

# 資通系統分級/資安技術防護基準

洪明賢

ISO27001資訊安全管理系統主導稽核員認證

ISO27701個人資料隱私管理系統主導稽核員認證

BS10012個人資料管理系統主導稽核員認證

EC-Council CND資安防禦認證

EC-Council CEH駭客技術專家認證

教育體系ISMS/PIMS稽核員



# 課程大綱

---

- 資通系統風險評鑑原則
- 資通系統防護需求分級原則
- 資通系統防護基準
- 資安防禦策略探討



# 資通系統風險評鑑原則



# 什麼是風險

---

- 所謂「**風險**」乃是當「**威脅**」利用其相對應「**脆弱性（弱點）**」直接或間接造成組織或政府機關一個或一群「**資訊資產**」受到漏失或損害的「**可能性**」。
- 風險主要運用「**可能性**」與「**衝擊**」的結合定義其特性。
- 「**衝擊**」指的是對**組織或資訊資產**產生的影響，可能是負面或正面。

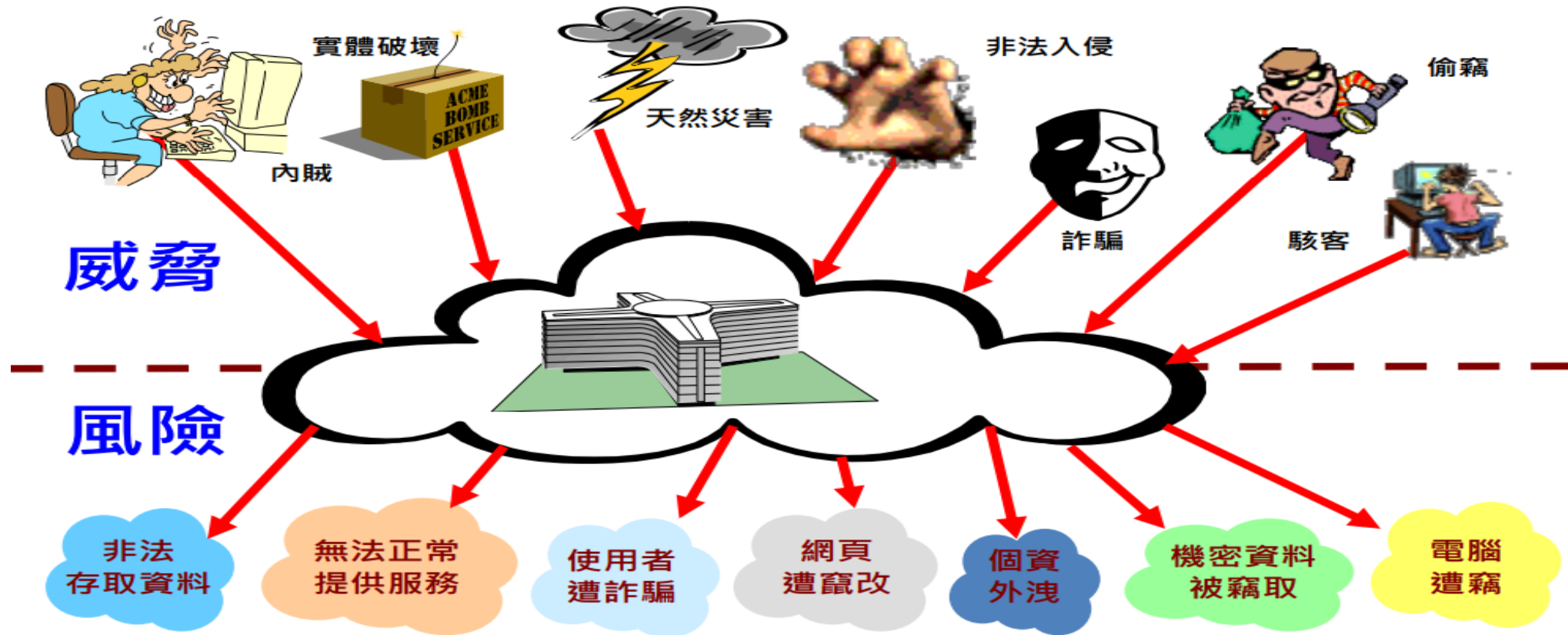
# 風險管理在做些什麼？

---

- 風險管理程序是要透過一套有系統的方法，來達到以下的目的：
  - 管控或降低資訊安全意外事件所可能造成的損失：風險管理要能夠辨識出可能發生的意外事件或風險，並採取適當回應，以使得可能的損失被控管在一個可接受的範圍內。
  - 提升資訊安全措施的成本效益：風險管理的方法要能夠協助企業或組織，在需要控管某項風險時，能夠找到最有成本效益的措施來進行控管。
  - 滿足法規或是利害關係人(如客戶與消費者團體)的相關要求。

