目　　錄

2. 人才培訓計畫

2.1. 計畫緣起與現況分析

為有效提升國家整體資通安全，行政院自民國九十年起實施「建立我國通資訊基礎建設安全機制計畫」，其中第九項執行要點--加強通資訊安全人力培訓及觀念宣導，完成資訊人員及主管人員的資安管理課程之訂定。而後繼之第二期計畫(民 94~97)，更將『提升通報應變時效、健全資安防護能力、深化資安認知及教育、促進國際交流合作』列為四大目標。當中，各部會資安人才培訓情況與結果如下：

主(協)辦	計畫依據	培訓課程	培訓對象	課程時數

單位				
研考會、目的事業主管機關會	行動方案 29 推動資安專業證照培訓工作 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 2005/07 及 ICST 政府人員資安學程規劃	資安管理系統主導稽核員	AB 級機關 資訊主管、 業務人員、 政風人員	40 小時
		資訊安全管理系統建置	AB 級機關	40 小時
		資通安全技術訓練	A 級機關 資訊人員、 資安人員、 資訊主管	96 小時
		警示系統教育訓練	AB 級機關	3 小時
		弱點掃描教育訓練	AB 級機關	6 小時
		e-learning 技術、管理、其他類	ABCD 級機關 資訊人員、 資安人員、 資訊主管、 業務人員、 政風人員	120 小時
教育部	行動方案 30 推動教育體系資安計畫 執行要點(4)輔導縣(市)教育網路中心建置 ISMS、(6)資安教育訓練與認知推廣	資安管理系統主導稽核員	ABCD 級機關學校 資訊人員	
		資安認知	ABCD 級機關學校 一般人員	2~6 小時
	行動方案 31 推動大專院校開辦資安學程			
	行動方案 32 設立資安研究與教學中心 執行要點(4)種子培訓	e-learning 資安防護措施	一般民眾	
		資安宣導手冊與	一般民眾	

	與教育推廣	光碟		
		資安暑期課程	大專學生與各界人士	54 小時
		資訊安全監控中心 (SOC) 理論與建置實務	資訊/資安人員或主管	6 小時
經濟部中小企業處	縮減產業數位落差計畫	e-learning (電子郵件安全、電子商務安全、資安自我檢測、資訊資產管理、營業秘密與個人資訊保護)	一般員工(1門) 高階主管(2門) 資訊/資安人員(2 門)	2.5 小時

在學校體系的資安教育投入上，依據行政院國科會「知識經濟時代人才培育之基礎平台與架構計畫」之「資安人才培育分項計畫」，規劃成立資通安全研究與教學中心，以整合分散於各大專院校與研究機構之人才資源。由國科會經費補助，李德財院士(中研院資訊所)召集，資通安全研究與教學中心（Taiwan Information Security Center, 簡稱 TWISC）自 2005 年 4 月 1 日正式陸續成立北、中、南大專院校和研究資源整合中心，以提昇我國資安科技學術與工程能量、資安產業工程應用與管理能量、促進資安國際合作交流，及培育資安種子，推廣資安新知與認知，已見到初步的成效。

另一方面，除學校體系之在職培訓外，為提升人力素質需依賴有效的培訓系統，而所謂「有效」的培訓系統，即為一套能增進目標達成的流程管理工具。為此，本人才培訓計畫依據 RFP 所訂定之工作項目『參酌 ISO 10015 國際培訓品質標準之規範，以職能管理模式』，設計一套有系統的培訓架構來協助達成培訓目標，期能做為我國資通安全相關人員與一般員工/民眾訓練課程規劃、執行與控制的標準。

2.2. 範疇描述

（一）適用對象

1. 高階主管：擁有企業或組織整體決策權之高階主管。
2. 資訊/資安主管：負責統籌、管理、訂定、稽核企業或組織資訊安全事務之管理人員。
3. 資訊/資安人員：負責執行與維運企業或組織資訊安全事務之工程技術人員。
4. 一般員工/民眾：企業或組織內使用資訊系統之一般員工及一般資訊系統使用之民眾。

（二）設計原理

1. 本計畫依ISO 10015國際培訓品質標準，強調組織目標(係指組織資訊安全管理目標)與人員目標的連結；人員目標與培訓目標的連結；培訓目標與培訓投入、流程和產出的連結。
2. 本計畫依教案設計模型(Instructional systems design model, ISD)，應用訓練需求分析、成人學習理論、訓練遷移和訓練評估的原理，來規劃培訓投入、流程與產出的課程架構。
3. 本計畫依人力計分卡(Workforce Scorecard)，有效地區分促成人員績效背後的要素和因果關係，包括行為、職能(知識技能)與觀念，將人員目標、培訓目標與課程架構做合理的連結。

（三）工作期程

期間	工作任務	交付標的
第一階段 (18 個月)	高階資通安全培訓規劃 中階資通安全培訓規劃/執行 初階資通安全培訓規劃/執行/評估	高階課程的課程計劃書 中階課程的課程計畫/訓練記錄 初階課程的計畫/記錄/評估報告
第二階段 (12 個月)	高階資通安全培訓執行 中階資通安全培訓評估	高階課程的訓練記錄 中階課程的評估報告
第三階段 (6 個月)	高階資通安全培訓評估	高階課程的評估報告

