導入資訊安全之安全控制措施，以強化資訊系統安全及風險管理。

資安選擇控制措施架構說明

◎林子群

壹、前言

資安選擇控制措施旨在為支援政府機關執行業務之資訊系統，提供安全控制措施有關「選擇」與「描述」的指導，可應用在處理、儲存及傳輸政府機關資訊之資訊系統所有元件，並且透過下列來協助政府機關強化資訊系統安全及更有效的風險管理：

1. 採用具一致性、可比較性及可重複性的方法為資訊系統選擇與描述安全控制措施。
2. 提供資訊系統分類分級之各級「安全等級」選擇控制措施的建議。
3. 提供穩健且具備彈性的安全控制措施目錄，以符合目前機關資訊系統安全防護的需求，並考慮在持續變動的安全需求及技術的發展下，也能符合未來防護的要求。

貳、資訊安全控制措施的分類

資訊安全控制措施的分類方式，為融合ISO/IEC 27002:2005與NIST SP800-53 Rev3之分類方式，以ISO/IEC 27002:2005的11項安全控制節次（Clause）為控制措施之「主分類」，以NIST SP800-53的16項安全控制族系（Family）為控制措施之「次分類」，詳見表1。

表1　安全控制措施的分類

章節	主分類	章節	次分類	類別
5	安全政策與程序	5.1	資訊安全政策與程序	管理類
6	資訊安全的組織	6.1	內部組織	管理類
		6.2	外部團體	管理類
		6.3	規劃	管理類
		6.4	安全評估及授權	管理類
7	資產管理	7.0	組態管理	操作類
8	人力資源安全	8.1	人力資源安全	操作類
		8.2	認知及訓練	操作類
9	實體與環境安全	9.1	實體與環境保護	操作類
		9.2	維護	操作類
10	通訊與作業管理	10.1	系統與網路連線防護	技術類
		10.2	系統與資訊完整	操作類
		10.3	媒體保護	操作類
11	存取控制	11.1	識別與鑑別	技術類
		11.2	存取控制	技術類
		11.3	稽核與可歸責性	技術類
12	資訊系統獲取、開發及維護	12.1	系統和服務獲取	管理類
13	資訊安全事故管理	13.1	事故反應	操作類
14	營運持續管理	14.1	緊急應變規劃	操作類
15	遵循性	15.1	遵循適法性要求	管理類
		15.2	安全政策與標準的遵循性以及技術遵循性	管理類

資料來源：行政院研考會「安全控制措施參考指引」

參、安全控制措施內容說明

安全控制措施內容包含控制措施編號、控制措施名稱、控制措施、實作指引、強化控制措施、控制措施應明確定義的參數、參考資料、優先序等。內容範例詳見圖1，分述如下：

9.1.5.實體存取監視

・控制措施：
機關：
監視資訊系統的實體存取，以偵測及回應實體安全事故。
定期審查實體存取紀錄。
與機關的事故反應能量協調審查及調查的結果。

・實作指引：
調查及回應偵測到的實體安全事故，包含明顯的安全違規或可疑的存取行為，是機關事故反應能量的一部分。

・強化控制措施：
（1）機關監視即時的實體入侵警報及監視設備。
（2）機關採用自動化機制來識別潛在的入侵及啟動指定的回應動作。

・控制措施應明確定義的參數：
定義定期審查實體存取紀錄的頻率。

・參考資料：
ISO/IEC 27002:2005：9.1.2、9.1.5、10.10.2。
NIST SP800-53 Rev3：PE-6。

・優先序：第一優先。

資料來源：行政院研考會「安全控制措施參考指引」

圖1　安全控制措施範例

一、控制措施編號：為利於識別每一項控制措施，其第一階編號（如：9）及第二階編號（如：9.1）分別為控制措施的「主分類」及「次分類」，第三階編號（如：9.1.5）則為「安全控制措施編號」（如：圖1中第一行之「9.1.5」）。

