

國立中興大學計資中心 因應行政院國家資通安全會報資訊系統 分類分級之策略

Jerry Yang, 高級顧問師
2010/11/18

ADVISORY

大綱

- ◆ 資訊系統分類分級與鑑別機制
- ◆ 資訊系統風險評鑑介紹
- ◆ 建議因應策略

國家資通訊安全發展方案

◆ 推動資訊與資訊系統分類分級

— 執行要點：

- 整合機關、資訊及資訊系統之分類分級作法
- 建立分類分級標準，設定基本資安防護需求水準
- 對資訊與資訊系統進行分類分級鑑別，並要求達到最基本的資安防護需求

— 績效指標：

- 99年A級機關完成資訊與資訊系統鑑別
- 100年B級機關完成資訊與資訊系統鑑別
- 101年由主管機關自行列管所屬各級資訊系統達到基本資安防護需求



國家資通訊安全發展方案

◆ 目的

- 鑑別資訊系統安全等級
- 掌握重點保護標的採行適當安全控制措施
- 有效運用資源

◆ 適用範圍

- 各級政府機關、公營事業機構、公立研究機構、學校等（以下簡稱機關）之資訊系統
- 資訊內容屬「國家機密保護法」所稱國家機密之資訊系統，除參考本機制外，亦應依據「國家機密保護法」相關規定辦理。



國家資通訊安全發展方案

◆ 要求

- 機關每年度應針對各項資訊系統至少進行1次分類分級與鑑別。
- 已通過資訊安全管理驗證（例如：ISO/IEC 27001、CNS 27001等）機關，準用已採行之風險評鑑方法，須將資訊系統衝擊評估結果轉換為本機制之普、中、高三個安全等級。
- 屬於資安防護處理相關控制措施（例如：防毒系統、防火牆系統、入侵偵測/防禦系統、弱點掃描系統、網頁/郵件內容過濾系統等），不需進行資訊系統分類分級與鑑別。



鑑別機制處理程序－安全等級評估表

		執行步驟	參與者
①	識別資訊類別	各資訊系統均須依循處理程序填寫「安全等級評估表」	承辦單位主管
		資訊類別即為施政分類（定義詳見行政院秘書處彙編「行政院施政分類架構」），資訊系統依其處理資料之性質，可包含多項資訊類別	業務承辦人
②	設定影響構面等級	依資料保護、業務運作、法律規章、人員傷亡、組織信譽、其他（如：財物損失）等六大構面，分別評估對各資訊類別之影響衝擊，並設定影響構面等級	業務承辦人
③	識別業務屬性	依據資訊系統之業務屬性（分為關鍵性業務、支援性業務、行政性業務三類），檢視安全等級之合理性	承辦單位主管
	檢視安全等級		
④	設定資訊系統安全等級	資訊系統安全等級經資訊主管、業務主管確認後，由資訊安全長核定	資訊安全長、資訊主管
	資訊系統清冊	資訊單位將各單位完成的「安全等級評估表」彙整成「資訊系統清冊」	資訊單位



安全等級評估表－識別資訊類別

「○○○ (資訊系統名稱)」安全等級評估表

功能說明：

業務屬性：關鍵性業務 支援性業務 行政性業務

日期：____年____月____日

編號	資訊類別 (施政分類)		影響構面				資訊類別安全等級	
	第一層	第二層	1. 資料保護受到損害	2. 影響業務運作	3. 影響法律規章遵循	4. 人員傷亡		5. 損害組織信譽
1								
2								
3								
4								
5								
註：資訊類別 (施政分類) 欄位可多選						資訊系統安全等級：		



©2010 KPMG Advisory Services Co., Ltd., a Taiwan company limited by shares and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

7

識別資訊類別 (施政分類)

- ◆ 行政院以業務功能為導向，參照資訊隸屬特性及組織執掌研訂「施政分類架構」架構分為19類包含：
 - 內政及國土安全、外交僑務及兩岸、國防及退伍軍人、財政金融、教育及體育、法務、經濟貿易、交通及建設、勞動及人力資源、農業、衛生及社會安全、環境資源、文化及觀光、國家發展及科技、海洋事務、原住民族、客家、其他政務及輔助事務等



