的三分之一加驗 ISO27011，但小數點後是否進位？也是驗證公司關心的重點。建議比照 ISO27006，針對驗證的範圍，訂定人天，驗證公司才會有遵循的標準，業者也不會遇到諮詢不同顧問公司得到不同答案的窘況。

21. NCC 要求執行 ISO27011 驗證時，稽核員的資格應有通訊產業的背景，特別是首次執行時，NCC 均會參與，應不致於發生顧問公司不瞭解相關作法的情況。

22. ISO27004，根據完整的架構，訂出適當的目標，因此不同類型的產業會訂出不同的目標，應不會發生強制用單一目標要求所有產業適用的情況。

七、散會（中午 12 點 00 分）

附件 11　　第 2 場次資通安全管理機制座談會會議紀錄

國家通訊傳播委員會

100 年度「資訊安全管理系統研究」計畫

一、會議名稱：資通安全管理機制座談會(第二類電信)

二、時間：100 年 5 月 10 日(二)14：00

三、地點：中華軟協大會議室(北市承德路二段 239 號 6 樓)

四、主席：協同計畫主持人鍾榮翰顧問　　記錄：鍾如郁

五、出席人員：　詳見簽到表

六、討論意見綜整：

1. 對服務業來說，信賴度最重要。推動制度時，人才流動最令企業頭痛，制度建立過程中，若沒有透過國際標準以第三者的角度、以標準程序加以驗證，球員兼裁判，無法客觀地評估此機制是確實可行的。附加價值則是同仁因建立制度而產生信心，也因建立此機制而趨向專業化，透過此機制也可檢視員工是不是都做了對的事。
2. 資安人人有責，而不只是技術部門的責任。導入 ISO 就像為企業作體檢，知道自己的強處與弱點之後，面對挑戰時，會比較清楚因應之道。不是為 ISO 而 ISO，而是為了要合理化整個過程，跨國經營時，與其他國家仍能有共通語言。ISMS 做好，會有許多附加價值，例如參加政府標案、拿行銷科技獎，這些都是必要條件。
3. 我們看這些國際標準就像許多官樣文章，但在實務上，尤其是風險管理，BS25999 反而比較好。它是由企業衝擊分析再到風險評鑑，原來的目的是要建立一套 BCP 的關聯。從業務流程中分析，才會比較清楚問題出在哪裡。
4. 不管要不要通過認證，安全機制有它的好處，從安全防護的角度來看，不外乎三個階段：嚇阻、阻擋、拖延，有系統化的結構，至少在嚇阻上會發揮很大的作用，如果能取得證書當然更好。對於 attacker 來講，不會故意去挑很難侵入的公司，柿子挑軟的吃，若有相關系統、流程，控

管機制已經存在，無論對內或對外，都能發揮嚇阻作用。阻擋則是指確實引入了哪些安全機制，不管多好的機制都有被破解的風險，所使用的機制能否拖延入侵，爭取到足夠的時間建立補救措施。以電信業來說，目前常用的都是 ISO27000 系列，重點放在資訊安全，並未在製造流程上著墨；BS25999 則跳脫了 IT 的範疇，由組織的角度來看營運持續。建議本計畫案應適度呈現其他相關的電信標準，例如美國的電信機房建設標準等，會更完備。

5. 資訊安全不要悶著頭做，可以尋求很多的外部資源協助。目的事業主管機關對下級單位的行政檢查權是很重要的作為，其依據就是資通安全管理作業要點與手冊，業者應該認真研究這些文件並有充分的瞭解，畢竟官方標準仍是最必要遵循的。
6. 實務上常見：通過 ISO27001 認證卻依然出現資安問題，進一步檢討後，發現發生問題的全都是在驗證範圍之外，表示驗證範圍的劃定大有問題，並未納入核心業務與作業流程。
7. task force 一定要有相關部門參與，發生風險異常時能否承擔責任，如果不行，有告知主管的義務。
8. 民法、刑法中早就對個資保護有相關規定，只是大家都不習慣，個資法的通過對於企業主管來說是很大的危機，但若做得好，危機就可以轉化成商機。
9. 客戶帳務資料是目前因應個資保護最大的問題，以往曾將大量資料開放給經銷商運用，發生過系統被入侵、資料被竊取的資安事件，之後則進行實體切割，以杜絕類似事件。第二類電信事業必須快速因應環境的變化，個資法通過後，為維持企業的持續運作，需要建置一套更完整的機制。
10. 總公司已通過 ISO27001，但臺灣分公司並未納入，未來希望透過政策推動，訂出明確的施行細則讓業者有所遵循。
11. 臺灣分公司雖有機房，但客戶資料都存在國外的總部，主要客戶為企業用戶，哪些資料屬於個資保護範疇？可參考「電腦處理個人資料保護法」

附件中有關個人資料「識別類」的說明。相關保護措施可參考 NIST SP800-122 與 Europe Privacy Standard，完備個資保護之後，再藉由 ISO27000 系列加強安全的控制措施。

12. 個資不准移往境外的規定，是所有資料都不可以，還是只有敏感資料？個人資料的國際傳輸規定應由主管機關訂定，至於 NCC 內部權責如何分工，需再與 NCC 確認。
13. 經銷商與 OEM 所使用的電腦設備各有其架構，如何納入加以規範？
14. 客戶個資保存在集團內部另一部門，委託機關與受委託機關的責任如何釐清？
15. 多媒體複合平台，介接各家廠商，讓他們提供服務，在介接過程中，自然會有大量申辦證件個資在其中流通，目前雖有相關資安防範機制，但萬一發生個資外洩情況，如何舉證釐清責任歸屬？應在與廠商洽談合約時加以規範。按理說，廠商應該要配合平台的相關規範，但目前的情況卻是以營利為優先，平台反過來配合業者的需求，技術部門雖然想要盡力防範，卻未能獲得主管支持。
16. 組織內的資訊部門，可引進外部資源，經由資安顧問的協助，與高階主管溝通，爭取支持。
17. 資訊應用不能悖離安全的原則，若沒有安全支持，就會喪失使用者的信賴。資安不能等到事件發生才做，也不需等到主管機關明文規定才做，目前已是很好的時機點，企業應開始投入這方面的工作。獲益的不會只有企業，個人也會有收穫，進而形成良好的企業文化。

七、散會（下午 3 點 45 分）

附件 12　　第 3 場次資通安全管理機制座談會會議紀錄

國家通訊傳播委員會

100 年度「資訊安全管理系統研究」計畫

一、會議名稱：資通安全管理機制座談會(傳播事業)

二、時間：100 年 5 月 12 日(二)10：00

三、地點：中華軟協大會議室(北市承德路二段 239 號 6 樓)

四、主席：協同計畫主持人鍾榮翰顧問　　記錄：鍾如郁

五、出席人員： 詳見簽到表

六、討論意見綜整：

1. 傳播事業規模落差很大，CIA 中著重的是可用性，特別是線路的穩定性與內容的傳遞，關乎其營運能否持續，目前都已做得非常好，本計畫的重點應在於如何透過有效性量測加以檢驗。
2. 目前的資通安全管理作業要點與手冊若要適用於傳播業，恐怕會遇上難以解讀的困境，建議修訂時應將電信業與傳播業分流，訂定適合其產業特性的參考指南。
3. NCC 打算引進國際標準與目前業者的成果做比對，是很好的概念，若發現有不足處再予以補強。
4. 有關風險評鑑的作法，目前高階風險評鑑作法的六個構面，是很適當的，假如發生資安事件，會有多少的財務損失，主管對於這樣的議題通常會很重視，後勤支援單位對企業營運是否有效果？ISO27004 有效性量測很重要，藉由這方面的評估提醒主管資安的重要性，若沒做好，對於營運產生影響，會產生更大損失。本計畫建議應協助業者將業務的需求（主管的需求）轉化為資安的需求。量測目標值與結果的具體化，是後續要加強的地方。
5. 建議後續修訂資通安全管理作業要點與手冊時，能將 ISO27011 檢查表內容中相關名詞解釋增訂進來，讓名詞的定義能有一致性。
6. 有關範圍的部分，大家談到通信傳播業的匯流與分流，目前電信業已有

