INDUSTRIAL DEVELOPMENT BUREAU,
MINISTRY OF ECONOMIC AFFAIRS
經 濟 部 工 業 局

資安相關規範說明

111年3月

INDUSTRIAL DEVELOPMENT BUREAU,
MINISTRY OF ECONOMIC AFFAIRS
經 濟 部 工 業 局

簡報大綱

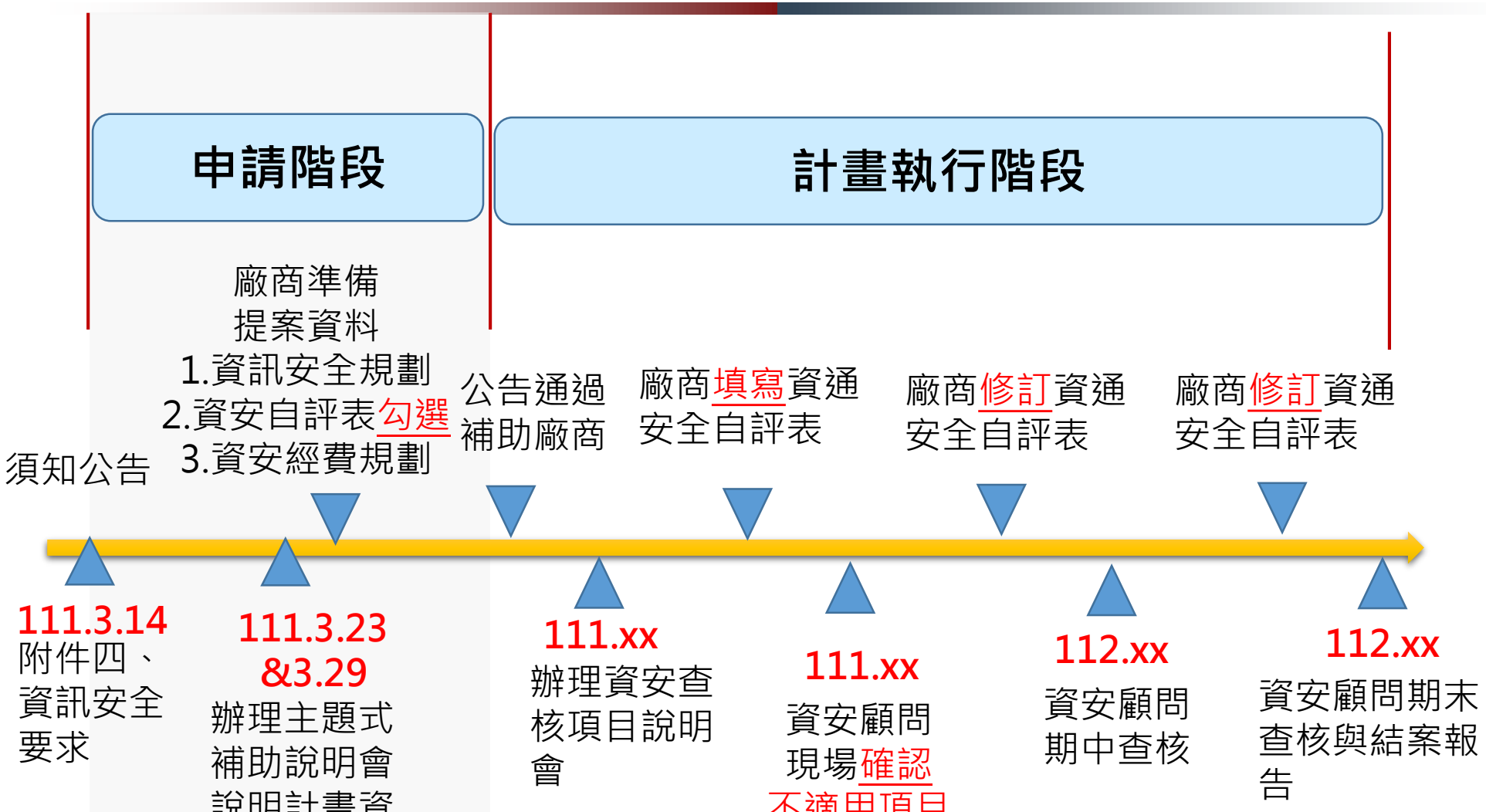
壹、資安自評與查核流程

貳、「提案階段」資安規劃

參、「執行階段」資安要求

INDUSTRIAL DEVELOPMENT BUREAU, MINISTRY OF ECONOMIC AFFAIRS
經 濟 部 工 業 局

壹、資安自評與查核流程



INDUSTRIAL DEVELOPMENT BUREAU, MINISTRY OF ECONOMIC AFFAIRS
經 濟 部 工 業 局

貳、「提案階段」資安規劃(1/3)

一.資安管理:

請提案廠商須說明雲服務在建置及營運時採用的資安管理項目，且建置及導入35%以上應為國內業者產品及服務，計畫驗收至少須達必要要求之條件如下:

依序	項目	說明
1	網路管理	須有防火牆、入侵偵測等資安設備保護，若透過遠端連線進行管理則必須透過加密通道，登入時必須採用安全的身分鑑別機制。
2	資料安全	應具體說明包含啟用資料加密、保護資料之傳輸、紀錄存取機敏資料，以及定期備份資料等。
3	存取控制	應具體說明包含實體存去限制、異常通報機制、異常日誌紀錄以及防竄改機制等。
4	資安管理	應具體說明包含強制使用強密碼、限制遠端對安全網路的存取、密鑰管理的職責分離以及保持軟體/韌體更新等。
5	營運持續	應具體說明包含加密備份、自我監測、監控及偵測容量使用情況等。
6	生命週期保護	應具體說明包含資通訊系統須於上線前及營運期間定期進行弱點掃描及滲透測試，高風險漏洞應被評估並依計畫可接受方式處理。

貳、「提案階段」資安規劃(2/3)

二.資安資源投入說明:

(一)請提案廠商須詳細填妥資安管理自評表

自評項目		項目說明	自我評核				佐證資料說明	顧問查核結果			
			符合	部分符合	不符合	不適用		符合	部分符合	不符合	不適用