©2010 KPMG Advisory Services Co., Ltd., a Taiwan company limited by shares and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

8

安全等級評估表－影響構面

「○○○（資訊系統名稱）」安全等級評估表

功能說明：

業務屬性：關鍵性業務 支援性業務 行政性業務

日期：____年____月____日

編號	資訊類別（施政分類）		影響構面						資訊類別安全等級
	第一層	第二層	1. 資料保護受到損害	2. 影響業務運作	3. 影響法律規章遵循	4. 人員傷亡	5. 損害組織信譽	6. 其他(如：財物損失)	
1									
2									
3									
4									
5									
註：資訊類別（施政分類）欄位可多選						資訊系統安全等級：			



影響構面－「資料保護受到損害」

安全等級	說明
普 (等級1)	<ul style="list-style-type: none"> (資料機密性) 一般性資料；資料外洩不致影響個人權益或僅導致個人權益輕微受損。 (資料完整性) 資料遭竄改不致影響個人權益或僅導致個人權益輕微受損。
中 (等級2)	<ul style="list-style-type: none"> (資料機密性) 敏感性資料；資料外洩將導致個人權益嚴重受損，如：涉及個人出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情形、社會活動及其他得以直接或間接識別個人之資料。具有敏感屬性之個人資料，如：中途輟學學生、收養兒童等資料，資料外洩可能導致個人隱私遭冒犯。 (資料完整性) 資料遭竄改將導致個人權益嚴重受損。
高 (等級3)	<ul style="list-style-type: none"> (資料機密性) 機密性資料；資料外洩將危及國家安全、導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損。例如：戶役政資訊系統、護照管理系統、醫療系統等。 (資料完整性) 資料遭竄改將危及國家安全、導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損。



影響構面－「影響業務運作」

安全等級	說明
普 (等級1)	<ul style="list-style-type: none"> 系統容許中斷時間較長(如:72小時)。 系統故障對社會秩序、民生體系運作不致造成影響或僅有輕微影響。 系統故障僅影響機關非核心業務執行效能,或造成核心業務執行效能輕微降低。
中 (等級2)	<ul style="list-style-type: none"> 系統容許中斷時間短。 系統故障對社會秩序、民生體系運作將造成嚴重影響。 系統故障將造成機關核心業務執行效能嚴重降低。
高 (等級3)	<ul style="list-style-type: none"> 系統容許中斷時間非常短(如:30分鐘)。 系統故障對社會秩序、民生體系運作將造成非常嚴重影響,甚至危及國家安全。 系統故障將造成機關核心業務執行效能非常嚴重降低,甚至業務停頓。



影響構面－「影響法律規章遵循」

安全等級	說明
普 (等級1)	系統運作、資料保護、資訊資產使用等須依循相關規範辦理,否則將導致機關違反法律規章並伴隨輕微不良後果,如:使用經授權資訊系統或軟體、智慧財產權兒童及少年福利法、電腦網路內容分級處理辦法等。
中 (等級2)	系統運作、資料保護、資訊資產使用等須依循相關規範辦理,否則將導致機關違反法律規章並伴隨嚴重不良後果。
高 (等級3)	系統運作、資料保護、資訊資產使用等須依循相關規範辦理,否則將導致機關從根本上違反法律規章。



影響構面－「人員傷亡」

安全等級	說明
中 (等級2)	若系統發生資訊安全事故，無法完全排除造成人員傷亡的可能性。
高 (等級3)	若系統發生資訊安全事故，可能造成人員死亡，或非常可能造成人員肢體傷害的危險。