ISO27011，傳播業又要再訂一個標準，MOD 被歸在電信業，可是又有傳播業的色彩，是否也要適用？第二類電信業者經營 VOD，被歸為電信業，是否也要適用傳播業的規定？傳播業者取得電信執照的，要如何適用？執行稽核時是一家公司去 2 次？還是一次去看 2 份報告？

7. 有關量測指標，建議適當融入 ISO27000 系列，ISO27011 從客戶服務等級協定(SLA)開始，NCC 訂出很多的定型化契約，規範業者與客戶之間的關係，以往 ISO27001 的框架並無法落實這部分的管理，納入 ISO27011 後可加強服務的落實。
8. ISO27001 對於事件與事故有清楚的定義，對傳播業者來說，強調的是服務，可納入 ISO20000 系列對事件的定義，包括客戶來電詢問，都會影響服務的品質，都可包含在 ISO20000 系列的事故。資訊安全管理系統中納入與可用性(Availability) 有關的部分，對於傳播業者會比較有幫助，因產業的特性，較少發生與機密性有關的事故，反而常遇到與服務(可用性)相關的事故。
9. 如果不以取得 ISO 認證為前提，主管機關要如何評估業者執行導入的有效性？解讀標準、條文、作業程序、表單種種工作搞得人仰馬翻，最後卻沒有幾個人回答得出公司的機密資料是什麼，程序與證據的有效性要如何做判斷？即使都能回答清楚，是否就能論定其為有效？或者只要在驗證時看起來該具備的都有就發證書，只要不出事大家都沒事，如此是否值得投入這麼多的資源？如果能夠加上一些標準，即使不作認證，仍然能夠評估其有效性，也比較能夠說服主管，資安工作是值得長期投資的。
10. ISO27000 系列比較高階、比較抽象，執行層面的東西建議參考 BS25999 的營運衝擊分析，可以判斷出業務流程，風險評估也會比較準確，因此，營運持續管理才是傳播業真正重要的議題。
11. 傳播事業的經營狀況正在改變，經營方式在數位時代是會改變的，數位電視全面普及之後，收視率的調查業者是否還會存在？答案當然是否定的，數位電視與顧客之間的互動密切，能夠直接掌握顧客行為時，就能

主導廣告預算的分配。為了因應數位時代的來臨，傳播業者要儘快做出風險評估，才能有所因應。

12. 業者導入控管機制多半從執行面著眼，是為了讓工作更輕鬆，控管機制一定會有數據，呈現在主管眼前就是績效，而非真正考慮到制度面。平時主要配合會計師簽證、查核時的要求，若主管機關有要求，業者自然會調整腳步來配合。

13. 頻道代理商代理境外頻道，主要的客戶就是各有線電視台，擁有的個資數量很少，受到個資法的影響也很小。

14. 參加電視台活動的抽獎明信片包含民眾大量個資，大部分都由協力廠商負責處理，因個資法明文規定委託機關與受委託機關都有責任，因此與協力廠商的合約內容要求必須明確，應訂定處理的流程，包括如何銷毀，且委託機關也需做到相關查核，萬一有外洩情事，才能舉證無故意或無過失。對於個資的合理運用，資訊單位屬於行政後勤支援單位，沒有能力單獨處理，一定要由業務單位主導，甚至應加入法務單位共同討論，個資隱私長應由業務單位擔任，IT 單位建議只擔任資訊安全長。

15. IT 部門在公司的位階較低，只是系統的維運單位，在內部無主導權，提出資安相關預算時，很難向主管說明會對公司的營運有何影響、不做會造成什麼損失，既然會減少營收，對主管的經營績效又沒有直接助益，除非高階主管有 IT 背景，否則多半不會支持。

16. 由營運持續的觀點來看，傳播業反而做得更好，目前 NCC 雖然是由資安的角度切入，但資安不應只限縮在資訊系統，更不是只有機密資料，可用性涵蓋在資安範圍內，如何協助主管重視，並取得足夠的資源，彰顯資訊單位的績效，是當務之急。

七、散會（上午 11 點 50 分）

附件 13　　第 4 場次資通安全管理機制座談會會議紀錄

國家通訊傳播委員會

100 年度「資訊安全管理系統研究」計畫

一、會議名稱：資通安全管理機制座談會(第一類電信)

二、時間：100 年 8 月 12 日(二)10：00

三、地點：中華軟協大會議室(北市承德路二段 239 號 6 樓)

四、主席：計畫主持人張國鴻秘書長　　記錄：鍾如郁

五、出席人員：詳見簽到表

六、討論意見綜整：

1. 安全管理手冊中有關通報的部分提到「事件」一詞，行政院國家資通安全會報已將「事件」改為「事故」。
2. 三個影響構面，「資料保護受到損害」、「影響業務運作」及「法規遵循」，附件 1 與附件 2 出現的是「違反法規遵循」，兩者是不是同一件事？
3. 簡報 p.21 有關結構方程模式修正，在規劃階段「法規遵循」的部分是 0.74，但在維持階段的「法律影響」落到 0.67，兩者的關聯性為何？
4. 簡報 p.69 定義安全等級分為 A 級與 B 級，由行政院國家資通安全會報的角度來看，機關應分為 A、B、C、D 四級，通訊傳播事業分為 A、B 兩級，會不會產生混淆的現象？
5. 本研究最主要的目的主要是導出管理要點要做的部分，但兩者的聯結看起來是薄弱的。資通訊從業廠商的資安認知水平到何程度，需要如何加強，這是一種研究方式。如果廠商要導入 ISMS，有哪些重要因素需要被找出來。資訊安全文化建構來自於資安治理，有強烈的連帶關係。步驟的實施過程，談得比較少。國家資通安全發展方案中並未將資安治理的評估表清楚的揭露，但希望從成熟度的角度去看組織資安治理的成熟度，再去推動資訊安全的行動方案。這兩部分我是建議可以再做一些思考。如果從這個角度來看，資訊與資訊系統分類分級，以及 ISMS 所要訴求的，在某種層次上是不一樣的。或許看起來管理要點是著重在

ISMS，所以會有從部門別、系統別、業務別的角度去切入，可是最後連帶的，不管用何種分類方式，最後還是要定義出組織內的資訊與資訊系統的分級。建議步驟的部分，不管用何種範圍定義別去導入，都不可忽略資訊與資訊系統分類分級以及資訊治理兩部分。