2.3. 培訓目標

(一) 組織目標

為提升國家整體資通安全，有賴各類營業與非營利組織在資訊安全管理機制上的建立，其內容包括：「安全政策與資源」、「風險管理」、「人員安全」、「實體安全」、「系統與網路」、「存取控制」、「軟體管理」、「業務持續運作」與「資訊稽核」等九大安全管理構面。而本培訓計畫，最終目標即在藉由培訓，以強化各組織中高階主管、資訊/資安主管、資訊/資安人員，與一般員工對資訊安全管理與技術上的績效表展現，繼而提升其組織的九大資訊安全管理構面之評比。

(二) 人員目標

為強化各組織在九大資訊安全管理構面，各類人員在資通安全上的期望績效展現與目標如下：

人員類別	績效展現	衡量指標
高階主管	支持與推動組織資安管理制度與系統	資安支出佔資訊支出比重 通過第三方稽核比重
資訊/資安主管	建立組織資安管理制度與系統	實施資安管理制度比例 實施資安教育訓練比例 資安事件復原時間 具資安專業證照比例
資訊/資安人員	維護組織資安管理制度與系統	資安事件發生率
一般員工/民眾	遵守組織資訊安全與資安制度	資安行為調查結果(高標) 全民資安健檢成績(高標)

(三) 培訓目標

1. 培訓需求

前述各類人員之績效展現，有賴其對於資通安全基本觀念與專業知識認知程度之提升，其培訓需求概略歸納如下：

(1) 高階主管:理解資安管理與企業永續經營之關聯性和具備資訊安全管理知識、法令和道德規範
(2) 資訊/資安主管：能規劃與實施資安教育訓練；能規劃資安事件危機處理機制;能進行組織之資安內部稽核；並具備資安管理的專業知識技術
(3) 資訊/資安人員：具備資安管理的專業知識技術，並能進行資安事件危機處理
(4) 一般員工/民眾：具備資訊安全危機意識，理解資訊安全政策、法令與道德規範，並能落實資安行為

2. 職能分類

根據上述各類人員的培訓需求分析，同時將我國資通安全培訓

體系與先進國家資通安全專業知識標準接軌，本計畫參考CBK(Common Body of Knowledge)知識庫、國際電腦稽核協會(International System Audit and Control Association, ISACA)電腦稽核人員認證內容、(ISC)2 資訊安全課程模組、以及行政院研考會所建議的資安數位課程學習內容，並依職能模型(Competency Model)的架構，將資通安全專業職能歸類如下：

職能	知識領域	行為事例
1.資訊安全管理	資訊安全管理概念 資訊資產分類程序 落實安全政策 職務與責任 風險管理 安全警覺	1-1.能說明資訊安全管理的政策、標準與程序 1-2.能指出使用者面對資訊安全上的重點議題，並規範正確行為 1-3.能依區分資訊資產風險等級，規劃降低資訊風險的方法和工具
2.存取控制	控制種類和型態 存取控制威脅 控制作業 鑑別及授權	2-1.能應用各類存取控制的技術，以降低風險 2-2.能指出使用者在資訊系統上的安控點
3.通訊及網路安全	通訊及網路管理相關概念 通訊及網路技術相關概念	3-1.能應用區域網路、廣域網路和遠端資料存取之通訊及網路安全元件 3-2.能應用內部網路、外部網路和網際網路的傳輸協定、防火牆與閘道技術 3-3.能應用預防、偵測、和回復之安全技術，以管控病毒或駭客入侵
4.密碼學	密碼技術 同步加密金鑰 非同步加密金鑰 網際網路密碼應用	4-1.能應用同步與非同步之加密金鑰 4-2.能因應不同類型風險與可能攻擊事件，選擇適當的加密演算型態和方法 4-3.能應用數位簽章和電子郵件防護機制
5.安全架構及模型	安全架構 安全保證 資訊安全模型	5-1.能應用資訊安全架構與模型 5-2.能說明如何規劃電腦與網路安全管理系統
6.作業安全	控制與保護 監視與稽核 威脅及弱點	6-1.能規範與說明資訊軟硬體安全控制的要點 6-2.能說明如何評估環境控制設計 6-3.能指出資訊使用人員之作業安全要點

7.應用系統開發	系統開發生命週期 軟體能量成熟度 物件導向系統 人工智慧系統 資料庫系統 應用系統控制	7-1.能規劃各階段軟體開發生命週期之風險控制要項 7-2.能說明應用系統與資料庫的維護程序 7-3.能說明惡意軟體之偵測與防護措施
8.營運持續與復原	營運持續計畫 災難復原計畫	8-1.能說明營運持續計畫與流程 8-2.能說明災難復原計畫和行動方案
9.法令/調查與道德	法令 犯罪調查 權利 道德	9-1.能回答資通犯罪與個資保護之相關法令 9-2.能應用鑑識技術來偵查與蒐集資通犯罪 9-3.能回答資通安全人員之倫理與道德條款
10.實體安全	實體安全威脅 實體安全管控	10-1.能辨視實體安全可能威脅、建立弱點清單和反制措施 10-2.能說明如何規劃實體安全管控制度
11.資訊系統稽核	標準與指引 風險分析 內部控制 資訊稽核之執行 自行評估 ISA 程序之新變革 ISO 27001/17799	11-1.能說明如何建置以風險為基礎資訊系統稽核策略及目標 11-2.能說明組織內資訊風險管理系統及內控制度的推動方式 11-3.能說明如何評估程式化及人工控制之設計與建置，以確保企業作業程序之風險均被識別，並在可接受程度內

