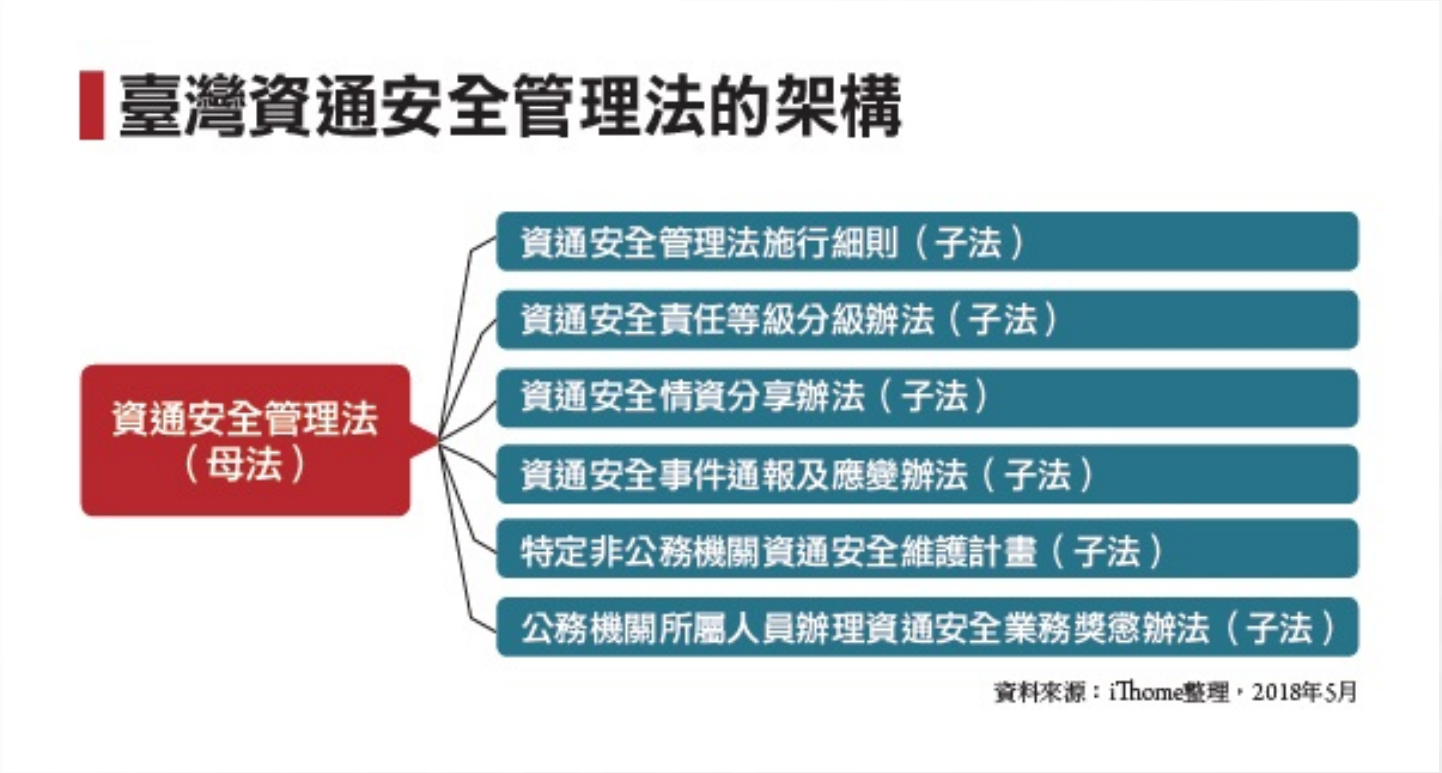
資通安全管理法暨執行細則

全方位解決方案

MICRO FOCUS®

政策面
行政院通過資通安全管理法

- 107年5月11日 立法院院會中，《資通安全管理法》三讀通過
- 107年6月6日 總統令公告



資通安全管理法適用對象

- 依據資通安全管理法第三條第五、六款
  - 公務機關：指依法行使公權力之中央、地方機關（構）或公法人。但不包括軍事機關及情報機關。
  - 特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。