二、控制措施名稱：跟隨在控制措施編號之後的標題文字即為控制措施的名稱（如：圖1中第一行之「實體存取監視」）。

三、控制措施：為該項控制措施的說明欄位，用來定義該控制措施的各項「基本要求」；機關若選用該控制措施，則必須實作該項控制措施的所有基本要求。

四、實作指引：進一步說明控制措施要求的內容及實作建議，有些會透過舉例指引使用人使其更了解控制措施要求的內涵。

五、強化控制措施：為該控制措施基本要求的延伸及強化要求之項目，機關可參考「資訊系統分類分級與鑑別機制參考手冊」對資訊系統所分類之「安全等級（普、中、高）」，再依「安全措施參考指引」之安全控制措施基準表的建議來選用強化控制措施。機關亦可依機關風險評鑑之結果視需要選擇。

每一控制措施中之強化控制措施編號以「(1)、(2)、(3)…」依序編號，完整的強化控制措施編號前應加上控制措施編號（如：9.1.5(1)）；選用強化控制措施編號必須包含其控制措施之「基本要求」。

六、控制措施應明確定義的參數：在控制措施基本要求或強化控制措施中，若有需要機關再明確定義的相關參數，會在本項目中描述。相關參數應明確定義在資安政策文件中，或者在程序文件或內部相關規定文件中明確記載，如：應定期執行事項的頻率或期限、機關可容許特定狀況的最大值或最小值等。

七、參考資料：本項為控制措施與其他安全控制措施標準（如：ISO/IEC 27002:2005或NIST SP800-53 Rev3）或其他實作安全控制措施之參考指引（如：研考會發展之相關資訊安全參考指引或NIST SP800系列的文件）的參考資料。

八、優先序：機關選用所需之控制措施後，可依控制措施的優先序來安排控制措施實作的先後次序。控制措施的優先序分為四種，即：最先、次之、最後、無，詳見表2。

表2　控制措施優先序

優先序	順序	動作
第一優先	最先	優先實作「第一」優先序的控制措施
第二優先	次之	完成「第一」優先序控制措施的實作後，再實作「第二」優先序的控制措施
第三優先	最後	完成「第一」、「第二」優先序控制措施的實作後，再實作「第三」優先序的控制措施
無	無	安全等級防護基準未選用之控制措施

資料來源：行政院研考會「安全控制措施參考指引」

控制措施優先序的建議，在於確保基礎性的控制措施優先被實作，再架構基礎控制措施的其他控制措施。這個建議作法可以讓機關在有限的資源內優先實作重要的控制措施，同時使得控制措施的實作更具結構性與時效性。

肆、安全控制措施防護基準

安全控制措施防護基準是描述資訊系統依「資訊系統分類分級與鑑別機制參考手冊」評定的資訊系統各級「安全等級（普、中、高）」防護基準，所建議選用之初始安全控制措施只適用在採用「高階風險評鑑作法」的資訊系統環境。其基準表中包含107項「普」級控制措施計、155項「中」級控制措施計及162項「高」級控制措施計，其餘24項為安全等級基準在普、中、高均標示為「不適用」的項目。這些控制措施為提供機關必要時可選用之參考。詳細內容，詳見行政院研考會「安全控制措施參考指引」。

如果控制措施在其中一個基準中被選用，那麼在相對應的欄位中就會標定該控制措施的編號；如果在特定基準中沒有選用該項控制措施，則該欄位會標示「不適用」。例如：「9.1.5(1)(2)」被標示在「9.1.5」的「高」基準欄位中，就表示若資訊系統之安全等級為「高」且選用「9.1.5」這項控制措施的話，則需實作「9.1.5控制措施」的基本要求外，尚包含其強化控制措施「9.1.5(1)」及「9.1.5(2)」。

標示為「不適用」的欄位僅代表在特定基準中，採用「高階風險評鑑作法」「選擇初始安全控制措施」時，沒有建議選用該項控制措施，並不代表可以無理由排除該項控制措施。

有些強化控制措施並沒有被任何「安全等級防護基準」所要求，機關可視需求自行決定是否採用，例如：當機關風險評鑑結果指出需要額外的控制措施或控制措施強化，才能適切降低對國家、機關營運、資產及人員的風險時採用之。