使用防火牆與VPN	須有防火牆、入侵偵測等資安設備保護，若透過遠端連線進行管理則必須透過加密通道，登入時必須採用安全的身分鑑別機制。	請受查驗計畫提供網路架構圖，簡述防禦機制是否合理跟恰當。				V					
資料安全											
啟用資料加密	對於資通訊系統中的資料應評估決定是否採取加密保護措施。	計畫應評估資通訊系通那些需要加密保護，並使用業界公認									

如勾選不適用，
廠商須說明原因

貳、「提案階段」資安規劃(3/3)

二.資安資源投入說明:

(二)請提案廠商須說明資安支出規劃，填寫範例如下。

資安項目	內容說明	適用管理項目	支出經費(千元)	占總經費比率
(範例 1) 單網域 SSL 憑證(1 年)	XXX 資訊應用服務系統 https 加密傳輸使用	網路管理 (保護資料之傳輸，使用及儲存)	15	X%
(範例 2) 網站落點掃描(WebVA)-遠端服務(1 個 URL)	XX 資訊應用服務軟體-弱點掃描	生命週期保護 (進行安全檢測)	9.69 以【108 年第 5 次電腦軟體共同供應契約-資通安全服務】收費標準為例	Y%
(範例 3) 教育訓練	雲服務資安教育訓練	營運持續 (提高企業資安認知)	50	Y%

INDUSTRIAL DEVELOPMENT BUREAU, MINISTRY OF ECONOMIC AFFAIRS
經 濟 部 工 業 局

參、「執行階段」資安要求(1/8)

-共同規範-

一. 提案廠商須提出雲服務的資訊安全規劃，包含定期審查服務流程並持續改善，以達到資安防護之目的。

二. 雲服務相關產品如已有國家資安相關檢測標準，須採用通過資安驗證之產品。

三. 資訊安全項目經費應占總經費合理比例，驗收時應提供支付資安廠商之給付證明、說明於該案中所提供之產品及服務、解決哪些資安需求等。

四. 資安業者不應有過度再外包的情形 (不得超過資安經費50%)。

五. 使用的資安軟、韌、硬體產品，不得為中國大陸生產或開發。

六. 計畫內資安軟、韌、硬體產品，非國內 (台製)之資安產品佔比不得超過資安經費的 50%；若有特殊情形，須於計畫書、審查會中明文說明。

INDUSTRIAL DEVELOPMENT BUREAU,
MINISTRY OF ECONOMIC AFFAIRS
經 濟 部 工 業 局

參、「執行階段」資安要求(2/8)