3. 評鑑標準

此外，為明確設定培訓目標，本計畫採用職能評鑑技術(Competence Assessment Technique)的概念，依行為定錨量法(Behaviorally Anchored Rating Scale, BARS)，將各項職能行為事例分為四大評鑑標準：

3 分：能回答該行為事例背後的專業知識、通過或取得被認可的知識測驗或相關認證，並能獨立執行該行為事例所描述的大部份活動於資通安全管理系統中。

2 分：能回答該行為事例背後的專業知識，並通過或取得被認可的知識測驗或相關認證，在他人指導下，可執行該行

為事例所描述的簡單活動於資通安全管理系統中。

1 分：能回答該行為事例相關的通識概念，有相關課程學習記錄，並可將其概念應用在日常通資訊系統的使用，但尚無法執行該行為事例於資通安全管理系統中。

0 分: 無法回答該行為事例相關的通識概念，未通過或取得相關課程學習記錄、知識測驗或證照，亦無法應用其概念在通資訊系統的使用或資通安全管理的相關活動中。

4. 職能水準

整合上述資通安全各職能分類和評鑑標準，各類人員可藉由培訓活動來達成的職能水準如下：

職能	**各類人員的培訓目標**(職能水準的平均得分)			
	高階主管	資訊/資安主管	資訊/資安人員	一般員工/民眾
1.資訊安全管理	2	3	2	1
2.存取控制	1	2	3	1
3.通訊及網路安全	1	2	3	1
4.密碼學	1	2	3	0
5.安全架構及模型	1	2	3	0
6.作業安全	1	2	3	1
7.應用系統開發	0	2	3	0
8.營運持續與復原	2	3	2	1
9.法令/調查與道德	2	3	3	1
10.實體安全	1	2	3	1
11.資訊系統稽核	2	3	2	1

2.4. 課程模組

依據本計畫各類人員的培訓目標和考量資源分享，參考行政院研考會在文官學院所設計的資通安全數位課程，擬出十八大課程模組。每個課程模組所明訂的項目包括：

(一) 課程項目：即該課程模組所含的職能有那些？

(二) 課程目標：即該課程模組所要達成的課程項目包括那些行為事例？要達到什麼樣的職能水準？以做為自辦訓練單位、委託培訓機構或講師在設計課程的依據。

(三) 課程大綱：為達成每條課程項目的課程目標，應該要教授的知識領域包括那些？

(四) 學習方式：根據課程模組所設定的培訓目標與課程大綱，根據學習理論和成本效益，建議採用的學習與發展方式有那些？

(五) 綜合整理，十九大課程模組的內容，歸納如下：

1. 個人資訊安全

課程項目	課程目標	課程大綱	學習方式
1.資訊安全管理	1-1 (1 分) 1-2 (1 分)	資訊安全概念 落實安全政策 安全警覺	數位學習 -生活實例 -基本概念 -議義 -練習題
2.存取控制	2-2 (1 分)	控制作業	
3.通訊及網路安全	3-2 (1 分) 3-3 (1 分)	通訊及網路安全概念和防護技巧	
6.作業安全	6-3 (1 分)	資訊作業安全要點	
10.實體安全	10-1 (1 分)	實體安全防護	

2. 資訊安全管理通識

課程項目	課程目標	課程大綱	學習方式
1.資訊安全管理	1-3 (1 分)	資訊資產分類程序 職務與責任 風險管理	數位學習 -理論架構 -實務案例 -講義 -練習題
2.存取控制	2-1 (1 分)	控制種類和型態 存取控制威脅 控制作業 鑑別及授權	
3.通訊及網路安全	3-1 (1 分)	通訊及網路管理與技術相關概念	
6.作業安全	6-1 (1 分) 6-2 (1 分)	控制與保護 監視與稽核 威脅及弱點	
8. 營運持續與復原	8-1 (1 分) 8-2 (1 分)	營運持續概念 災難復原概念	
10.實體安全	10-2 (1 分)	實體安全管控	

3. 資訊安全法令通識

課程項目	課程目標	課程大綱	學習方式
9. 法令/調查/道德	9-1 (1 分) 9-2 (1 分) 9-3 (1 分)	法令 犯罪調查 權利 道德	數位學習 -理論架構 -實務案例 -講義 -練習題

4. 資訊安全制度

課程項目	課程目標	課程大綱	學習方式
11.資訊系統稽核	11-1 (1 分) 11-2 (1 分) 11-3 (1 分)	標準與指引 ISO 27001/17799	數位學習 -理論架構 -實務案例 -講義