影響構面－「損害組織信譽」

安全等級	說明
普 (等級1)	若系統發生資訊安全事故，將導致機關形象、信譽受到輕微損害，如：導致區域性媒體報導負面新聞、造成多位民眾電話抱怨等情形。
中 (等級2)	若系統發生資訊安全事故，將導致機關形象、信譽受到嚴重損害，如：導致全國性媒體報導負面新聞、造成民眾至機關抗議或陳情等情形。
高 (等級3)	若系統發生資訊安全事故，將導致機關形象、信譽受到非常嚴重損害，如：導致國際性媒體報導負面新聞、造成民眾大規模遊行抗爭等情形。

安全等級評估表－業務屬性

「○○○（資訊系統名稱）」安全等級評估表

功能說明：

業務屬性：關鍵性業務 支援性業務 行政性業務

日期：____年____月____日

編號	資訊類別（施政分類）		影響構面						資訊類別安全等級
	第一層	第二層	1. 資料保護 受到損害	2. 影響業務 運作	3. 影響法律 規章遵循	4. 人員傷亡	5. 損害組織 信譽	6. 其他(如： 財物損失)	
1									
2									
3									
4									
5									
註：資訊類別（施政分類）欄位可多選						資訊系統安全等級：			



業務屬性

◆行政性業務：

- 係指機關內部輔助單位之業務，若輔助單位工作與機關職掌相同或兼具業務單位性質，機關得視情形調整業務屬性

◆關鍵性業務：

- 機關在遭遇衝擊時，須確保持續運作之核心業務，以及與民眾生活機能相關之關鍵基礎建設（如：水、電力、通訊電信、農產運銷、金融服務等），均屬關鍵性業務。

◆支援性業務：

- 機關內部業務單位之業務但非列核心業務者，屬支援性業務。



安全等級評估表－檢視資訊安全等級

- ◆ 資訊系統安全等級與業務屬性通常具有高度關聯性，因此可進行勾稽

「〇〇〇（資訊系統名稱）」安全等級評估表

功能說明：

業務屬性：關鍵性業務 支援性業務 行政性業務 日期：____年____月____日

編號	資訊類別（施政分類）		影響構面						資訊類別安全等級
	第一層	第二層	1. 資料保護 受到損害	2. 影響業務 運作	3. 影響法律 規章遵循	4. 人員傷亡	5. 損害組織 信譽	6. 其他(如： 財物損失)	
1									
2									
3									
4									
5									

註：資訊類別（施政分類）欄位可多選 資訊系統安全等級：

資訊類別安全等級 = MAX(影響構面)



安全等級評估表－資訊系統安全等級

- ◆ 資訊系統安全等級與業務屬性通常具有高度關聯性，因此可進行勾稽

「〇〇〇（資訊系統名稱）」安全等級評估表

功能說明：

業務屬性：關鍵性業務 支援性業務 行政性業務 日期：____年____月____日

編號	資訊類別（施政分類）		影響構面						資訊類別安全等級
	第一層	第二層	1. 資料保護 受到損害	2. 影響業務 運作	3. 影響法律 規章遵循	4. 人員傷亡	5. 損害組織 信譽	6. 其他(如： 財物損失)	
1									
2									
3									
4									
5									

註：資訊類別（施政分類）欄位可多選 資訊系統安全等級：

資訊系統安全等級 = MAX(資訊類別安全等級)



資訊系統清冊

◆ 由資訊單位彙整資訊系統清冊

資訊系統清冊					
					表單編號：
彙整日期： 年 月 日					
編號	資訊系統名稱	業務屬性	資訊系統安全等級	承辦單位	備註
1					
2					
3					
4					
5					
資訊單位		複核主管		資訊安全長	