6. 目前有幾家業者已申請 ISO27011 稽核的驗證服務，年底會陸續完成。管理作業要點修正條文對照表 p.3 第 5 條提到:「通訊、傳播事業申請『開放赴大陸投資業務項目』前，應將其資通安全管理之實施作業範圍報經 NCC 核准後，就核准之作業範圍申請驗證。」要提醒業者的是：在申請範圍前，以往在申請 ISO27011 時，申請方與驗證方就 ISO27006 與 ISO27011 相關的規定要求去作範圍的制定，這部分會有主管機關的意見要表達，主管機關會希望期程之內，資源上或技術上沒有困難的情況下，逐步 scope expand 的計畫，會裡面會要求要包含到個資、核心業務等等。
7. 簡報內有建議：針對 A 級組織，未來在進行 ISMS 建置或設計時，考慮採用 BCM 裡面的專業作業 BIA(營運衝擊分析)。目前在增項稽核查檢表裡面並未針對 BIA 細部要求查檢的項目，未來這部分若列在 A 級的建議要求之內，增項稽核查檢表裡面對應的控制措施也要發展出來，提供申請單位或驗證單位作參考。
8. 目前分為 A、B 級，手冊上的規定，A 級沒問題，基本上都會通過驗證，B 級自行導入會有困難，也不太可能申請驗證。以我接觸的經驗，尤其第二類電信，單位規模大概都在 50 人以下，甚至 20 人以下。在這種情況下，手冊上的定義是 B 級單位也要做內部稽核，查檢表是否同時有是否符合與不適用三種選項，NCC 是否可以同意其自行勾選不適用？假如不是的話，在執行上，對 B 級單位還是會有蠻大的困難。因為有很多項目，B 級單位不是沒有就是做不到。設計一個表讓業者自行勾選，這個表的意義不大。若是回到主計處的內部查檢表的話，是不能選擇「不適用」的，要嘛就是做得很好，要嘛就是做得不盡完善，可是並沒有「不適用」的選項。所以，是不是可以考慮在執行上，被歸到 B 級的單位，

在能力上已無法自行建立 ISMS 體系，在你們的幫助之下，能夠有一個合適的查檢表，他們就做這些事就好，差別只是做得完善或不盡完善。

9. 業界選擇認證時的有效性可以將資訊安全的精神落實在組織內部，如何將 NCC 的要求對應到各個業務單位能將業務鑑別出來，最後能落實到核心業務，將其分為 A、B 級。選擇認證範圍時，其核心業務是否有效，查檢表不一定鑑別得出來，NCC 站在主管機關的角度上，應有一些方式與能力判別每一個不同的業者各有其不同的核心業務，對應後續送審的驗證範圍可以有個跟核心業務的關聯。

10. 基於輔導、指導的角色，中華電信非常感謝，簡報 p.79 提到行政檢查，以中華電信的意見，資安認知很重要，但資安文化或資安治理過程很長，希望 NCC 長官能讓業者有較多時間聚焦在核心業務或個資保護上，比較有多餘的力氣來做這些事，行政檢查的部分建議先刪除。

11. p.47~48，管理要點第四點：「本會執行電信事業資通安全管理，認有必要時，得向電信事業索取文書、資料或物品，甚至設備」，業者覺得較困擾，除了企業本身，有時會牽涉到第三者，這點是業者比較關切的。

12. p.49 有關客服中心的議題，審查原則第三點提到：「均限制不得移往大陸設置營運或於當地投資、合作」，政府希望業者走出去，但這樣的要求與政府的政策不是那麼一致。事實上可以要求業者將客戶資料存放在台灣，客服中心營運的地點則不一定要在台灣。國外客服最多的大概是印度，菲律賓這幾年也搶了不少生意，美國人更重視個資，但即使經過 911 事件，美國也沒有限制業者外移。

13. 簡報 p.71 提到：資通設備安全審驗作業要點基礎型設備或進階型設備的要求，電信業者設備多向國外採購，基於支持國內產業的立場，中華電信也願意配合，相關的辦法是否能清楚說明，讓業者有所遵循。

14. p.72 資通安全等級為 A 級者，鼓勵通過 ISMS 第三方驗證，這部分是否呼應 p.68，是以核心業務或個資為主，還是全業務都包含？是否能再說明清楚。

15. 涉及法規解釋與政府政策的部分，本研究案不宜提出建議。管理要點草

案條文對照表第 5 條第 2 項：「涉及國人個人資料之事項或業務部門、業務功能及系統等，例如電信業者之用戶資料庫、客服系統／客服中心、帳務系統／帳務中心等，均限制不得移往大陸設置營運或於當地投資、合作。」這部分其實是經濟部投審會的審查原則，隨時會因為時空環境而變動，放在要點裡面，後續若不合時宜，還需要修正，建議不應放入第 5 條。

16. 有關法律的強制性，赴大陸投資需通過 ISO27011 的增項驗證條款，現階段針對附件 6 增項稽核表內容的妥適性，NCC 應積極主動提出詳細說明與完善的解釋，讓業者在申請驗證時，有遵循的方向。

七、散會（上午 11 點 30 分）

附件 14　　第 5 場次資通安全管理機制座談會會議紀錄

國家通訊傳播委員會

100 年度「資訊安全管理系統研究」計畫

一、會議名稱：資通安全管理機制座談會(第二類電信)

二、時間：100 年 8 月 12 日(五)14：30

三、地點：中華軟協大會議室(北市承德路二段 239 號 6 樓)

四、主席：計畫主持人張國鴻秘書長　　記錄：鍾如郁

五、出席人員：詳見簽到表

六、討論意見綜整：

1. 管理手冊修正草案 p.3(5)設計 ISMS。編號誤植，應該是(6)。
2. 管理手冊修正草案 p.6，通訊傳播事業只要經過外部稽核單位驗證通過 ISO27001，即可免除交付證明文件，立意即在鼓勵業者通過公正第三方的稽核。但其實要求業者提供的資料還是蠻多的，依本管理手冊規定仍需提交附件七、附件八等文件，建議簡化相關程序，直接以驗證報告替代，增加業者接受外部稽核之誘因，並可同時減少 NCC 在行政檢查上的人力負擔。
3. 附件八資通安全管理矯正／預防措施單之設計，應考量發生 3、4 級資安事故時需填入的欄位。例如：「檢查項目內容」似乎僅針對內外稽檢查出的項目，另外缺少矯正預防單負責單位、承辦人員欄位，亦缺少覆核欄位。
4. 建議可參考支付卡行業資料安全標準(PCI DSS)，適度加入要求較明確的管控項目。
5. 管理手冊修正草案 p.2，評估資訊安全等級提到三項評估準則，包括「資料保護受到損害」、「影響業務運作」及「法規遵循」等三個構面，「資料保護受到損害」這個構面描述的不是很清楚，是資料的機密性、完整性及可用性受到損害？還是資料保護機制失效？建議應修正為「資料保護失效時造成損失」。