			-練習題

5. 資訊安全技術

課程項目	課程目標	課程大綱	學習方式
4.密碼學	4-1 (1 分) 4-2 (1 分) 4-3 (1 分)	密碼與金鑰應用	數位學習 -理論架構 -實務案例 -講義 -練習題
5.安全架構及模型	5-1 (1 分) 5-2 (1 分)	安全架構 安全保證 資訊安全模型	

6. 資訊系統稽核

課程項目	課程目標	課程大綱	學習方式
11. 資訊系統稽核	11-1 (2 分) 11-2 (2 分) 11-3 (2 分)	標準與指引 內部控制 自行評估 ISA 程序之新變革 ISO 27001/17799	數位學習 -理論架構 -案例分享 -議義 -練習題 認證專班 *CISA *CISM *GSNA

7. 資訊安全管理

課程項目	課程目標	課程大綱	學習方式
1.資訊安全管理	1-1 (2 分) 1-2 (2 分) 1-3 (2 分)	資訊安全管理概念 資訊資產分類程序 落實安全政策 職務與責任 風險管理 安全警覺	數位學習 -理論架構 -案例分享 -議義 -練習題 認證專班 *CISSP *GSEC *GISO *ITE

			*CISA *GSNA

8. 存取控制

課程項目	課程目標	課程大綱	學習方式
2.存取控制	2-1 (2 分) 2-2 (2 分)	存取控制種類型態 存取控制威脅 控制作業 鑑別及授權	數位學習 -理論架構 -案例分享 -議義 -練習題 認證專班 *CISSP *GSEC *CISA *GSNA

9. 通訊及網路安全

課程項目	課程目標	課程大綱	學習方式
3.通訊及網路安全	3-1 (2 分) 3-2 (2 分) 3-3 (2 分)	通訊及網路安全技術	數位學習 -理論架構 -案例分享 -議義 -練習題 認證專班 *CISSP *ITE *GSWN *GSUX *GSNA *GCFW *GCIA

10. 密碼學

課程項目	課程目標	課程大綱	學習方式

4.密碼學	4-1 (2 分) 4-2 (2 分) 4-3 (2 分)	密碼技術 同步加密金鑰 非同步加密金鑰 網際網路密碼應用	數位學習 -理論架構 -案例分享 -議義 -練習題 認證專班 *CISSP *GSEC

11. 安全架構及模型

課程項目	課程目標	課程大綱	學習方式
5.安全架構及模型	5-1 (2 分) 5-2 (2 分)	安全架構 安全保證 資訊安全模型	數位學習 -理論架構 -案例分享 -議義 -練習題 認證專班 *CISSP *GSEC *ITE *GISO

12. 作業安全

課程項目	課程目標	課程大綱	學習方式
6.作業安全	6-1 (2 分) 6-2 (2 分) 6-3 (2 分)	控制與保護 監視與稽核 威脅及弱點	數位學習 -理論架構 -案例分享 -議義 -練習題 認證專班 *CISSP *GSEC

13. 應用系統與開發

課程項目	課程目標	課程大綱	學習方式
7.應用系統與開發	7-1 (2 分) 7-2 (2 分) 7-3 (2 分)	系統開發生命週期 軟體能量成熟度 物件導向系統 人工智慧系統 資料庫系統 應用系統控制	數位學習 -理論架構 -案例分享 -議義 -練習題 認證專班 *CISSP *GSEC *ITE *CISA *GSNA

14. 營運持續與復原

課程項目	課程目標	課程大綱	學習方式
8.營運持續和復原	8-1 (2 分) 8-2 (2 分)	營運持續計畫 災難復原計畫	數位學習 -理論架構 -案例分享 -議義 -練習題 認證專班 *CISSP *GSEC *GCIH *CISA *GSNA

15. 法令/調查與道德

課程項目	課程目標	課程大綱	學習方式
9.法令犯罪調查與倫理	9-1 (2 分) 9-2 (2 分) 9-3 (2 分)	法令 犯罪調查 權利 倫理	數位學習 -理論架構 -案例分享 -議義 -練習題 認證專班

			*CISSP *GSEC *GCFA *GIAC

16. 實體安全

課程項目	課程目標	課程大綱	學習方式
10.實體安全	10-1 (2 分) 10-2 (2 分)	實體安全威脅 實體安全管控	數位學習 -理論架構 -案例分享 -議義 -練習題 認證專班 *CISSP *GSEC *ITE

17. 資通安全管理實務

課程項目	課程目標	課程大綱	學習方式
1.資訊安全管理	1-1 (3 分) 1-2 (3 分) 1-3 (3 分)	安全政策規劃 風險管理實務	互動數位學習 -實作架構 -互動摸擬 -實作題 認證專班 *CISSP *CISA *GSEC
8.營運持續作業和復原計畫	8-1 (3 分) 8-2 (3 分)	營運持續計畫設計 災難復原計畫設計	
9.法令犯罪調查與倫理	9-1 (3 分) 9-2 (3 分) 9-3 (3 分)	法令 犯罪調查 權利 倫理	