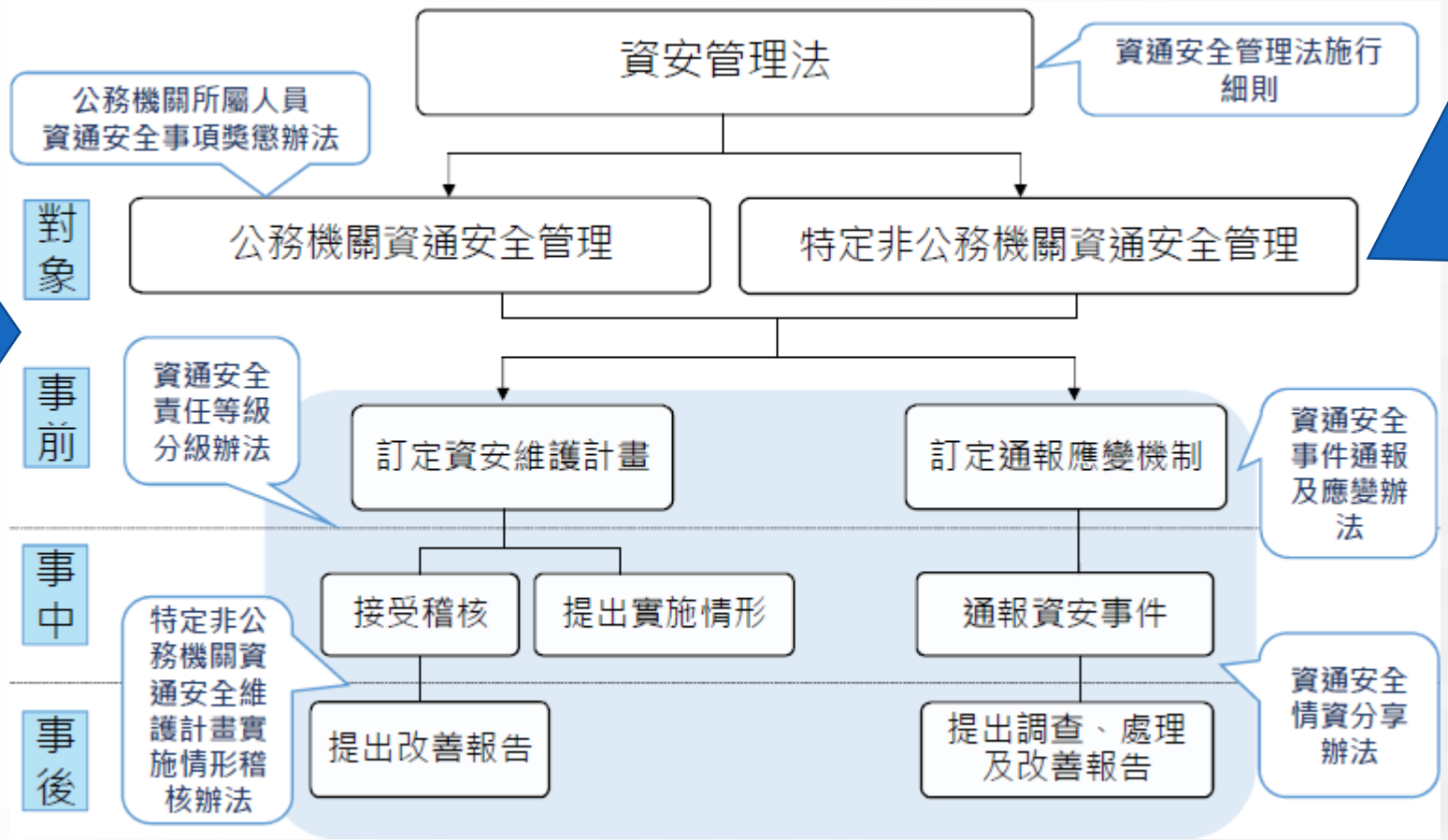
資安管理法架構

資通安全責任等級之公務機關**應辦事項**

- 應辦事項：詳附表一至附表八

資通系統分級及防護基準執行作業

- 資通系統防護分級及防護基準：詳附件九及附表十



未依規定制定資通安全計畫並且落實計畫者，依法可處10萬元以上100萬元以下罰鍰；

未依規定通報資通安全事件者，可處30萬元以上500萬元以下罰鍰，限期未改正者，按次處罰

資料來源: 行政院資通安全辦公室

資通安全責任等級之公務(非)機關應辦事項
應辦事項_管理面

辦理項目	辦理內容	A	B	C
資通系統分級及防護基準	完成資通系統分級，並完成防護基準；每年至少檢視一次妥適性	1年內	1年內	2年內
資訊安全管理系統之導入及通過公正第三方之驗證	全部核心資通系統導入資訊安全管理系統，並於三年內完成第三方驗證；並持續維持其驗證有效性	2年內	2年內	2年內
業務持續運作演練	全部核心資通系統	每年1次	每2年1次	每2年1次
辦理內部資通安全稽核		每年2次	每年1次	每2年1次
資通安全專責人員(一年內)		專職(責)4人	專職(責)2人	專職(責)1人
資安治理成熟度評估(公務機關)		每年1次	每年1次	

A與B級機關初次受核定或等級變更後之**一年內**依附表八完成資通系統分級，並完成附表九之控制措施。

C級機關若初次受核定或等級變更後之一年內依附表八完成資通系統分級，系統等級「高」者，應於初次受核定或等級變更後之**二年內**完成附表九之控制措施。

資料來源: 行政院資通安全辦公室

資通安全責任等級之公務(非)機關應辦事項

應辦事項_技術面(1/2)

辦理項目	辦理內容	A	B	C
安全性檢測	全部核心資通系統網站安全弱點檢測	每年2次	每年1次	每2年1次
	全部核心資通系統系統滲透測試	每年1次	每2年1次	每2年1次
資通安全健診	網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆連線設定檢視	每年1次	每2年1次	每2年1次
資通安全威脅偵測管理機制	完成威脅偵測機制建置，並持續維運	1年內	1年內	
	依主管機關指定之方式提交監控管理資料(公務機關)	V	V	

