法務部及所屬機關資訊安全風險評鑑管理規範

1、 目的

為確保法務部（以下簡稱本部）及所屬機關執行資訊安全風險評估作業時，得以整合納入業務流程及資訊資產之資安風險，並確保評鑑方法之一致性，特訂定本規範。

2、 適用範圍

本部及所屬機關資訊安全管理制度範圍內之所有業務流程及相關資訊資產。

3、 名詞定義

（1） 弱點（Vulnerabilities）

現行資訊資產或控制措施中可能遭受威脅利用之脆弱點。

（2） 威脅（Threats）

導致管理系統或機關遭受損害之事件潛在原因。

（3） 衝擊（Impact）

對營運的受損、信譽的損害、資訊安全的危害、業務和財務價值的損失及違法情事等之後果。

（4） 風險（Risks）

事件發生機率與後果之組合。

1、 風險評鑑作業

（1） 建立風險管理全景

1、應識別內、外各方面之資訊安全需求，包括資訊安全政策以及法令、法規、規章與合約以及其他可能影響資訊安全之事務。

2、應界定風險評鑑範圍，以利執行風險評鑑作業。

3、應規劃與定義「風險準則」、「風險等級」及「風險接受準則」等風險管理準則

(1)風險準則（Risk Criteria）：

評估風險顯著性時所用之評估條件及其評估方法。評估方式採用「定性」方式，評估條件應考量下列項目：

A.弱點

B.威脅

C.衝擊

(2) 風險等級（Level of Risk)：

以風險評估條件評估結果之總合方式表示之風險顯著性。

(3)風險接受準則（Risk Acceptable Criteria）：

機關用以決定留置或承受風險之原則。機關應考量影響風險接受準則的項目如下：

A.業務需求及目標。

B.法律、法令、規章及合約方面之要求。

C.智慧財產權（Intellectual Property Right, IPR）。

D.資源分配狀況。

E.技術成熟度。

F. 經費預算。

G.社會與輿論因素。

4、違反法令之行為視為不可接受之風險項目，應採行下列預防措施，不納入風險評鑑作業：

A.鑑別適用法令之清單。

B.訂定資訊安全管理制度之規範文件時，應檢視並確保符合現行法令之需求。

C.辦理資訊安全法令宣導。

（1） 風險評鑑過程

風險評鑑區分為針對業務流程評估之「高階風險評鑑」與重要業務流程相關資訊資產之「詳細風險評鑑」兩部分。

1、高階風險評鑑

(1) 針對內部所有業務流程，依據「法務部及所屬機關資訊安全風險評鑑管理程序」，進行初步之「高階風險評鑑」，以決定是否需進行「詳細風險評鑑」。

(2) 不需進行「詳細風險評鑑」者，直接進行安全監控，進入風險之再評估階段。

2、詳細風險評鑑

包括「風險分析(Risk Analysis)」及「風險評估(Risk Evaluation)」。

(1)風險分析

透過系統化方式，尋求業務流程相關之資訊資產於風險準則中所定義的風險評估條件，並用「定性」方式，得出資訊資產風險等級。

(2)風險評估

(1) 依「風險接受準則」評估「風險分析」之結果，以決定需要管控的資訊資產。

(2) 「風險分析」之結果值高於「可接受風險等級」之資訊資產，應列為「風險處理」之對象。

1、 風險處理

（1） 資訊資產列為「風險處理」對象者，應將風險評估之結果提報單位主管審查，並將審查結果提報本部資通安全會報（資訊安全執行小組），以審查風險改善方式。

可採用之風險改善方式包括：

1、規避風險。

2、降低風險發生機率。

3、降低風險影響程度。

4、轉移風險。

5、接受風險。

（2） 超過「可接受風險等級」之風險項目，應擬訂風險改善計畫。

風險改善計畫之擬訂，應預估完成後殘餘風險是否可降低至可接受風險值以下，並考量所需資源、優先順序、責任分配等因素，至少包含下列內容：

1、風險項目。
2、採取之控制方法。
3、所需投入資源。
4、相關負責人員。
5、預估完成日期。

（3） 風險改善計畫應符合整體資訊安全目標。

（4） 風險改善計畫執行結束後，應重新評估殘餘風險是否均已降低至可接受風險值以下。

（5） 風險改善計畫執行之成果應提報本部資通安全會報（資訊安全執行小組）之管理審查會議中進行確認。

1、 風險之再評估

（1） 風險評鑑應每年進行全面評估。但機關政策、單位業務、資訊資產等發生重大變更時，或遇有任何重大專案新增或變動時，應就該重大變更影響部份於2個月內進行再評估。

（2） 再評估之因素：

應識別下列狀況所可能帶來之風險：

1、識別與外部團體有關之風險。

2、當機關因作業需要，新增或變更開放授權外部團體存取機關資訊系統或機關所持有之業務資訊前，應進行評估及識別相關可能之風險。

3、設備產生之風險：

(1)設備應考量來自實體環境之風險，如資訊資產所在之實體環境發生變動時，應考量是否增加未經授權存取之機會。

(2)設備如須於辦公處所以外之區域使用時，應考量可能遭受之風險。

4、外部團體服務變更之風險：

當外部團體服務合約、服務內容及服務人員發生變更時，應考量可能帶來之風險。

5、資訊應用系統技術脆弱性之風險：

應取得資訊應用系統技術脆弱性之及時資訊，並評估該脆弱性對現行資訊應用系統之影響，以控制可能產生之風險。

（1） 當相關作業發生新增或變動時，應針對所涉及之資訊資產是否造成資產價值變動，以考量是否進行再評估。