6. 管理手冊修正草案 p.3，教育訓練包含「設計 ISMS」，後面實施、檢查沒有列出來，感覺就缺了什麼。教育訓練的內容，通常會針對不同職位的人員設計不同課程，可能要定義不同職位的人員要受什麼樣的資通安全訓練。如果沒辦法寫得很具體，建議只要寫執行教育訓練就好。
7. 管理手冊修正草案 p.3 提到「防護縱深」，A 級、B 級各列出一些需符合的項目，這些項目的妥適性到什麼程度，可以再作討論。ISMS 為人所詬病的就是沒有縱深，如果要談縱深，建議像美國 NIST SP800-60，把認證方式分類，再要求不同等級的單位應做到什麼樣的等級。但差異在哪裡，建議要清楚說明。
8. 管理手冊修正草案 p.4 推動方式，要推動 ISMS 第三方驗證，這是好事，但重點是範圍，例如僅是機房的維運，或是整個單位。
9. 附件 1-2 資料保護受到損害部分，後面的說明和前面的標題沒有對應到。
10. 增項稽核表建議要對應到前面的內部稽核表項目。
11. 管理手冊修正草案 p.1，「基於保障資通安全及維護使用者權益原則，確保通訊、傳播事業『資料』、系統、設備及網路安全..... 」，建議更改為『資訊』。
12. 管理手冊修正草案 p.2，「需將通訊傳播事業之核心業務及支援個人資料蒐集、處理及利用之特定目的範圍內之所有資產納入...」，建議拿掉「特定目的範圍內」，即使超出特定目的範圍內，只要蒐集、處理及利用，還是必須被盤點進來。單純的蒐集、處理及利用，涵蓋面比較廣，且大部分的人也很難分辨是否在特定目的範圍內。
13. 管理手冊修正草案 p.2 第(3)點，針對每個定義別依「資料保護受到損害」、「影響業務運作」及「法規遵循」之影響構面，分別評定影響構面之安全等級屬 A 級或 B 級，以確認「資訊安全需求」，建議改為「資訊通訊安全需求」或「資通安全的需求」。
14. 管理手冊修正草案 p.3，「並定期進行內部稽核或外部驗證」，內稽每年被要求進行，此處的「或」易造成誤解。(p.4 資通安全等級為 A 級或 B 級者，稽核方式均為每年至少執行一次內部稽核。)

15. 管理手冊修正草案 p.3，「獲得管理階層的承諾，啟動 ISMS 專案」，此處之 ISMS 縮寫是第一次出現，於文件內並未定義且未有中文說明，且整本管理手冊談的都是資通安全，ISMS 為資訊安全管理系統與本手冊資通安全管理系統亦有差距。
16. 管理手冊修正草案 p.3，(5)選擇控制措施，其內容應包括下列項目: (A)資訊安全政策訂定。建議刪去「訂定」兩個字，因為該單元包括訂定與定期審查，原 CNS 27001 並無「訂定」兩個字。(F)通信與作業管理。建議修訂為「通訊」與作業管理(CNS 27001 原文)。
17. 管理手冊修正草案 p.4，B 級單位可能包括無資料庫者，要求資料庫稽核設備可能過於嚴格，垃圾郵件對於 B 級或較小單位的防禦意義不大。
18. 管理手冊修正草案 p.4，通訊、傳播事業應建立資通安全「事件」應變作業機制，p.3(I)資安「事故」管理，建議統一名詞。
19. 管理手冊修正草案 p.4，資通安全等級為 A 級者，其「資訊」人員、業務人員及一般人員，每年至少須分別達到 12、6、3 小時之資通安全教育訓練。建議更改為「資通訊」人員。B 級亦同。
20. 管理手冊修正草案 p.4，「….計畫，並依據法定期限之要求，保存適當之「資訊」活動記錄。」建議修改為「資訊通訊」活動紀錄。
21. 管理手冊修正草案 p.6，(3)附件五至附件十、各檢查項目之佐證資料、或經「本會認可」之資通安全管理機制驗證機構產出之稽核報告。本會認可驗證機構須被定義，是否同於 p.5 之「前項驗證機構須經『本會認可』之本國認證體系認證」？
22. 附件 1-2，「系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關違反法律規定，遭致損害賠償或是『刑事處分』，並導致嚴重不良後果。」上面違反的是法律，下面違反的是法規命令，此處會產生混淆之處，施行細則算法律還是法規？會不會造成損害賠償，此處區隔 A、B 級方式為刑事或行政處分，但刑事處罰的是行為人，行政罰處罰的是行政單位或自然人，以此區分似有不妥。因為 B 級的違反很可能還是會伴隨著刑事處罰。

23.附件 3-1，每年辦理社交工程演練及檢測企業網站安全弱點乙次。弱點掃描的部分建議為企業網路環境，僅檢查網站範圍太小。

24.附件 4-1，3.資通安全事件資料：

影響等級：『4』級：影響公共安全、社會秩序、人民生命財產

『3』級：業務無法運作，系統停頓

『2』級：系統效率降低，業務中斷

『1』級：業務短暫停頓，可立即修復

98 年 2 月會報的通報辦法已修正，判定影響定級不會僅從營運中斷考量，建議此處的影響等級需考慮 CIA 三個構面，資料洩漏與完整性破壞都需要通報。

25.手冊中多處提到「安全等級」，為避免混淆，建議提到「資通安全等級」時，均以全稱表示。

26.ISO27011 增項稽核表實際稽核時問題非常多，至少 30 個以上，建議應另案討論。

27.管理手冊修正草案 p.1，建議參照下列 ISO/IEC 27000 系列國際標準或國家標準之對應標準，惟所列 6 項標準均有 CNS 國家標準，是否考量增列？

28.有 CNS 國家標準者，應以國家標準之中文翻譯為準；例如：p.1 第 1 項依 CNS27001 應為「資訊技術－安全技術－資訊安全管理系統－要求事項」，而非「資訊安全管理系統要求事項」；第 2 項依 CNS27002 應為「資訊技術－安全技術－資訊安全管理之作業規範」；第 3 項依 CNS27003 應為「資訊技術－安全技術－資訊安全管理系統實作指引」;第 4 項依 CNS27004 應為「資訊技術－安全技術－資訊安全管理－量測」；第 5 項依 CNS27005 應為「資訊技術－安全技術－資訊安全風險管理」；第 6 項依 CNS27011 應為「資訊技術－安全技術－資訊安全管理系統－植基於 CNS 27002 之電信組織資訊安全管理指導綱要」。

29.管理手冊修正草案 p.2 出現「法規遵循」，附件 1-1 為「法律遵循」，附件 1-2 為「違反法規遵循」，其實講的是影響構面，是否考量其一致性？

30. 管理手冊修正草案 p.3，(5)選擇控制措施時，如何依資通安全等級選擇適切控制措施是有難度的，可考量讓此管理手冊與研考會所頒「安全控制措施參考指引」有相當程度上的連結。例如：若資通安全等級為 B 級者，選擇安全控制措施參考指引等級「普」之控制措施，若資通安全等級為 A 級者，選擇安全控制措施參考指引等級「中」或「高」之控制措施。
31. 管理手冊修正草案 p.3 之(1)防護縱深第 1 項 A 級同時有 IDS 與 IPS，因 IPS 已含 IDS 功能，且 IDS 為過時產品，有必要兩者都寫嗎？A 級是否只須放 IPS 即可？
32. 管理手冊修正草案 p.4 之(1)防護縱深第 2 項 B 級有入侵防禦系統，但附件 3-1 並未列入，兩者不吻合。
33. 管理手冊修正草案 p.4 之(4)資安教育訓練時數要求，未要求主管應參加教育訓練，高階主管的支持是非常重要的，應考慮要求主管接受教育訓練？
34. 附件 1-2 有關以「業務別定義」與「以部門別定義」似乎重疊類似，均以業務為出發點；有關「以部門別定義」的描述應考量予以修正？
35. 附件 3 備註描述的社交工程與網站安全弱點檢測，管理手冊內文並未描述此項，建議在 p.4 考量加入(5)說明社交工程與網站安全弱點檢測。
36. 附件 8-1 缺少「稽核員」與「受稽者」簽名欄位，不利後續追蹤；亦可考量加入「稽核領隊」與「受稽者主管」簽名欄位。
37. 附件 5 與附件 6 均有檢查項目 1-1 與 1-2，填寫附件 7 的檢查項目編號欄位時，如何分辨為附件 5 或附件 6 之檢查項目？是否考量於附件 7 第一列加入填寫範例，備註欄位註明範例，提供填寫者參考。
38. 管理手冊修正草案 p.3，防護縱深的部分提到資通安全等級為 A、B 級者，應分別建置防火牆…等。電信業者提供的服務通常都是網路存取服務，若有額外服務都是視客戶的需求，設備或軟體的保護標的是指二類電信本身內部的系統？還是提供給外部的服務？這部分似乎沒有明確的定義。