18. 資通安全技術實務

課程項目	課程目標	課程大綱	學習方式
2.存取控制	2-1 (3 分) 2-2 (3 分)	安全政策規劃 風險管理實務	互動數位學習 -實作架構

3.通訊與網路安全	3-1 (3 分) 3-2 (3 分) 3-3 (3 分)	防火牆建構及設定 網路封包、流量解析與監控 網路攻擊技術分析 弱點掃瞄技術	-互動摸擬 -實作題 認證專班 *CISSP *CISA *GSEC (可依職能類別切割成不同的課程)
4.密碼學	4-1 (3 分) 4-2 (3 分) 4-3 (3 分)	密碼設計	
5.安全架構及模型	5-1 (3 分) 5-2 (3 分)	Windows 安全架構 Linux 安全架構 作業系統漏洞修補	
6.作業安全	6-1 (3 分) 6-2 (3 分) 6-3 (3 分)	資訊作業安全規劃	
7.應用系統與開發	7-1 (3 分) 7-2 (3 分) 7-3 (3 分)	應用系統與資料庫的維護規劃 惡意軟體攻擊防護	
10. 實體安全	10-1 (3 分) 10-2 (3 分)	實體安全制度規劃	

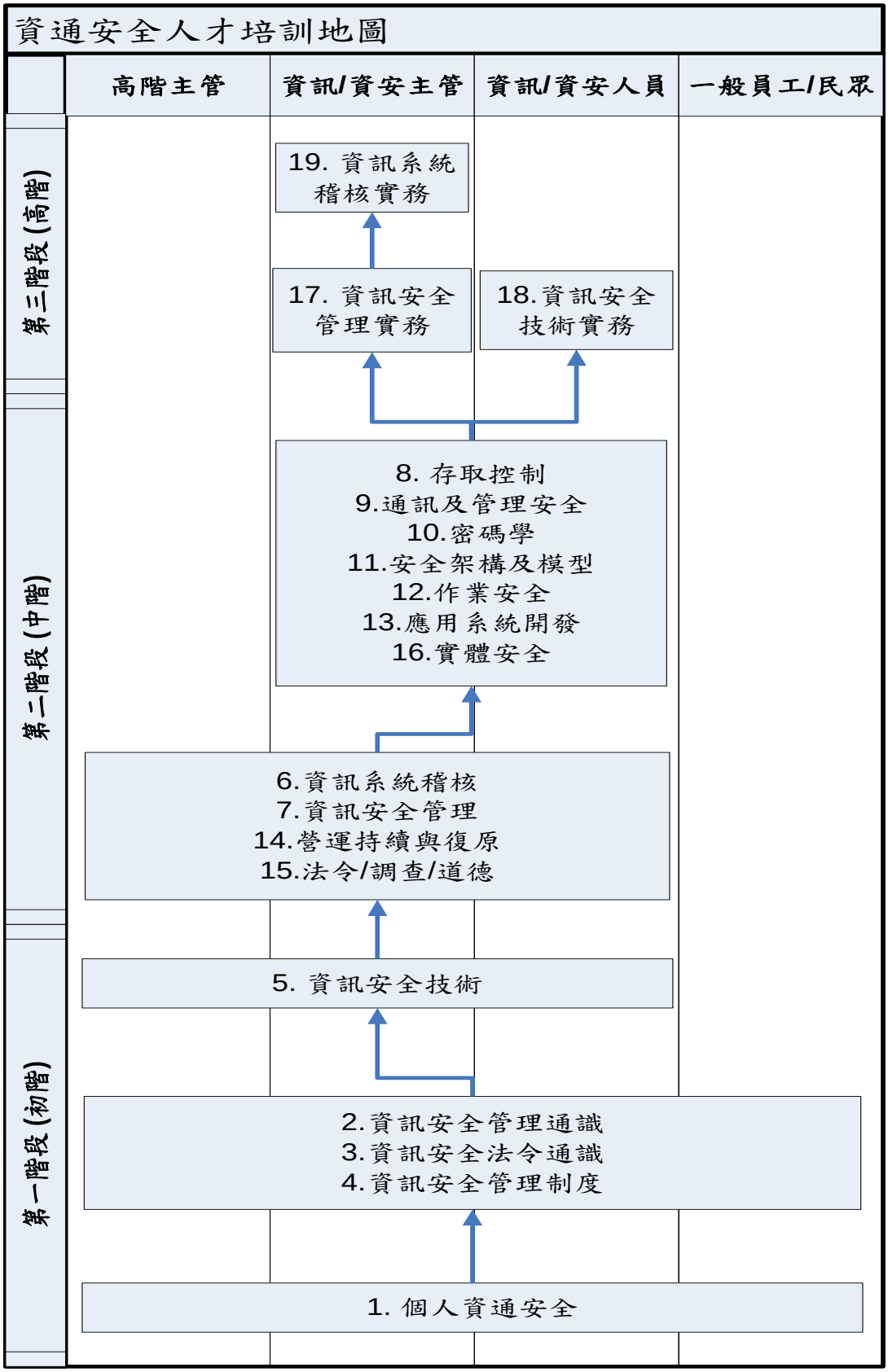
19. 資訊系統稽核實務

課程項目	課程目標	課程大綱	學習方式
11. 資訊系統稽核	11-1 (3 分) 11-2 (3 分) 11-3 (3 分)	風險分析 內部控制 資訊稽核之執行 自行評估 ISO 27001/17799	互動數位學習 -實作架構 -互動摸擬 -實作題 認證專班 *CISA *CISM *GSNA