資料來源: 行政院資通安全辦公室

資通安全責任等級之公務(非)機關應辦事項
應辦事項_技術面(2/2)

辦理項目	辦理內容	A	B	C
資通安全防護(啟用，並持續使用及適時進行軟、硬體之必要更新或升級)	防毒軟體、網路防火牆、具有郵件伺服器者，應備電子郵件過濾機制	1年內	1年內	1年內
	IDS/IPS、具有對外服務之核心資通系統者，應備應用程式防火牆(WAF)	1年內	1年內	
	APT攻擊防禦	1年內		
政府組態基準	依主管機關公告之項目，完成政府組態基準導入作業，並持續維運(公務機關)	1年內	1年內	

資料來源: 行政院資通安全辦公室

資通安全責任等級之公務(非)機關應辦事項

應辦事項_認知與訓練

辦理項目	辦理內容	A	B	C
資通安全教育訓練	資通安全及資訊人員，每年接受之資通安全專業課程訓練或資通安全職能訓練	4名各12小時	2名各12小時	1名12小時
	一般使用者及主管，每人每年至少接受之一般資通安全教育訓練	3小時	3小時	3小時
資通安全專業證照及職能訓練證書	初次受核定或等級變更後之一年內，資通安全專職(責)人員總計應持有之資通安全專業證照，並持續維持證照之有效性	4張	2張	1張
	資通安全專職人員總計應持有之資通安全職能評量證書，並持續維持證照之有效性(公務機關)	4張	2張	1張

資料來源: 行政院資通安全辦公室

資通安全責任等級之公務(非)機關應辦事項

應辦事項_D級、E級

面向 / 作業名稱 / 等級	技術面	認知與訓練
	資通安全防護	資通安全教育訓練
D級	初次受核定或等級變更後之一年內，完成下列資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級 一、防毒軟體 二、網路防火牆 三、具有郵件伺服器者，應備電子郵件過濾機制	一般使用者及主管，每人每年至少接受三小時以上之一般資通安全教育訓練
E級		一般使用者及主管，每人每年至少接受三小時以上之一般資通安全教育訓練

資料來源: 行政院資通安全辦公室

資通系統分級及防護基準執行作業

機關資訊系統

依據資通系統防護需求分級原則 (附表八)

評量資訊系統等級 (高 / 中 / 普)

依據系統等級執行資安防護基準 (附表九)