39.管理手冊修正草案 p.4，推動方式的部分，A、B 級核心業務是由業者自行評定嗎？屆時會有單位負責審查所訂等級是否符合實際狀況嗎？p.6 第 2 點，如果有第三方驗證機構認可通過 ISO27001，即可免提報相關資料。是要 NCC 業管範圍內通過認證才可以免除？還是只要某個小範圍資訊系統通過即可？希望也能明確說明。

40.商業司針對無店面零售業者推動 DP-mark 的管理制度，未來業者若通過相關管理制度，是否即可符合 NCC 管理辦法的要求？是否考慮統一來推行。

41.有關驗證範圍，手冊中並未提到內稽的範圍有多大，若企業未通過外稽，必須要通過全公司的內稽；若已通過部分範圍的外稽，例如資訊機房，只需要做資訊機房的內稽。這是管理手冊裡的漏洞，總之，還是鼓勵大家通過外稽。

七、散會（下午 16 點 00 分）

附件 15　　第 6 場次資通安全管理機制座談會會議紀錄

國家通訊傳播委員會

100 年度「資訊安全管理系統研究」計畫

一、會議名稱：資通安全管理機制座談會(傳播事業)

二、時間：100 年 8 月 15 日(一)14：30

三、地點：中華軟協大會議室(北市承德路二段 239 號 6 樓)

四、主席：協同計畫主持人喻維貞資深處長　　記錄：鍾如郁

五、出席人員：詳見簽到表

六、討論意見綜整：

1. 資安問題是國安層級的問題，不只是企業營運面或一般用戶權益保障的問題。政府持續運作案的推動，主要內容分為幾部分，包括關鍵基礎設施防護、政府核心業務的持續運作、首長人身安全的保障維護及危機的處理等。這幾項元素中，幾乎超過一半，或多或少都與資訊安全有關。因為資訊就是政府持續運作的神經中樞，如果資安沒辦法確保，不要談什麼政府持續運作，更不要談關鍵基礎設施是否能受到保護。因為有政府持續運作案的推動，發現資安問題有必要拉高到國安會層級來處理。也因為如此，才會開始用國家安全的角度來看待資安議題。
2. 從國安的角度來看資安議題，會考慮到實體安全的部分，倘若遇到天災人禍，普通的保全人力根本無法維持重要設施的實體安全，目前列管清單上的關鍵基礎設施都與軍警簽有聯合支援協定，一旦有事，設施的安全將由軍警接管。除此之外，是否也有其他未列入的重要設施，其防護等級也必須提高。廣播電台與電視業者在危機時刻都扮演重要角色，有必要提高實體安全的防護等級。
3. 要求民間業者建置備用系統，似乎是浪費投資的事，但是假設主

要系統在危機時已無法使用，備用系統確有必要。因此，備用系統的建置應列入資通安全實體防護面的議題加以考量。

4. 遇到災難時，政府可能需要民間通訊傳播業者的支援，例如遇到地震或水災等緊急狀況時，負責救災的官員需要有優先通訊權，需要有通盤的考量與相關規定。
5. 實體安全、備用系統及變時支援三項議題，需要有更明確的規範，讓業者有所遵循。
6. 核心系統是由業者的觀點來看，還是主管機關的觀點？目前電信業者通過認證的大多是帳務系統，但這是主管機關關注的重點嗎？主管機關是否重視業者在維運過程中的資訊？尤其是傳播業，這些資訊真的會影響到業務的持續運作嗎？真正會影響到業務持續運作的可能是設備的實體安全，有些資安事件發生的時候，資訊的漏失並不是主管機關想要控管的重點。
7. 個案訪談後找到 22 項關鍵的控管措施，大部分與資訊安全有關，是否真正是傳播業想要做或能夠做的，做了之後是否真的對於提升資通安全的保護水平有幫助？我個人的看法是幫助並不會太大。這時就會產生困擾，到底主管機關在管理資通安全業者的時候，希望他們能做到什麼樣的水準？主管機關的期許為何？這就回到當初的目標，若是從關鍵設施的角度來看，以德國的經驗來看，大部分都不是由業者來做，而是由政府(資訊安全局)來做，政府在第一時間已經做出評比，列出重要設施清單，動用國安資源進行保護，甚至業者也不能隨意啟動這些機制。這部分是有一個關鍵基礎設施的專責小組負責。這部分業者能做的並不多，大部分是由政府來執行。
8. 若要將這些安控措施都訂進來，以 NCC 的管轄範圍，通訊業與傳播業在本質上就有差異，運用同一套資訊安全管理規範，是否能達到當初 NCC 期望的目的，這部分建議再思考。

9. 主管機關在進行資通安全的確保時，要同時考量關鍵基礎設施的保護與業界的資通安全水準提升。關鍵基礎設施的保護既有國際標準，也有國際慣例，主管機關要做並不困難。一旦主管機關發動了，鑑別出業者的設施屬於關鍵基礎設施後，要對業者提供什麼樣的資源？業者為了營運的需求，投資了這些設備，為了國安層級的需求，就要業者如何如何，對業者來說根本不可能做到。所以，政府必須要有配套的措施。若不屬於關鍵基礎設施，則適用一般的資通安全規範，政府制定的角度是從維持社會穩定、民生秩序，這就不是國安層級的問題，就是一般的業者都要做到的，如果沒做好，民眾沒有得到適當的服務，會向主管機關抗議，主管機關就會產生壓力，所以主管機關必須對業者有所要求。
10. 政府組織再造，會產生新的資通安全權責單位，這是一個很好的時機，對 NCC 來說，只要多出一分力量，就可以把這些不同的單位連結起來，可以把這些事情做得更完美。
11. 未必要修改電信法才能對業者有所要求，舉例來說，金融單位的資安問題也層出不窮，主管機關只要公布某某銀行發生資安問題，業者自然會產生壓力去進行改善。今天我們討論的是一個認證的過程，認證過程所需的要件滿足了，就發給認證，在這些要件裡面，就可以把剛才考慮到的那些事情放進要件裡面，這部分是主管機關可以做的。
12. 通訊業與傳播業的本質有所差異，當時之所以要保護通訊事業的資通安全，主要是因為其擁有大量的民眾個資與通聯紀錄等。另外也包含了通訊系統的可用性，所以我們對他們的要求都有一些相關的要件，比如說可能參照了一些國際標準，還有最近新增的到大陸投資需通過 ISO27011 的要求。仔細去看 ISO27011 的要求，原則上還是立基於前述的兩點，首先要確保通聯紀錄只有被授權的人才能存取，其次是如果通訊事業發生任何中斷的情況，業者