2.5. 培訓地圖

本計畫根據各類人員的培訓目標與課程模組內容，所規劃之培訓地圖(Training Roadmap)如下頁，以明確描繪出在本培訓計畫，所要達成

的專案里程碑下，和各類人員應參加訓練的課程模組之先後順序。


資通安全人才培訓地圖
高階主管
資訊/資安主管
資訊/資安人員
一般員工/民眾
第三階段 (高階)
第二階段 (中階)
第一階段 (初階)
19. 資訊系統稽核實務
17. 資訊安全管理實務
18.資訊安全技術實務
8. 存取控制
9.通訊及管理安全
10.密碼學
11.安全架構及模型
12.作業安全
13.應用系統開發
16.實體安全
6.資訊系統稽核
7.資訊安全管理
14.營運持續與復原
15.法令/調查/道德
5. 資訊安全技術
2.資訊安全管理通識
3.資訊安全法令通識
4.資訊安全管理制度
1. 個人資通安全

2.6. 實施要點

(一) 培訓前

1.需求分析

1-1. 組織分析

為強化政府與民間機構的資訊安全管理機制，各組織可依據Hong, Chi, & Chao. (2003)所編制的資訊安全評估量表(如附件 2-A)進行自評，以瞭解組織在規劃與執行資訊安全管理系統上是否出現缺口。若不符預期，應進一步瞭解造成缺口的因素來自於技術資本投入不夠？資通衛防設施配置不佳？資訊安全政策規劃不當？亦或人員在資訊安全上的績效展現不足？

1-2 工作分析

若缺口因人員資訊安全績效不足所致，應針對不同類型的人員，改善不同類型的資訊安全行為。例如組織內部的高階主管，是否支持與推動組織資安管理制度與系統？組織資訊/資安主管，是否有效建立組織資安管理制度與系統？組織一般員工,是否遵守組織資訊安全制度？本培訓計畫 2.3 之(二)「人員目標」之各項指標，即可判斷資安績效展現是否足夠。而本計畫 2.3 之(三)的「培訓目標」又進一步定義了不同角色為達成人員目標，其背後應具備的資訊安全專業職能和水準為何。

1-3 人員分析

因此，在培訓計畫實施前，應先針對各類人員的資安績效指標(人員目標)進行評估，若不足，則應進一步對人員的資安

專業職能(培訓目標)進行評鑑，以作為培訓前的缺口分析工具，以了解各類人員在資安風險管理上的專業知識上有那些不足？差距多大？繼而才能根據本計畫的 2.5 培訓地圖，選合適合自己的課程模組。

2.課程規劃

2-1 數位學習

根據本計畫所設計的課程模組 1~19，建議與具公信力的數位影音教材製造商合作，共同編製數位課程，租賃或外包伺服器，免費供使用者於線上進行自我學習。或尋求能提供資訊安全數位學習的機構，根據課程模組內容，製作數位課程或學習光碟。或尋求已提供相似數位課程的機構(如由行政院研考會在文官學院所設計的數位資安課程、各地社區大學線上課程，皆可免費供民眾使用)。此外，NII 宣導的資通安全教材和講義，應放置(或提供超連結)在各社區大學學習網站、資策會、經濟部工業局、資安人等網頁，供民眾下載。

2-2 推廣專班

根據本計畫所設計的課程模組 1~5，可利用各社區大學之推廣課程進行。

2-3 認證專班

根據本計畫所設計的課程模組 6~19，與提供資訊安全相關認證考試訓練的機構合作(例如經濟部中小企業處、資訊工業策進會)，不限數位或實體教學，並以專案方式提供獎學金給取得認證學員 。

2-4 執行單位

課程階段	課程種類	主協辦單位	承辦單位	課程時數
初階	數位課程	研考會技服中心	研考會技服中心	5 組課程*1 小時
	推廣課程	教育部協請各縣市政府	社區大學	5 組課程*2 小時
中階	數位課程	研考會技服中心	研考會技服中心	11 組課程*1.5 小時
	認證專班	經濟部中小企業處、工業局、資策會	資安認證訓練機構	11 組課程*2 小時
高階	數位課程	研考會技服中心	研考會技服中心	3 組課程*2 小時
	認證專班	經濟部中小企業處、工業局、資策會	資安認證訓練機構	3 組課程*4 小時