-必要要求-

一. 網路管理:

使用防火牆與VPN

二. 資料安全:

啟用資料加密、保護資料之傳輸、紀錄存取機敏資料、定期備份資料

三. 存取控制:

實體存取限制、異常通報機制、異常日誌紀錄、防竄改機制

四. 資安管理:

強制使用強密碼、限制遠端對安全網路的存取、密鑰管理職責分離、保持軟體/韌體更新

五. 營運持續:

加密備份、自我監測、監控及偵測容量使用情況、進行多雲架構的服務備援機制

六. 生命週期保護:

進行安全檢測

參、「執行階段」資安要求(3/8)

-必要要求-

一.網路管理:

- 須有防火牆、入侵偵測等資安設備保護，若透過遠端連線進行管理則必須透過加密通道，登入時必須採用安全的身分鑑別機制。

參、「執行階段」資安要求(4/8)

-必要要求-

二.資料安全:

- 啟用資料加密：對於資通訊系統中的資料應評估決定是否採取加密保護措施。
- 保護資料之傳輸，使用及儲存：若存在機敏性資料時，無論傳輸、使用和儲存都應進行加密保護。
- 紀錄存取機敏資料：針對機敏性資料的存取應控管並留存相關日誌紀錄。
- 定期備份資料：應對資料進行備份。

參、「執行階段」資安要求(5/8)

-必要要求-

三.存取控制:

- 實體存取限制：應有實體安全的保護措施，外連線端口需最小化管理機制。
- 異常通報機制：若服務發生異常時 (包含但不限於 服務中斷、更新失敗)，需有通知管道或機制。
- 異常日誌紀錄：針對資通訊系統的異常狀況應有日誌紀錄。
- 防竄改機制：應確保資通訊系統內的資料防竄改機制：應確保資通訊系統內的資料(設定檔、程式碼、資料庫等設定檔、程式碼、資料庫等)不被不被未經授權的篡改。未經授權的篡改。

參、「執行階段」資安要求(6/8)

-必要要求-

四.資安管理:

- 強制使用強密碼：應建立密碼管理機制，系統應審核所使用之密碼強度，並提供密碼恢復及重置機制
- 限制遠端對安全網路的存取：對於遠端連線應實施適當的存取管制，至少包含使用加密方式通訊、依工作性質給予 低權限權、應保留遠端連線日誌
- 密鑰管理的職責分離：對於金鑰的產生、儲存與使用應保存日誌紀錄，宜採用職責分離方式管理金鑰
- 保持軟體 /韌體更新：資通訊系統應建立軟體、韌體安全性更新機制及部署時機，若更新部署失敗應可成功回復至前一個版本

參、「執行階段」資安要求(7/8)

-必要要求-

五.營運持續:

- 加密備份：應識別重要的應用程式、設定檔、機敏資料並進行加密備份
- 自我監測：資通訊系統應建立自我檢測功能，如完整性檢查、定期回報、零組件異常偵測，若發生上述情況時應有發送通知機制
- 監控及偵測容量使用情況：應監控全資通訊系統使用狀況，如：CPU、記憶體、儲存空間、頻寬使用率 ...等若達到警戒值應存日誌紀錄並進行通知 。全資通訊系統需符合計畫自訂的可用性百分比
- 進行多雲架構的 服務備援機制：應建立業務持續運作計畫 (BCP) 或災難復原計畫 (DRP)，定期進行演練並持續改善

參、「執行階段」資安要求(8/8)

-必要要求-

六.生命週期保護:

- 進行安全檢測：資通訊系統須於上線前及營運期間定期進行弱點掃描及滲透測試，高風險漏洞應被評估並依計畫可接受方式處理

簡報結束
敬請指教