必須在一定時間內回復到正常可用狀態。這些都是針對通訊事業所作的一些基本的要求。可是反過來看，就傳播事業來講，是不是跟通訊事業有同樣的需求存在？在看作業要點與管理手冊時，尤其是管理手冊，其實都有提到內稽的部分，要求通訊傳播事業每年要去檢視評估的計畫等級，要填寫 ISO27011 的增項稽核表，某種程度對傳播業者來說，個資數量與可用性都不是那麼的高，但若要求通訊傳播業者都要拉成同一個水平，其實某些業務並沒有那麼重要，業者可能會覺得不是那麼必要，對一般民眾來說，也不是那麼必要。在這麼多業務當中，找出關鍵業務是需要被保護的，對傳播業者來說，也許只有 10%，剩下的 90%是否也要遵循與通訊一樣嚴格的標準？第一、二類電信業者在導入 ISMS 時都會遇到一些困難，更何況是傳播業者，要投入的人力成本與資源投入都是難以控制的。

13. 資通安全管理作業要點修正，初期鎖定的目標是通訊業，引用的標準是 ISO27011，修正之後變成作業要點實施，成為後續驗證的需要。目前預計分為 A、B 兩級，A 級鼓勵通過第三方驗證。要點修正條文對照表 p.3 第 5 條，「電信事業申請赴大陸地區投資，應於系統審驗前，向本會認可之資通安全管理機制驗證機構，就核准之作業範圍申請驗證，並取得驗證合格證明。」，這一點是很多業者關切的。比較可惜的是當初在研擬相關作業要點與增項稽核表時，是引用 ISO27011，核心業務的定義都是以電信業者的角度來思考，所以第 5 條提到客戶個資的資料庫、客服系統、帳務系統都會偏向電信業者。所以很多業者都會擔心核心業務要如何認定，要點中的敘述好像跟實際的業務有所差距，範圍如何界定？其實是要報 NCC 審核的，所以要點第 5 條「資通安全管理之實施作業範圍報經本會核准後」，才能實施後續的認驗證。資訊安全管理系統傾向要有內部機制去評量出所謂的核心業務，但依目前的

作業辦法，是要由 NCC 來加以認定。未來業者如果有需要，特別是針對認證範圍要做個釐清。未來如何將個資保護的議題融入 ISMS，也是業者需要思考的。

14. 管理手冊 p.4，倒數第二段，「資通安全管理實施計畫範圍內，若涉及個人資料保護者，應依據『通訊傳播事業個人資料管理辦法』之規定，訂定個人資料檔案安全維護計畫，並依據法定期限之要求，保存適當之資訊活動記錄。」是否強調實施範圍需涵蓋個人資料保護？與範圍內涉及個人資料保護，強度是不同的。目前業者選擇 ISO27001 的認證範圍多偏向機房管理，因業者覺得機房是公司內部目前較能掌握的部分。個資法施行細則雖尚未公布，後續仍是需考量的重點。
15. 管理手冊 p.6，ISO 27011 相關條款較適用第一類電信業者，有時候連第二類電信都不見得適用，更何況現在連傳播業者都要適用，在增項稽核表的填寫時，應該要多作考量，哪些部分是可以預先刪除掉的，也可以事先考量，畢竟 ISO 27011 是針對第一類電信的整個範圍，如果範圍還未涵蓋到所有基礎設施，而只涵蓋到部分機房時，也不見得完全適用。
16. 簡報 p.63，ISO27005 已於 2011 年改版，建議改採 2011 年版。
17. 以國際標準來說，通常要求的是大原則，主管機關在訂定相關的規範時，若有不同的要求，應訂定相關量測的指標，ISO27001 是有提到一些量測的項目，但並未針對特定的行業，如果我們對通訊業者有特定的要求，應提供量測的數據，若未量測，很難有效具體改善。
18. 傳播業者多為單向傳播，傳送的只有節目內容，與資訊的關聯性不高，擁有民眾的個人資料並不多，資安方面可能只有有線電視業者會較相關。
19. 雖然是同一個主管機關 NCC，傳播業者與電信業者本質上就有差

別。即使是辦活動，也多是委外，並未擁有大量民眾個資，但管理手冊裡的相關規定這麼多，傳播業者擔心不能做到管理手冊所要求的各項要求。且管理手冊只是將原來的「電信事業」改為「通訊傳播事業」，細則並沒有修改，很擔心實施上會不會有困難，應考慮產業別的差異，可能需要再與 NCC 溝通。

20. 目前公司內部推動資安，主要是針對員工個人與對外的網站，除此之外，設備邁向數位化，採購防火牆、加強縱深等等這些是有的，但傳播業這一塊與電信業的落差還是蠻大的，這種情況下，電視公司只能就內部已有的規劃持續去做，管理手冊裡面規範的這麼多，但並不是業者會遇到的問題，業者會有不知從何著手的困擾。

21. 光是內部稽核表就令業者相當頭痛，不知如何做到全面稽核。業者雖然擁有數位設備與少量的民眾個資，但其營運管理非常的單純，若管理手冊要實施，光為了應付內部稽核，可能就不是企業的 IT 部門應付得了的事情。我們也贊同資通安全是非常重要的事，但請 NCC 也要考量業者營運上的困難。是否有什麼樣的模式可以協助傳播事業做好營運事業體的內部稽核，而不是套一個那麼大的圈圈，感覺上不是那麼容易做到的事情。

22. 不能僅是將「電信事業」改為「通訊傳播事業」，否則修正後的管理手冊要施行，會有窒礙難行之處。赴大陸投資需要額外通過的相關認證，是否有必要，值得再商榷。

23. 開放赴大陸投資業務項目，僅限第二類電信業者的一般業務，並未針對傳播事業。ISO27011 偏重第一類電信，把對第一類電信的要求放在第二類電信的一般業務，是否恰當，值得再討論。

24. 通訊與資訊一定有其相關之處，才會同時由 NCC 所業管。資訊安全不僅指資訊被竊取，也包括資訊的承載、資訊是否被完整與及時的傳送。傳播業雖然未擁有大量民眾個資，但做為重要的資訊

承載者，不應妄自菲薄，應將觀念、格局放大一點。舉個最極端的例子來說，軍事上的入侵或政變，控制了資訊就控制了國家的命脈。至於傳播業者是否要跟第一類電信業者負同樣的責任與義務，細節上則可以再討論。

七、散會（下午 16 點 00 分）

附件 16　資通安全管理機制成果發表會會議紀錄

國家通訊傳播委員會

100 年度「資訊安全管理系統研究」計畫

一、會議名稱：資通安全管理機制成果發表會

二、時間：100 年 8 月 12 日(五)14：30

三、地點：文化大學大夏館 210-211 會議室(北市建國南路二段 231 號 B2)

四、主席：計畫主持人張國鴻秘書長　記錄：鍾如郁

五、出席人員：詳見簽到表

六、專家意見綜整：

1. 延續行政院國家資通安全會報六個構面政策，為落實於通訊傳播事業，分析六大構面在通訊傳播事業中不同的重要性，分為關鍵性業務、支援性業務及行政性業務。有此依據，較容易切入。雖不至於可永保平安，但至少會比較安全。目前已發展到實務的推展，有基準線(baseline)的概念，接下來要發展的，是否有可資依循防護的措施。假設業者做到了，誰來告訴業者已經達到標準了。ISO 27006 自動化稽核，要如何做驗證。前面風險評鑑的六大構面與三大等級，將變成可資依循的指引，但只有指引還不夠，業者還希望有範本供參考。實施的步驟應如何進行，希望還是有明確的參考。目前的重點已經不在風險評鑑，這部分已經很清楚說明，反而步驟流程才是重要的。