(二) 培訓中

1. 擬建立資通安全學習護照，依本計畫的課程模組分類，蒐集各類人員的學習記錄、受訓小時數與相關認證資格。
2. 須蒐集所有的課程文件和教學檔案，並不定期檢核教案設計與培訓方式是否符合本計畫課程模組的課程大綱與目標。
3. 不定期勘察數位教學的環境，檢核是否提供充份的教具和設備給講師和學員，並作成查核記錄。
4. 對於需要實作的課程，亦須定期勘察互動數位課程是否有應用該課程模組中所有課程大綱的知識，並提供實作練習的機會。

(三) 培訓後

1. 須以問卷方式蒐集講師/訓練人員和學員對於課程的意見回

饋，並記錄之。

2. 須定期根據不同課程班別的意見回饋，做成檢討報告，以改善課程模組的內容設計，或改善課程規劃的活動。

3. 於課程結束前，須要求學員進行該課程模組所要求的課程大綱進行知識測驗，並在課程結束後一到三個月內，針對該課程模組所要求的課程目標，請學員進行職能自評，並記錄知識測驗與職能評鑑結果。

2.7. 培訓評估

(一) 學員反應

於課程結束前，須依照數位教學與實體認識專班不同的特性，自行設計或採用培訓機構的滿意度調查問卷，以瞭解學員對課程的滿意程度(包括教材內容、影音品質、連線速度、互動設計、課程時間)，以預測下一次參與課程的動機。

(二) 學習效果

為評估學員是否從課程中學到該課程大綱所期望的知識，須在課前與課後進行知識測驗。該知識測驗建議採題庫制。可針對每個課程模組，設計 2 個以上的測驗試卷，並在前後二次測驗中採不同試卷。

試卷包含的題目，須先委請該知識體系的專家進行主觀內容效度之檢核與調整，同時對不同試卷進行複本效度(Alternate forms reliability)的評估，建議最少為 0.7。

最後將兩次測驗的後測與前測的總分相減，以評估學員的相關知識是否因課程而增加，並作成記錄。或用整個班級學員的兩次的個別成績進行平均數的獨立性檢定(T test)，以判斷是否因

該課程創造前後知識的顯著性(p<=.05)差異(後測平均數須高於前測平均分數)。

(三) 行為改變

為評估該課程模組是否因此而提升學員的職能，並達到訓練遷移(Training Transfer)的效果。在學員上課前須用本計畫所設計的職能評鑑標準，依該課程模組所要求的課程目標，請學員先進行自評，並在課後一到三個月內，請求學員再一次進行相同的職能自評。經後測與前測相減，可了解各別學員是否因該課程而真正提升了職能水準。為減低其他因素的干擾，可針對同班級個別學員在職能自評項的前後測分數進行平均數的獨立性檢定(T test)，以判斷是否因該課程創造前後職能水準的顯著性(p<=.05)差異(後測平均數須高於前測平均分數)。

此外，為進一步確認每個課程模組的職能細項目標，是否可被歸類在同一個職能大項之課程項目，以確保學員在每個職能細項目上的平均得分合宜地反應該職能大項的職能水準，可進行內部一致性的信度分析，其指標為 Cronbach's α 係數，建議最少為 0.5。

(四) 培訓成果

為評估本培訓計畫是否達成預計的人員目標(即資通安全的績效展現)，在計畫開始前，須針對不同類型人員進行績效指標的評估和記錄，如本計畫 2.3 之(二)的人員目標所定義的衡量指標。

根據本計畫的專案里程碑所排定的階段，須定期評估上述績效指標的達成狀況。進行前後比對，以了解本計畫是否如期如質地達成預計的專案目標。

(五) 培訓報酬率

除了上述四個培訓評估項目外，為更進一步評估本培訓計畫之投資報酬率(Training ROI)，可採用簡單的方式進行，步驟如下：

1. 利用簡單迴歸分析(Regression Analysis)，將組織人員在資通安全職能的平均分數與組織資訊風險評比分數，得出判定係數百分比 X1。分析組織資訊風險評比分數與資訊安全事故成本之間的判定係數 X2。
2. 將所有組織資訊安全事故降低成本(例如:Annualized loss expectancy, ALE）除以本計劃的培訓成本，再乘上 X1 與 X2，即為簡單的培訓報酬率！

2.8. 培訓品質稽核表

構面	項目	投入	流程	產出
需求分析	組織分析	□組織資安風險評比 □組織 ALE	□培訓問題與對策 □培訓預算 □培訓時程表	□三階段培訓規劃書
	工作分析	□資安職能評鑑表 □專業證照體系表	□人員目標評估 □職能水準評鑑	□職能要求規範
	人員分析	□人員目標評估表 □專業職能評鑑表 □個人培訓記錄	□績效問題診斷表 □績效改善建議表 □職能缺口分析表	□個人培訓需求表
規　程	課程目標	□個人培訓需求表	□界定職能與水準	□課程目標

	培訓限制	□三階段培訓規劃書 □培訓地圖 □培訓機構清冊	□評估培訓限制	□培訓限制列表
	授課方法	□課程目標 □培訓限制列表 □學習方式列表 □培訓機構列表	□選擇的學習方式 □選擇培訓機構	□學習方式 □授課流程 □授課地點 □課程預算 □課程評估表 □訓練機構和契約
	計畫撰寫	□課程目標 □學習方式 □授課流程 □授課地點 □課程預算 □課程評估表 □培訓機構和契約 □作業流程檢核表	□撰寫授課計畫 □設計課程教材	□課程計畫書