附表八 資通系統防護需求分級原則

防護需求 等級構面	高	中	普
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。

資通系統防護分級及防護基準
七大構面29項控制措施類別

構面	控制措施類別
存取控制	帳號管理 最小權限 遠端存取
稽核與可歸責性	稽核事件；稽核紀錄內容 ；稽核儲存容量；稽核處理失效之回應 ；時戳及校時 稽核資訊之保護
營運持續計畫	系統備份 系統備援
識別與鑑別	內部使用者之識別與鑑別；身分驗證管理；鑑別資訊回饋；加密模組鑑別 ；非內部使用者之識別與鑑別
系統與服務獲得	系統發展生命週期需求階段；系統發展生命週期設計階段；系統發展生命週期開發階段 ；系統發展生命週期測試階段 ；系統發展生命週期部署與維運階段；系統發展生命週期委外階段 ；獲得程序 系統文件
系統與通訊保護	傳輸之機密性與完整性 資料儲存之安全
系統與資訊完整性	漏洞修復 資通系統監控 軟體及資訊完整性

控制措施1：存取控制

系統防護需求分級	高	中	普
措施內容			
帳號管理	一　逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出。 二　應依機關規定之情況及條件，使用資通系統。 三　監控資通系統帳號，如發現帳號違常使用時回報管理者。	一　已逾期之臨時或緊急帳號應刪除或禁用。 二　資通系統閒置帳號應禁用。 三　定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。	建立帳號管理機制，包含帳號之申請開通、停用及刪除之程序。
最小權限	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。		無要求。
遠端存取	一　應監控資通系統遠端連線。 二　資通系統應採用加密機制。 三　資通系統遠端存取之來源應為機關已預先定義及管理之存取控制點。 四　依維運需求，授權透過遠端執行特定之功能及存取相關資訊。		對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，並採用伺服端之集中過濾機制檢查使用者之授權。

控制措施1：存取控制
解決方案 :身分帳號存取與特權帳號管理

系統防護需求分級	高	中	普
措施內容			
帳號管理	一　逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出。 二　應依機關規定之情況及條件，使用資通系統。 三　監控資通系統帳號，如發現帳號違常使用時回報管理者。	一　已逾期之臨時或緊急帳號應刪除或禁用。 二　資通系統閒置帳號應禁用。 三　定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。	建立帳號管理機制，包含帳號之申請開通、停用及刪除之程序。
最小權限	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。		無要求。
遠端存取	一　應監控資通系統遠端連線。 二　資通系統應採用加密機制。 三　資通系統遠端存取之來源應為機關已預先定義及管理之存取控制點。 四　依維運需求，授權透過遠端執行特定之功能及存取相關資訊。		對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，並採用伺服端之集中過濾機制檢查使用者之授權。

身分帳號管理
Identity and Access Manager (IAM)
存取與特權帳號管理
Access Manager & PAM

控制措施2:稽核與可歸責性

系統防護需求分級 / 措施內容	高	中	普
稽核事件	一 應定期審查稽核事件。		一 依規定時間週期及紀錄留存政策，保留稽核紀錄。 二 確保資通系統有稽核特定事件之功能，並決定應稽核之特定資通系統事件。 三 應稽核資通系統管理者帳號所執行之各項功能。 四 依規定時間週期及紀錄留存政策，保留稽核紀錄。 五 確保資通系統有稽核特定事件之功能，並決定應稽核之特定資通系統事件。 六 應稽核資通系統管理者帳號所執行之各項功能。
稽核紀錄內容	一 資通系統產生之稽核紀錄，應依需求納入其他相關資訊。		一 資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌紀錄機制，確保輸出格式的一致性。 二 資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌紀錄機制，確保輸出格式的一致性。
稽核儲存容量	一 依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。		
稽核處理失效之回應	一 機關規定需要即時通報之稽核失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。	一 資通系統於稽核處理失效時，應採取適當之行動。	
時戳及校時	一 系統內部時鐘應依機關規定之時間週期與基準時間源進行同步。		一 資通系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對映到世界協調時間(UTC)或格林威治標準時間(GMT)。
稽核資訊之保護	一 定期備份稽核紀錄至與原稽核系統不同之實體系統。	一 應運用雜湊或其他適當方式之完整性確保機制	一 對稽核紀錄之存取管理，僅限於有權限之使用者。