伍、結論

行政院資安會報與行政院研考會近年依據「國家資通訊安全發展方案（98年至101年）」辦理「資訊系統分類分級鑑別機制」參考手冊、「資訊系統風險評鑑參考指引」及「安全控制措施參考指引」之訂定，其中「資訊系統分類分級鑑別機制」參考手冊旨在鑑別資訊系統的安全等級，協助機關掌握重點保護標的；「資訊系統風險評鑑參考指引」旨在進行資訊安全的風險評估，確定各項資訊作業的安全需求水準；「安全控制措施參考指引」則接續「資訊系統分類分級鑑別機制」與「資訊系統風險評鑑參考指引」，提供政府機關導入資訊安全之安全控制措施，以採行適當及充足之資訊安全措施，確保各機關資訊蒐集、處理、傳送、儲存及流通之安全，強化資訊系統安全。

（作者現任財團法人資訊工業策進會與行政院國家資通安全會報技術服務中心專案諮詢）

▲Top

安全控制措施選取完成後，應實作相關的安全控制措施，並檢視其成效作為修正之參考。

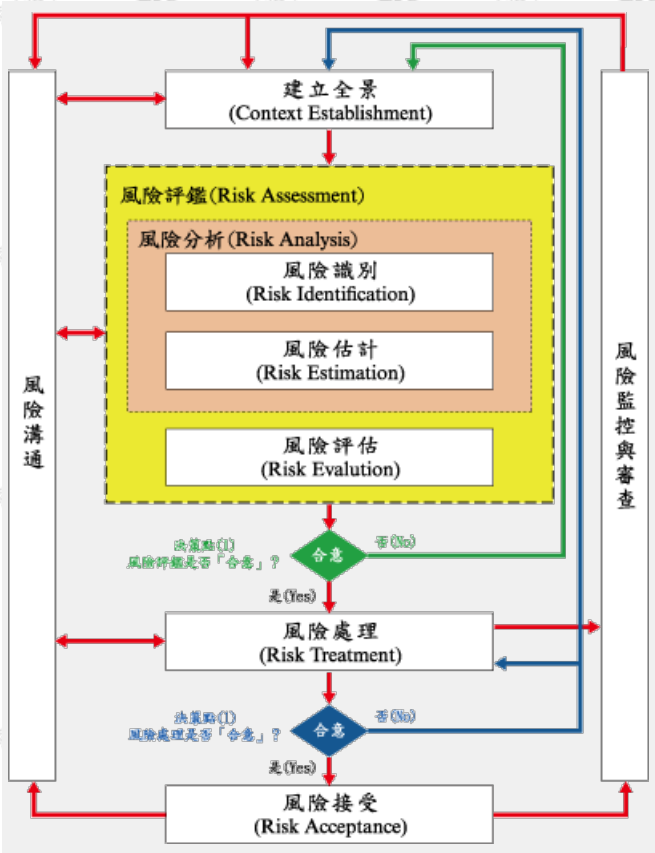
.

資安選擇控制措施篩選與分級作法

◎林子群

壹、前言

ISO/IEC 27005主要是在探討「資訊安全風險管理」，其架構包含下列6個程序，分別為建立全景（Context Establishment）、風險評鑑（Risk Assessment）、風險處理（Risk Treatment）、風險接受（Risk Acceptance）、風險溝通（Risk Communication）及風險監控與審查（Risk Monitoring and Review）。關於「資訊安全風險管理」所含6個程序的關係，詳見圖1所示。