構面	**項目**	**投入**	**流程**	**產出**
實施要項	**訓練前**	□課程計畫書	□訓練通知(學員) □教案設計(講師) □學員名單(講師)	□訓練通知文件 □講師/學員手冊 □報到名冊
	訓練中	□訓練通知文件 □報到名冊 □講師/學員手冊	□檢核教具教材 □檢核學員出席	□作業流程檢核表 □簽到表/簽入記錄
	訓練後	□作業流程檢核表 □簽到表/簽入記錄	□講師意見蒐集 □學員意見回饋	□意見彙整表
評　訓	**學員反應**	□意見彙整表 □學員滿意度問卷	□問卷實測與回收	□滿意度報告 □問題和對策報告

	學習效果	□知識測驗試卷	□訓練前測(自評) □訓練後測(自評)	□前後測評估報告
	行為改變	□職能評鑑表	□訓練前測(自評) □訓練後測(自評)	□前後測評估報告
	培訓成果	□個人目標評估表	□指標評估	□個人目標評估報告
	ROI	□培訓投入成本 □資安事故成本 □職能評鑑結果 □組織資安評比結果	□進行研究分析	□ROI 分析報告

附件 2-A

構面	準則
安全政策與資源	1.1 依據組織目標、策略、資訊政策及業務需要等 制定安全政策，並予文件化
	1.2 資訊安全政策之定期檢討修正
	1.3 設置資訊安全組織（人員）及資訊安全權責劃 分
	1.4 資訊安全資源規劃
	1.5 資訊安全預算
風險管理	2.1 進行資訊安全風險分析（威脅與弱點）
	2.2 資訊安全資產分類、區分機密等級、分別保護
	2.3 進行風險評估、差異分析（gap）
	2.4 資訊安全需求規劃與風險管理策略
人員安全	3.1 人員進用與調職之安全評估
	3.2 重要或特別權限人員之輪調、備援、權責分散
	3.3 對不同職務之資訊安全教育與訓練
	3.4 組織各階層之資訊安全意識
實體安全	4.1 依設備之重要程度區隔保護、管制及專人管理
	4.2 環境、電源之安全評估與控制
	4.3 機房與附屬設備之操作程序與管理
	4.4 硬體設備建置與維護之安全考量
系統與網路	5.1 系統與網路環境之設定與變更（如作業系統之 patch，未使用 port close 等）
	5.2 軟體開發與正式作業使用不同伺服器與資料庫
	5.3 內部網路與外部網路之區隔與安全措施(firewall、防毒、入侵偵測、弱點掃瞄等）
	5.4 資料傳輸與交換之安全控制（加密、數位簽章等）

附件2-A (續)

構面	準則
存取控制	6.1 使用者帳號與密碼管理,及其使用規範
	6.2 特權使用之限制與配置之管制
	6.3 對機密性、敏感性之系統與資料建立特別之 存取控制或保護措施
	6.4 網路之存取控制
軟體管理	7.1 將資訊安全列入應用系統開發與維護（含委外）的要求
	7.2 軟體執行碼之更新程序、專人管理與紀錄
	7.3 系統文件之管理、維護與保護
	7.4 軟體交換、引進新軟體之安全管制
業務持續運作	8.1 安全事故之通報與處理程序
	8.2 業務持續運作程序、定期演練與測試
	8.3 軟體與資料之備份與儲存媒體
	8.4 異地備援機制
資訊稽核	9.1 操作管理紀錄、日誌之記載與保管
	9.2 定期實施內外部稽核
	9.3 稽核結果之檢討修正與獎懲
	9.4 對資訊安全有關法令之遵守

參考文獻：

- 樊國楨 主編 (民 91)。資通安全專輯：資訊安全能力評鑑。國家實驗研究院科技政策研究與資訊中心。
- Cardy, R.L. & Dobbins, G.H. (1994). ***Performance Appraisal: alternative Perspective.*** South-Western.
- CISSP Common Body of Knowledge, CBK. (2004). International Information Systems Security Certification Consortium, Inc. (ISC)2.
- Huselid, M.A., Becker, B.E., & Beatty, R.W. (2005). ***The Workforce Scorecard: Managing Human Capital To Execute Strategy.*** Harvard Business School Press.
- Hong, K.S., Chi, Y.P., & Chao, L.R. (2003). A Study of Hierarchical Structure of Information Security Valuation Criteria. ***Journal of Library and Information Science***, 29(2), 22-44.
- ISO 10015: 1999. International Standard. Quality management Guidelines for training, 1-14.
- Mann, I. (2007). The human factor is key to good security. ***Computer Weekly***, 10 Apr.
- Noe, R.A. (2007). ***Employee Training and Development***. McGraw-Hill Education.
- Phillips, J.J. (2005). ***Handbook of Training Evaluation and Measurement Methods***. Jaico Publishing House.
- Spencer & Spencer (1993). ***Competence at work: model for superior performance.*** New York: John Wily.