2. 電信事業的通聯紀錄目前應保存半年，但這過程中的軌跡資料若未保存，一旦資料軌跡被視為個人資料，個資損害賠償訴訟五年

內都可提出求償，且業者需負舉證責任。目前業者大部分都考慮如何證明無故意或無過失，以減輕法律責任，但目前的實務上幾乎不可能做到，個資保護的重點在於防止訴訟的成立。不當揭露，要有原告與被告之間損害賠償的鏈結。應有類似標準的導入，以建立一套個資保護的機制。適法性調查、個人資料檔案清查，應該要先進行。分階段、分批投入預算。愈早進行，愈有可能找到合適的顧問協助。

3. 資訊安全管理系統負責的單位應該是誰？一般都認為是 IT 部門，但真是如此嗎？未來在執行資訊安全業務時，資訊安全並不侷限於資訊安全機房。在什麼範圍之內執行會較合理。大部分的業務主導還是 IT 部門。有哪一個主管會說資訊安全不重要？資訊的遺失，不是一個兩個檔案，通常都是數以 G 計。如果非 IT 設備，如何主導防禦縱深。為什麼要找出關鍵業務，最重要的概念還是營運持續。

七、散會（下午 16 點 00 分）

附件 17

ISO/IEC 27011 控制措施對照表

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
A.6	資訊安全的組織				
A.6.1		內部組織目標： 於組織內管理資訊安全		Internal organization Objective: To manage information security within the organization.	
A.6.1.5			機密性協議	Confidentiality agreements Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified and regularly reviewed.	1.1 是否訂定並定期審視保密及防止不當揭露組織需保護資訊之機密性協議（例如通訊資訊中的實體、內容、來源、目的地、日期時間）？
A.6.1.6			與權責機關的聯繫	Contact with authorities Appropriate contacts with relevant authorities should be maintained.Appropriate contacts with relevant authorities should be maintained.	1.2 組織提供執法機關所請求之資訊時，是否訂定控管程序以確認此申請依據國家法規之合法過程與程序？
A.6.2		外部團體目標： 維持外部團體所存取、處理、管理或與其通信之組織資訊與資		Objective: To maintain the security of the organization's information and information processing facilities that are accessed, processed,	

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
		訊處理設施的安全		communicated to, or managed by external parties.	
A.6.2.2			處理客戶事務的安全說明	All identified security requirements should be addressed before giving customers access to the organization's information or assets.	
A.6.2.3			第三方協議中之安全說明	Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirement.	
A.7	資產管理				

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
A.7.1.1			資產清冊	All assets should be clearly identified and an inventory of all important assets drawn up and maintained.	2.1 是否明確界定組織的電信設施與其他組織相連結或相關之部份的管理責任，並具體和明確的文件化？
A.7.2.1			分類指導綱要	Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.	
A.8	人力資源安全				
A.8.1		聘僱之前目標： 確保員工、承包者及第三方使用者了解其責任，並勝任其所被認定的角色，以降低竊盜、詐欺或設施誤用的風險		Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.	

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
A.8.1.1			角色與責任	Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy.	3.1 是否詳細檢查職務上能夠授權存取之必要服務：例如：客戶個人資料或是客戶通話內容等，並納入相關安全責任之中？ 3.2 對於人員進用，是否考量相關電信證照或具備適當的電信知識和技能？
A.8.1.2			篩選	Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.	3.3 對所有聘僱之應徵者、承包者及第三方使用者的之進用或委派，是否作適當之背景查驗工作，例如：工作職務涉及客戶個人資料或是通訊內容之存取者？

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
A.8.1.3			聘僱條款與條件	As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security.	3.4 聘請第三方機構之前，是否明確界定和溝通其安全角色和職責？ 3.5 對於委外承包商或是第三方使用者，是否在合約中加入安全角色與職責的要求？ 3.6 組織內任何人從事電信服務時，是否要求應保護職務上所知悉之營業秘密？ 3.7 組織是否依據相關法規命令，訂定防止不當揭露之責任？
A.8.2		聘僱期間目標： 確保所有員工、承包者及第三方使用者認知資訊安全的威脅與關切事項、其基本責任與強制責任， 並有能力在日常工作中支持組織安全政策與降低人為錯誤的風險		適用 ISO/IEC 27002 條文內容	
A.9	實體與環境安全				
A.9.1		安全區域目標： 防止組織場所與資訊遭未經授權的		Objective: To prevent unauthorized physical access, damage, and interference to the organization's premises	

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
		實體存取、損害及干擾		and information.	
A.9.1.1			實體安全周界	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.	4.1 電信營運中心是否有適當的實體入侵偵測系統？ 4.2 實體邊界發生異常狀況時，是否有權責人員可立即解決？
A.9.1.2			實體進入控制措施	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	4.3 控制中心與操作室是否有適當強度的進出控制措施（strong entry controls）？ 4.4 是否針對訪客的探訪紀錄進行適當保護？（訪客進入及離開時間、訪客身份等。） 4.5 接待人員是否檢查訪客是否攜帶危險物品進入及帶走未經授權的物品？

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
A.9.1.7				通訊中心的安全 Securing communication centres	4.6 通信中心（communication centers）是否選擇在適當地點?(避免選擇在易受水災、風災影響，與臨近強烈電磁及儲存危險物的場所） 4.7 通信中心是否裝設自動火災警報系統？ 4.8 通信中心是否為抗震建物？樓層地板是否有足夠的承載能力？ 4.9 通信中心是否盡可能使用防火建材？ 4.10 通信中心之設計是否盡可能避免火災蔓延？
A.9.1.8				Securing telecommunications equipment room	4.11 電信設備機房（telecommunications equipment room)或實體隔離的操作區（如：行動通信基地臺 mobile base station）是否有足夠的安全防護？
A.9.1.9				Securing physically isolated operation areas	
A.9.2		設備安全目標： 防止資產的遺失、損害、竊盜或破解，並防止組織活動的中		Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.	

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
		斷			
A.9.2.1			設備安置與保護	Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	4.12 不同客戶之代管設備是否實體分隔，並實行適當之保護措施？
A.9.2.2			支援的公用設施	Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.	4.13 關鍵設施是否有不斷電系統以及足夠電力保護？
A.9.3		Security under the control of other party			

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
A.9.3.1				Equipment sited in other carrier's premises Control： When telecommunications organizations install equipment outside of their own premises, the equipment should be sited in a protected area so that any risks from environmental threats or dangers and from the possibility of unauthorized access are reduced.	4.14 電信事業放置於其它場所的設備是否有足夠的安全防護，？
A.9.3.2				Equipment sited in user premises Control： When telecommunications organizations install equipment within the telecommunications service customer premises in order to connect with the customer equipment, the organizations' equipment should be protected in order to reduce risk from environmental threats or dangers and from the risk of	

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
				unauthorized access. Implementation guidance	
A.9.3.3				Interconnected telecommunications services Control In the provision of interconnected telecommunications services, the telecommunications organizations should specify a well-defined boundary and interface with other telecommunications organizations, so that each organization may be partitioned and isolated in a timely manner in order to evade an identified risk.	4.15 是否持續監控與其它通信服務互連的狀態？是否有適當的控制措施檢查與其它通訊服務互連是否正常？發生問題時，是否有方法可以檢查？ 4.16 其它通信服務互連是否已妥善定義範圍與介面？是否已定義一旦用戶發生斷線時如何處置的協議或合約？