註：請各機關依本身實際核陳流程調整簽核欄位，如：複核主管調整為主任秘書等

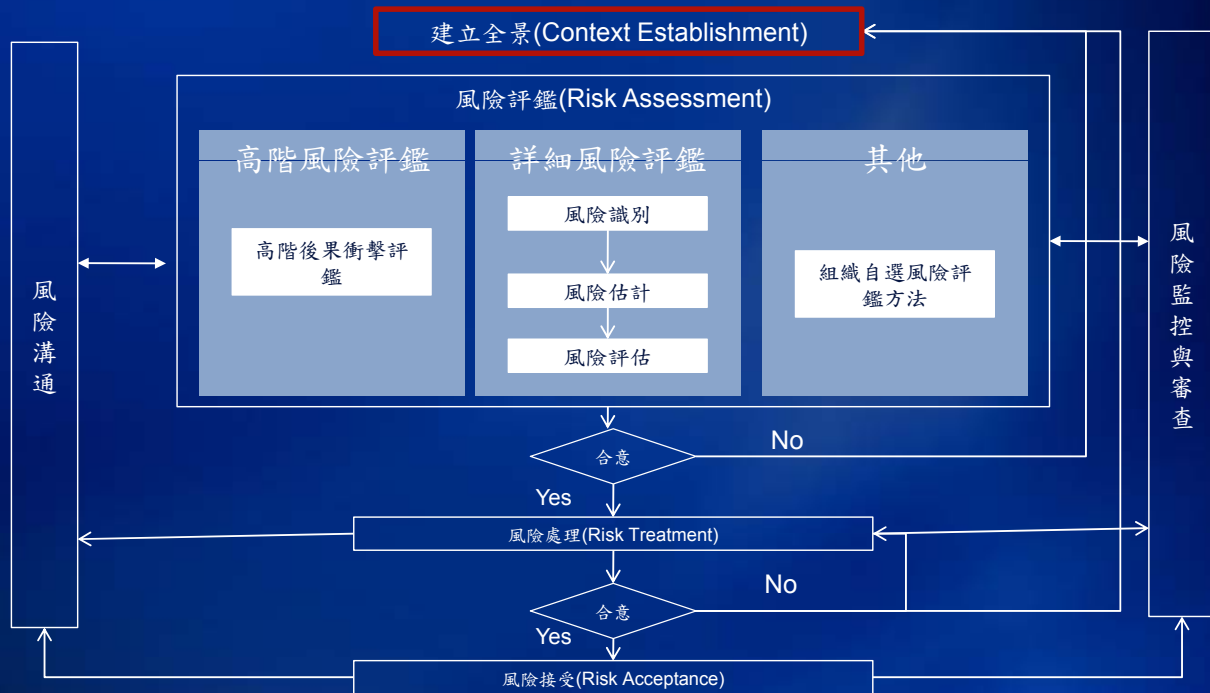


大綱

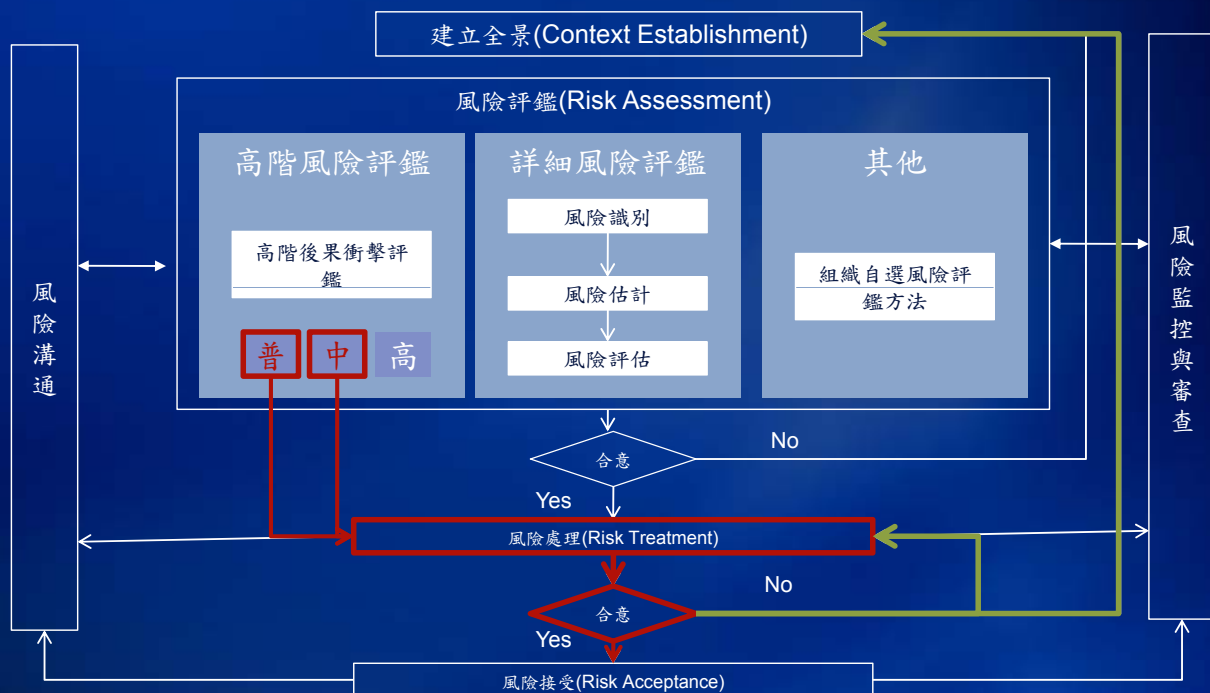
- ◆ 資訊系統分類分級與鑑別機制
- ◆ 資訊系統風險評鑑介紹
- ◆ 建議因應策略