資料來源：ISO/IEC 27005

圖1　ISO/IEC 27005資訊安全風險管理程序圖

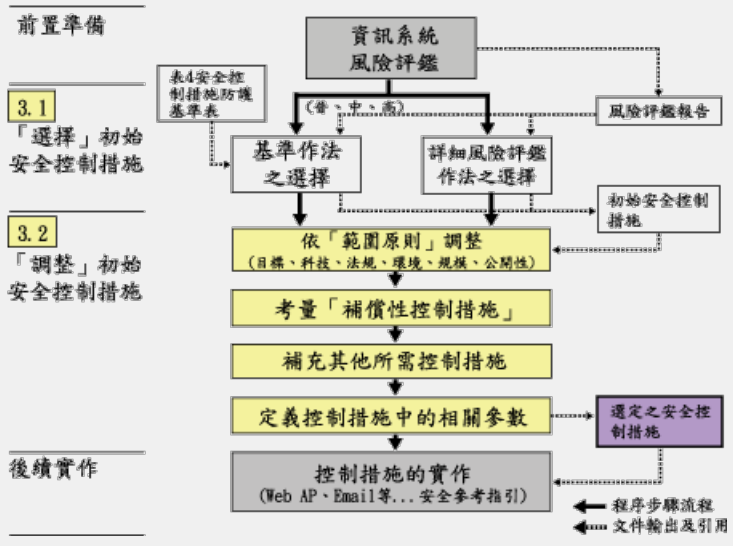
資安選擇控制措施為接續「資訊系統分類分級鑑別機制」與「資訊系統風險評鑑參考指引」，提供安全控制措施「選擇」與「描述」的指導，為資訊安全風險管理程序中之風險處理階段。

貳、資安選擇控制措施篩選步驟

資安選擇控制措施篩選主要分為兩個步驟，首先為「選擇初始安全控制措施」，其次為「調整初始安全控制措施」。

「選擇初始安全控制措施」可區分為依「基準作法之選擇」與「詳細風險評鑑作法之選擇」兩種選擇方法，完成此步驟後應產出「初始安全控制措施」清單的文件。

「調整初始安全控制措施」在提供「排除」、「調整」及「補充」，以進行初始控制措施的微調作業，並提供調整控制措施時應考量的原則，供機關於選擇控制措施時參考。有關選擇安全控制措施的步驟，詳見圖2。



資料來源：行政院研考會「安全控制措施參考指引」

圖２　選擇安全控制措施步驟

機關在安全控制措施選擇的過程中應記錄選用、排除、調整及補充的調整決定，並為該決定提供詳細與充分的理由。最終選用的安全控制措施（含選用之理由）與資訊系統使用限制，應記錄在資訊系統安全計畫內。在安全控制措施選擇過程中，應在安全計畫中記錄任何重要的風險管理決策，以便讓權責主管有足夠的資訊，可以在機關資訊系統的授權程序中做出可信任與風險考量之決策。此外，若缺少這些資訊，當資訊系統或營運環境的狀態變化時，將無法取得原始風險決策。

機關相關人員使用選擇資訊系統安全控制措施前，應先了解下列狀況：

1. 機關資訊系統之安全需求：機關資訊系統之安全需求源自於相關法律、行政命令、指示、政策、標準、指引、規範、程序及機關任務／業務所需，來確保資訊的處理、儲存，及傳送的機密性、完整性及可用性。機關可參考「資訊系統風險評鑑參考指引」對機關之資訊系統進行風險評鑑，以了解機關資訊系統之需求。可採用之風險評鑑方法分為高階風險評鑑作法與詳細風險評鑑作法。
2. 應選擇那些安全控制措施來降低機關資訊系統的風險：資訊系統安全控制措施的選擇應符合機關資訊系統之安全需求。本文建議依資訊系統風險評鑑作法進行安全控制措施的選擇。
3. 目前已實作或已計畫實施中之控制措施：了解目前已實作或已計畫實施中之控制措施，才能識別所選擇控制措施與現有實作中或已計畫實施中之控制措施的差異，利於「資訊安全計畫的擬定」及後續「安全控制措施的實作」。