控制措施2:稽核與可歸責性
解決方案 :日誌管理與系統稽核管理

系統防護需求分級	高	中	普
措施內容			
稽核事件	一 應定期審查稽核事件。		一 依規定時間週期及紀錄留存政策，保留稽核紀錄。 二 確保資通系統有稽核特定事件之功能，並決定應稽核之特定資通系統事件。 三 應稽核資通系統管理者帳號所執行之各項功能。 四 依規定時間週期及紀錄留存政策，保留稽核紀錄。 五 確保資通系統有稽核特定事件之功能，並決定應稽核之特定資通系統事件。 六 應稽核資通系統管理者帳號所執行之各項功能。
稽核紀錄內容	一 資通系統產生之稽核紀錄，應依需求納入其他相關資訊。		一 資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌紀錄機制，確保輸出格式的一致性。 二 資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌紀錄機制，確保輸出格式的一致性。
稽核儲存容量	一 依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。		
稽核處理失效之回應	一 機關規定需要即時通報之稽核失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。	一 資通系統於稽核處理失效時，應採取適當之行動。	
時戳及校時	一 系統內部時鐘應依機關規定之時間週期與基準時間源進行同步。		一 資通系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對映到世界協調時間(UTC)或格林威治標準時間(GMT)。
稽核資訊之保護	一 定期備份稽核紀錄至與原稽核系統不同之實體系統。	一 應運用雜湊或其他適當方式之完整性確保機制	一 對稽核紀錄之存取管理，僅限於有權限之使用者。

日誌管理與系統稽核管理
ArcSight, Sentinel,
Change Guardian, PAM

控制措施3:營運持續計畫

系統防護需求分級	高	中	普
措施內容			
系統備份	一　應將備份還原，作為營運持續計畫測試之一部分。 二　應在與運作系統不同處之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。	一　應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。	一　訂定系統可容忍資料損失之時間要求。 二　執行系統源碼與資料備份。
系統備援	一　訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。 二　原服務中斷時，由備援設備取代提供服務。		

控制措施3:營運持續計畫
解決方案 :備份與災難復原

系統防護需求分級	高	中	普
措施內容			
系統備份	一　應將備份還原，作為營運持續計畫測試之一部分。 二　應在與運作系統不同處之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。	一　應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。	一　訂定系統可容忍資料損失之時間要求。 二　執行系統源碼與資料備份。
系統備援	一　訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。 二　原服務中斷時，由備援設備取代提供服務。		

備份與災難復原
Data Protector
& PlateSpin

控制措施4:識別與鑑別

系統防護需求分級 措施內容	高	中	普
內部使用者之識別與鑑別	一　對帳號之網路或本機存取採取多重認證技術。	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能 禁止使用共用帳號。	
身分驗證管理	一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 二、密碼重設機制對使用者重新身分確認後發送一次性及具有時效性符記。	一、使用預設密碼登入系統時，應於登入後要求立即變更。 二、身分驗證相關資訊不以明文傳輸。 三、基於密碼之鑑別資通系統應強制最低密碼複雜度；強制密碼最短及最長之效期限制。 四、使用者更換密碼時，至少不可以與前三次使用過之密碼相同。 五、具備帳戶鎖定機制，帳號登入進行身分驗證失敗達三次後，至少十分鐘內不允許該帳號繼續嘗試登入。 六、上述第三點至第五點對非內部使用者，可依機關自行規範辦理	
鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。		
加密模組鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	無要求。	
非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為的程序)。		

控制措施4:識別與鑑別
解決方案 :多因子認證與身分存取管理

系統防護需求分級 措施內容	高	中	普
內部使用者之識別與鑑別	一、對帳號之網路或本機存取採取多重認證技術。	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	
身分驗證管理	一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 二、密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。		一、使用預設密碼登入系統時，應於登入後要求立即變更。 二、身分驗證相關資訊不以明文傳輸。 三、使用密碼進行鑑別時，資通系統應強制最低密碼複雜度；強制密碼最短及最長之效期限制。 四、使用者更換密碼時，至少不可以與前三次使用過之密碼相同。 五、具備帳戶鎖定機制，帳號登入進行身分驗證失敗達三次後，至少十五分鐘內不允許該帳號繼續嘗試登入。 六、上述第三點至第五點對非內部使用者，可依機關自行規範辦理
鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。		
加密模組鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。		無要求。
非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為的程序)。		