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
A.10	通訊與作業管理			in a protected area so that any risks from environmental threats or dangers and from the possibility of unauthorized	
A.10.1		作業之程序與責任目標： 確保正確與安全地操作資訊處理設施		access are reduced.	
A.10.1.1			文件化作業程序	Operating procedures should be documented, maintained, and made available to all users who need them.	5.1 是否具體定義啟動災害情況、緊急情況或危機之處理程序的條件？
A.10.1.2			變更管理	Changes to information processing facilities and systems should be controlled.	5.2 是否建立資訊處理設施與系統變更之管理程序？管理程序之紀錄是否包括設施之安裝、改位置及移除？
A.10.1.4			開發、測試及運作設施的分隔	Development, test, and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational system.	5.3 系統開發、測試及正式運作是否盡可能區隔在不同的作業環境處理？ 5.4 是否避免以真實之資訊進行系統開發與測試？

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
A.10.4.2			對抗行動碼的控制措施	Where the use of mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing.	5.5 行動碼（mobile code）的安裝是否作必要之授權處理或限制使用？內嵌行動碼之中介軟體（middleware）是否有考慮其限制使用？
A.10.6		網路安全管理目標： 確保對網路內資訊與支援性基礎建設的保護		Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.	
A.10.6.1			網路控制措施	適用 ISO/IEC 27002 條文內容 Further implementation guidance is in Annex B (informative).	
A.10.6.2			網路服務的安全	Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced.	5.6 是否訂定網路服務提供者及使用者之服務及使用範圍、相關權責及程序，並納入服務協議中？在服務提供前公告，並適切的維護與管理通信服務？

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
A.10.6.3				電信服務交付之安全管理 Security management of telecommunications services delivery Control Telecommunications organizations should set the security level for the various business propositions of telecommunications services provided, announce it to their customers prior to service delivery, and maintain and manage their telecommunications services properly.	
A.10.6.4				Response to spam Further implementation guidance is in Annex B (informative).	5.7 是否訂定相關政策以對應垃圾郵件並建置適切之控管措施？建立一個合適的、令人期待的電子郵件通信環境。

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
A.10.6.5				Response to DoS/DDoS attacks Further implementation guidance is in Annex B (informative).	5.8 是否訂定相關政策以對應阻斷服務（DoS）或分散式阻斷服務攻擊（DDoS）並建置適切之控管措施？建立一個合適的、令人期待的電信環境。 5.9 是否適當的保護網路設施，例如網路攻擊下的伺服器、路由器等？應具備經由 IP 位置、通訊埠與通訊協定等個別過濾通訊或限制通訊頻寬的機制。 5.10 是否具備偵測偽造來源地址（IP spoofing）的能力？ 5.11 是否運用嚴格的密碼控制措施及/或高強度憑證（strong authentication）的功能以防範來源造假(source impersonation）？ 5.12 是否事先經由定期的收集與量測有關於災難、意外事件、社會現象等導致電信設備失效與網路壅塞之相關資訊並彙集關鍵知識？ 5.13 通訊設備是否具備偵測網路壅塞並避免網路壅塞時通訊集中之機制？ 5.14 是否制訂維運規範以收集可能造成網路雍塞之災難及計畫中事件的資訊？

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
					5.15 是否將暫時的設備總處理能能力經由量測納入改善考量？經由量測以改進潛在之營運中斷與災難時分散式處理中心與支援性設備的建置，並在必要時考量適切的配置變更。 5.16 是否能鑑別並給予必要的通訊優先權以預防或減輕災難時交通維護、通訊、電力供應或維持社會秩序？
A.10.10		監視目標：偵測未經授權的資訊處理活動		Objective: To detect unauthorized information processing activities.	
A.10.10.1			稽核存錄	Audit logs recording user activities, exceptions, and information security vents should be produced and kept for an agreed period to assist in future investigations and access control	5.17 個人資料之留存時限是否依照權責單位之規定？

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
				monitoring.	
A.11	存取控制				
A.11.1		存取控制的營運要求目標： 控制資訊的存取		Objective: To control access to information.	
A.11.1.1			存取控制政策	An access control policy should be established, documented, and reviewed based on business and security requirements for access.	6.1 對於用戶端設備，電信事業是否策定適切的存取控制規則（例如：控制的要求應基於資訊擁有者而非設備擁有者；採原則禁止、例外開放之規則）？ 6.2 是否將網路運作及電腦運作之使用權責予以區隔？
A.11.4		網路存取控制目標： 防止網路服務遭未經授權的存取		適用 ISO/IEC 27002 條文內容	

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
A.11.4.8				Telecommunications carrier identification and authentication by users	6.3 是否有適切的控制機制，提供使用者能有效的辨識與認可正確的電信服務（如用戶無法證實時，應有的警示措施）？
A.12	資訊系統獲取、開發及維護				
A.12.4		系統檔案的安全目標：確保系統檔案的安全		Objective: To ensure the security of system files.	
A.12.4.1			作業軟體的控制	There should be procedures in place to control the installation of software on operational systems.	7.1 更新作業軟體、應用軟體、程式庫之人員，是否由經過適當訓練之管理員執行，並經過適當之管理授權？ 7.2 操作系統之環境中應只能保持一套經批准之程式碼，不能有發展中之程式碼與安裝有編譯器程式？ 7.3 是否採用型態管理控制系統來保持所有建置之軟體與文件一致？ 7.4 所有資訊系統變更實作前，是否均有適當之回復策略？ 7.5 是否針對所有運作中程式原始碼之更新維護稽核日誌？ 7.6 是否針對屬敏感性系統（如交換器設備等）

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
					之作業系統軟體或應用軟體，實施涵蓋所有路徑之完整測試？ 7.7 是否針對屬敏感性系統之應用軟體，至少保留前三代版本相關備份。
A.13	資訊安全事故管理				
A.13.1		通報資訊安全事件與弱點目標： 確保與資訊系統相關的資訊安全事件與弱點，被以能夠採取及時矯正措施的方式傳達		Objective: To ensure information security, events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.	
A.13.1.1			通報資訊安全事件	Information security events should be reported through appropriate management channels as quickly as possible.	

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
A.13.2		資訊安全事故與改進的管理目標：確保採用一致與有效的作法於資訊安全事故的管理		Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.	
A.13.2.1			責任與程序	Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.	8.1 是否建立資安事件之通報及事故回應與提報處理程序的管理責任與職掌定義？
A.13.2.2			從資訊安全事故中學習	There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.	8.2 是否建立資安事件或事故等事後管理會議，以協助單位能從資安事件、事故中學習？
A.14	營運持續管理				
A.14.1		營運持續管理的資訊安全層面目標：為對抗營運活動中斷，保護重要營運過程不受重大資訊系統失效或災害的影響，並確		Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.	

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
		保及時再續(resumption)			
A.14.1.1			資訊安全納入營運持續管理過程	A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.	8.3 是否擬定營運中斷後之各風險之處理優先順序或處理準則？
A.14.1.3			發展與實作包括資訊安全的持續計畫	Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time-scales following interruption to, or failure of, critical business processes.	
A.15	遵循性				

區分	安全領域	控制目標	CNS 27002 控制措施	ISO/IEC 27011	ISO/IEC 27011 增項稽核表（NCC）
A.15.1		遵循適法性要求目標：避免違反任何法律、法令、法規或契約義務， 以及任何安全要求		適用 ISO/IEC 27002 條文內容	
A.15.1.7				Non-disclosure of communications	
A.15.1.8				Essential communications	
A.15.1.9				Legality of emergency actions	