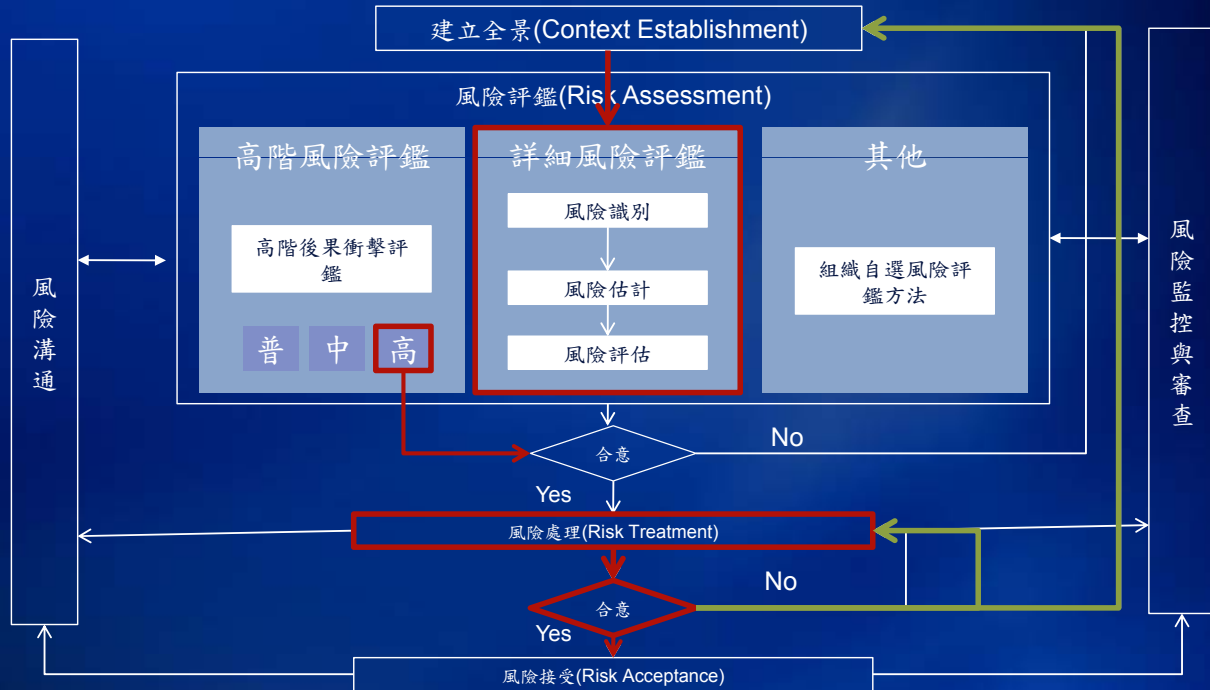
建立全景(Context Establishment)