多因子認證與身分存取管理
Advanced Authentication
& Access Manager (AM)

控制措施5:系統與服務獲得

系統防護需求分級 措施內容	高	中	普
系統發展生命週期需求階段	針對系統安全需求（含機密性、可用性、完整性），以檢核表方式進行確認。		
系統發展生命週期設計階段	一　根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。 二　將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。		無要求。
系統發展生命週期開發階段	一　執行「源碼掃描」安全檢測。 二　具備系統嚴重錯誤之通知機制。	一　應針對安全需求實作必要控制措施。 二　應注意避免軟體常見漏洞及實作必要控制措施。 三　發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息。	
系統發展生命週期測試階段	一　執行「滲透測試」安全檢測。	執行「弱點掃描」安全檢測。	
系統發展生命週期部署與維運階段	一　於系統發展生命週期之維運階段，須注意版本控制與變更管理。		一　於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。 二　資通系統相關軟體，不使用預設密碼。
系統發展生命週期委外階段	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。		
獲得程序	開發、測試及正式作業環境應為區隔。		無要求。
系統文件	應儲存與管理系統發展生命週期之相關文件。		

控制措施5:系統與服務獲得
解決方案 :軟體開發生命週期管理 & 黑白箱掃描工具

系統防護需求分級	高	中	普
措施內容			
系統發展生命週期需求階段	針對系統安全需求（含機密性、可用性、完整性）以檢核表方式進行確認。		
系統發展生命週期設計階段	一　根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。 二　將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。		無要求。
系統發展生命週期開發階段	一　執行「源碼掃描」安全檢測。 二　具備系統嚴重錯誤之通知機制。	一　應針對安全需求實作必要控制措施。 二　發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息。	
系統發展生命週期測試階段	一　執行「滲透測試」安全檢測。	執行「弱點掃描」安全檢測。	
系統發展生命週期部署與維運階段	一　於系統發展生命週期之維運階段，須注意版本控制與變更管理。	一　於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。 二　資通系統相關軟體，不使用預設密碼。	
系統發展生命週期委外階段	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。		
獲得程序	開發、測試及正式作業環境應為區隔。		無要求。
系統文件	應儲存與管理系統發展生命週期之相關文件。		

控制措施6:系統與通訊保護

系統防護需求分級 措施內容	高	中	普
傳輸之機密性與完整性	一　資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。 二　使用公開、國際機構驗證且未遭破解的演算法。 三　使用演算法支援的最大長度金鑰 四　加密金鑰或憑證週期性更換。	無要求。	無要求。
資料儲存之安全	靜置資訊及相關具保護需求之機密資訊應加密儲存。	無要求。	無要求。
漏洞修復	一　定期確認資通系統相關漏洞修復之狀態。		系統之漏洞修復應測試有效性及潛在影響，並定期更新。

控制措施6:系統與通訊保護
解決方案 :資料安全加密 &主機自動化與弱點管理

系統防護需求分級	高	中	普
措施內容			
傳輸之機密性與完整性	一　資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。 二　使用公開、國際機構驗證且未遭破解的演算法。 三　使用演算法支援的最大長度金鑰。 四　加密金鑰或憑證週期性更換。	無要求。	無要求。
資料儲存之安全	靜置資訊及相關具保護需求之機密資訊應加密儲存。	無要求。	無要求。
漏洞修復	一　定期確認資通系統相關漏洞修復之狀態。		二　對於漏洞修復應測試有效性及潛在影響，並定期更新。

資料安全加密Voltage
ZENworks磁碟加密

主機自動化與弱點管理
Server Automation & ZENworks Patch Mgmt

控制措施7:系統與資訊完整性

系統防護需求分級 措施內容	高	中	普
漏洞修復	一　定期確認資通系統相關漏洞修復之狀態。		系統之漏洞修復應測試有效性及潛在影響，並定期更新。
資通系統監控	一　資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。	一　監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。	發現資通系統有被入侵跡象時，應通報機關特定人員。
軟體及資訊完整性	一　應定期執行軟體與資訊完整性檢查。	一　使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。 二　使用者輸入資料合法性檢查應置放於應用系統伺服器。 三　發現違反完整性時，資通系統應實施機關指定之安全保護措施。	無要求。