參、選擇初始安全控制措施

初始安全控制措施是依據風險評鑑結果，為整個資訊系統範圍所挑選的初始安全控制措施，尚未詳細考量資訊系統元件間的差異、科技的使用及機關資源限制等考量。

1. 基準作法：若機關於資訊系統風險評鑑階段採用「資訊系統分類分級與鑑別機制參考手冊」之資訊系統安全等級分析，將資訊系統區分為「普」、「中」、「高」三個安全等級，在選擇初始安全控制措施時，可直接參考安全控制措施參考指引之「安全控制措施防護基準表」，選擇「資訊系統安全等級基準」欄位相對應的「普」、「中」、「高」欄位所列出之安全控制措施。例如：假設某機關資訊系統經評估之安全等級為「普」，則選取安全控制措施參考指引「安全控制措施防護基準表」所對照建議選擇的「普」級「資訊系統安全等級基準」為控制措施。
2. 詳細風險評鑑作法：若機關於資訊系統風險評鑑階段選擇採用「詳細風險評鑑作法」，在選擇初始安全控制措施時，應逐項審查詳細風險評鑑結果中每一項需處理的風險，並參考安全控制措施參考指引５至15章之安全控制措施章節，選擇可以有效降低該風險的控制措施或強化控制措施。惟特定風險選擇安全控制時必須了解其風險形成的原因，如：風險相關的資產、造成風險的威脅、資產本身的脆弱性、風險產生的機率及威脅的來源等，才能正確選擇適當的控制措施來降低該特定風險。

肆、調整初始安全控制措施

選出初始安全控制措施之後，機關可依個別需求來調整初始安全控制措施，俾使控制措施更貼切地符合機關特定的營運環境或安全現狀。

初始安全控制措施的調整活動，應與被核准的相關人員（如：系統管理人員、資訊部門主管、資訊安全主管、風險控制部門人員及資訊系統擁有人）進行協調。所有控制措施調整的決定與理由應明確記錄在資訊系統的安全計畫中，並由機關資訊安全主管核准。

機關針對初始安全控制措施進行調整的步驟包含下列項目：

1. 依「範圍原則」調整：範圍原則係提供機關在決定控制措施是否適用特定的條件與情況，協助機關在特定任務／業務需求與特定營運環境下，確保只實作必要的控制措施，並提供適切層級的資訊系統防護。範圍原則包含安全目標相關考量、系統元件配置相關考量、科技相關考量、實體基礎建設相關考量、政策與法規相關考量、作業與環境相關考量、公開存取相關考量等。
2. 考量「補償性控制措施」：有時機關需要採用補償性的安全控制措施，例如：當機關因特定資訊系統本質、作業環境或控制措施實作的成本效益太低，導致無法實作某項安全控制措施時，補償性控制措施是機關用來替代所建議的控制措施，作為資訊系統及系統所處理、儲存或傳送的資訊，提供相同或可比較的防護等級。
3. 補充其他所需控制措施：在許多狀況下，額外補充的安全控制措施或強化安全控制措施，是針對特定的威脅揭露資訊系統上的脆弱性，以及為

了滿足法律、行政命令、指示、政策、標準及規範的要求。

4. 定義控制措施中的相關參數：在安全控制措施中包含了需要機關定義的參數，讓機關可以彈性地定義控制措施的某些參數，以支援機關特定的需求或目標。在完成上述「三、補充其他所需控制措施」之後，機關審查調整後的安全控制措施清單，將控制措施中「應明確定義的參數」依機關的需求指定適切的值。

伍、結論

行政院研考會於「94年資通安全技術服務與防護管理計畫」中，責成「行政院國家資通安全會報技術服務中心」，訂定各機關辦理資通安全有關作業規範與參考指引；以往各參考指引之檢核表皆依其需求各自發展，無一致性之考量依據。安全控制措施參考指引則為未來發展或修訂參考指引與檢核表之選擇安全控制措施依據。

政府機關於安全控制措施選取完成後，應實作相關的安全控制措施，並依實作結果檢視其成效，作為修正之參考，亦即執行資訊安全風險管理程序之風險監控與審查。

（作者現任財團法人資訊工業策進會與行政院國家資通安全會報技術服務中心專案諮詢）

▲Top