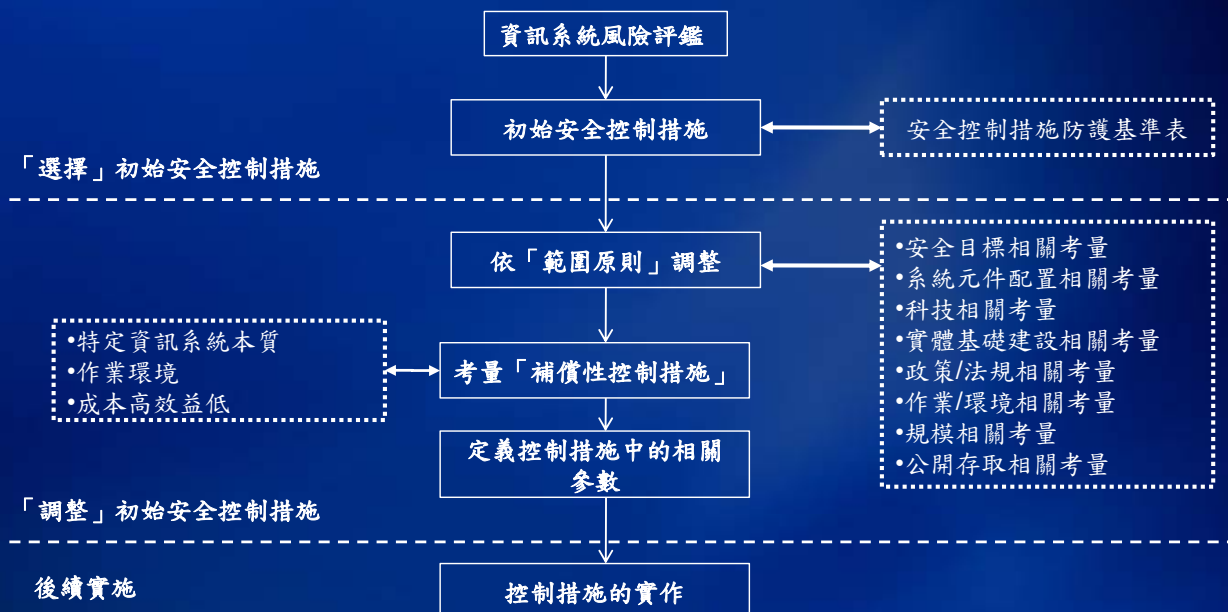
高階風險評鑑



詳細風險評鑑



安全控制措施參考指引



大綱

- ◆ 資訊系統分類分級與鑑別機制
- ◆ 資訊系統風險評鑑介紹
- ◆ 建議因應策略

資訊系統分類分級與鑑別機制因應策略

- ◆ 階段一：資訊系統分類分級與鑑別策略
 - 配合行政院國家資通安全會報進行資訊系統分類分級與鑑別
- ◆ 階段二：關聯性整合策略
 - 將『資訊系統分類分級與鑑別』調查後結果進行關聯性整合
- ◆ 階段三：風險評鑑再造策略
 - 採用『資訊系統風險評鑑參考指引』架構

階段一：識別驗證範圍與參與程度分析

◆ 關鍵性業務識別

- 驗證範圍 ≠ 關鍵性業務
- 部門關鍵業務 ≠ 組織關鍵業務



©2010 KPMG Advisory Services Co., Ltd., a Taiwan company limited by shares and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

27

階段一：業務（資訊系統）盤點

部門類別	資訊室	人事室	會計室	病歷室	教務處	掛號櫃台	...
資訊系統							
會計系統	M	U	U				
人事系統	M	U	U				
全球資訊網	M / U	U	U	U	U		
電子郵件系統	M / U	U	U	U	U		
電子公文件統	M / U	U	U	U	U		
醫療資訊系統	M						
校務行政系統	M				U		
稅務資訊系統	M						
批價掛號系統	M					U	
...							