控制措施7:系統與資訊完整性
解決方案 :弱點管理 &資安監控中心與身分存取管理

系統防護需求分級	高	中	普
措施內容			
漏洞修復	一　定期確認資通系統相關漏洞修復之狀態。		系統之漏洞修復應測試有效性及潛在影響，並定期更新。
資通系統監控	一　資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。	一　監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。	發現資通系統有被入侵跡象時，應通報機關特定人員。
軟體及資訊完整性	一　應定期執行軟體與資訊完整性檢查。	二　使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。 三　發現違反完整性時，資通系統應實施機關指定之安全保護措施。	一　使用者輸入資料合法性檢查應置放於應用系統伺服器。

弱點管理 SA & ZENworks

資安監控中心與身分存取管理

SIEM & IAM solution & ZENWorks

資通系統防護分級及防護基準方案對應解決方案(1/2)

構面	實施內容	解決方案	產品名稱
存取控制	帳號管理	身分帳號存取管理	Identity and Access Manager (IAM)
	最小權限	身分帳號存取管理	Identity and Access Manager (IAM)
	遠端存取	存取管理&特權帳號管理	Access Manager & PAM
稽核與可歸責性	稽核事件	日誌管理與系統稽核管理	ArcSight ADP Logger or Sentinel 系統稽核Change Guardian 資通系統管理者帳號稽核PAM
	稽核紀錄內容	日誌管理與系統稽核管理	
	稽核儲存容量	日誌管理與系統稽核管理	
	稽核處理失效之回應	日誌管理與系統稽核管理	
	時戳及校時	日誌管理與系統稽核管理	
	稽核資訊之保護	日誌管理與系統稽核管理	
營運持續計畫	系統備份	備份與災難復原	Data Protector
	系統備援	備份與災難復原	Data Protector & PlateSpin
識別與鑑別	內部使用者之識別與鑑別	多因子認證與身分存取管理	Advanced Authentication & Access Manager (AM)
	身分驗證管理		
	鑑別資訊回饋		
	加密模組鑑別		
	非內部使用者之識別與鑑別		

資通系統防護分級及防護基準方案對應解決方案(2/2)

構面	實施內容	解決方案	產品名稱
系統與服務獲得	系統發展生命週期需求階段	軟體開發生命週期管理	ALM Requirement Management
	系統發展生命週期設計階段	人力進行風險評估並提供修正	人力作業
	系統發展生命週期開發階段	應用程式資安原始碼掃描與測試工具	Fortify SCA & Webinspect
	系統發展生命週期測試階段	外部顧問進行滲透測試與軟體掃描	人力作業
	系統發展生命週期部署與維運階段	版本控管與機房自動化	Dimension CM (Serena) Release Control/ Deployment Automation Data Center Automation
	系統發展生命週期委外階段	將安全需求（含機密性、可用性、完整性）納入委外契約	人力作業
	獲得程序	分別建構開發、測試及正式作業環境	人力作業
	系統文件	軟體生命週期管理	ALM Requirement+ Defect
系統與通訊保護	傳輸之機密性與完整性	資料安全加密	Voltage & ZENworks磁碟加密
	資料儲存之安全	主機自動化與弱點管理	Server Automation & ZENworks
系統與資訊完整性	漏洞修復	主機自動化與弱點管理	ZENworks Patch Management, Server Automation
	資通系統監控	資安監控管理平台與身分存取管理	SIEM+IAM solution + ZENworks
	軟體及資訊完整性	資安監控管理平台與身分存取管理	SIEM+IAM solution + ZENworks

WHY Micro Focus

- 單一軟體公司可符合大1-7項資通安全管理法之防護基準要求。
- 在台灣政府與企業之大型專案都有許多成功案例。
- 各種解決方案在國內外客戶都有多年使用經驗，且持續使用中。
- 台灣政府軍方國安與府院高層均採用。
- 國內外資安專業服務團隊人數及資源最多。

Q & A