Manager Owner User



©2010 KPMG Advisory Services Co., Ltd., a Taiwan company limited by shares and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

28

階段一：資訊系統分類分級與鑑別

◆各單位產出『安全等級評估表』

- 方案一：全部內容由各單位填寫確認
- 方案二：影響構面欄位由各單位確認
- 方案三：全部內容由資訊單位預填後由各單位確認

◆資訊單位彙整『資訊系統清冊』



©2010 KPMG Advisory Services Co., Ltd., a Taiwan company limited by shares and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

階段二：關聯性整合 (1/3)

◆縱向關聯性

- 機密性/完整性 = MAX(資料保護受到損害)
- 可用性/RTO/RPO = MAX(影響業務運作)
- 適法性 = MAX(影響法律規章遵循)

「○○○ (資訊系統名稱)」安全等級評估表

功能說明： _____

業務屬性：關鍵性業務 支援性業務 行政性業務 日期：____年____月____日

編號	資訊類別 (施政分類)		影響構面				資訊類別安全等級	
	第一層	第二層	1. 資料保護受到損害	2. 影響業務運作	3. 影響法律規章遵循	4. 人員傷亡		5. 損害組織信譽
1								
2								
3								
4								
5								

註：資訊類別 (施政分類) 欄位可多選 資訊系統安全等級： _____



©2010 KPMG Advisory Services Co., Ltd., a Taiwan company limited by shares and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

階段二：關聯性整合(2/3)

欄位編號	欄位名稱	說明	關聯欄位	備註
1	* 資訊資產編號	此為唯一識別碼	N/A	安全等級 評估表
2	* 資訊系統名稱	資訊系統服務名稱	N/A	
3	* 業務屬性	關鍵性業務 支援性業務 行政性業務	6(勾稽)	
4	* 資訊類別 (施政分類)	(a) 第一層 依據「行政院施政分類架構」	N/A	
		(b) 第二層 依據「行政院施政分類架構」	4(a)	
5	* 影響構面	(a) 資料保護受到損害 (b) 影響業務運作 (c) 影響法律規章遵循 (d) 人員傷亡 (e) 損害組織信譽 (f) 其他(如：財物損失)	N/A	
6	* 資訊類別安全等級	影響構面MAX	5	
7	* 資訊系統安全等級	資訊類別安全等級MAX	6	



階段二：關聯性整合(3/3)

欄位編號	欄位名稱	說明	關聯欄位	備註
8	資訊系統說明	資訊系統功能與業務說明	N/A	營運衝擊 分析表
9	* 權責單位名稱	資訊系統擁有者	N/A	
10	* MTPD	Maximum Tolerable Period of Disruption	5(b)	
11	* RTO	Recover Time Object	5(b)	
12	* RPO	Recover Point Object	5(a) (b)	
13	依賴資訊系統/流程	此項資訊系統/流程失效時將直接影響本資訊系統完全無法運作	2	資訊資產 清冊
14	資訊安全要素	機密性	5(a)	
		完整性	5(a)	
		可用性	5(a) (b)	
		適法性	5(c)	



階段三：風險評鑑再造策略

◆ 風險評鑑再造

- 以資通安全會報架構為骨架；KPMG方法論為血肉



策略優缺分析

策略分析	階段一	階段二 / 階段三
優點	<ul style="list-style-type: none"> 變動調整衝擊較小 	<ul style="list-style-type: none"> 重新識別關鍵業務與驗證範圍 重點實施風險控制措施 資安管理跨單位水平整合 資安控管全組織參與
缺點	<ul style="list-style-type: none"> 資安防護與管理僅限於部份單位 資源投入目標廣泛造成浪費 無法實際反應全組織資安防護重點 無法達成一至資訊安全防護水準 	<ul style="list-style-type: none"> 達成一至資訊安全防護水準 符合未來行政院資通安全規範要求 整合階段需跨單位參與協調 資安管理程序需變動調整



問題與討論

Jerry Yang
**KPMG Advisory Services Co.,
Ltd.**
+886 (2) 8101 6666 ext.10258
jerryyang@kpmg.com.tw
www.kpmg.com.tw