# 風險管理在資安上的概念?

- 風險管理了解到威脅(T) 利用到弱點(V) 所可能造成意外事件的損失(R)。而採取適當的控制措施(S) 使得殘存風險(RR)，是可被企業接受的。



# 資訊安全風險管理架構

## 風險管理流程



# 風險處理

## ■ 風險修改(風險降低)

施行、移除或改變安全控制措施，以修訂或降低風險等級，使殘餘之風險得被重新評定為可接受

## ■ 風險保留

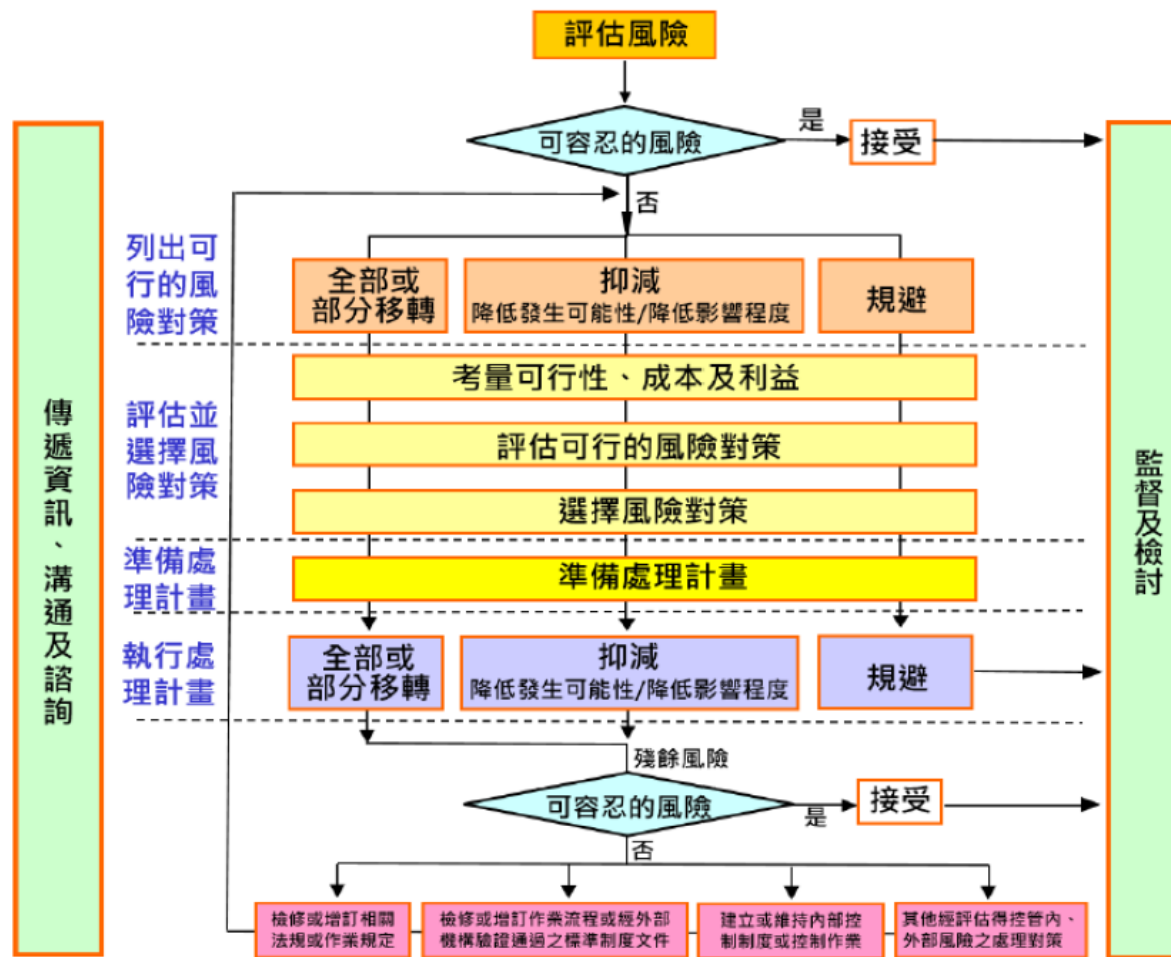
風險等級符合風險接受準則，則不需實作額外之控制措施，該風險保留

## ■ 風險避免

從已規劃或現有活動退出，或變更活動運作的情況

## ■ 風險分擔(風險轉移)

依據風險評估結果，將部分之風險分擔至能有效管理該特定風險之另一方





# 可接受風險考量

- 機關會因為任務與性質、服務對象、內部資源與經費預算，影響風險處理範圍。在有限資源處理下，以風險影響層面大，優先處理風險。資源欠缺情況下，暫時予以接受並保留風險。
  - 風險處理成本高過因資安事件造成之潛在損失
  - 機關有能力自主處理或控制相關資安事件發生
  - 因科技更迭速度快，尚無相關有效處理風險技術

# 詳細風險評鑑

1. 優先處理的資訊及資通系統資產所對應的**風險**
2. **風險評估準則**與**衝擊準則**執行風險分析，得到資通訊系統資產的風險值
3. 執行**風險評估**，以訂定**風險等級**
4. 依**風險接受準則**，決定**風險可接受等級**

## 風險識別

- 1. 資產識別
- 2. 威脅與脆弱性識別
- 3. 現有控制措施識別
- 4. 後果識別

## 風險分析

- 5. 後果評鑑
- 6. 事件可能性評鑑
- 7. 決定風險等級

## 風險評估

- 8. 決定風險可接受等級

# 高階風險評鑑

---

- 依資通安全責任等級分級辦法之規定，分別就機密性、完整性、可用性、法律遵循性評估資通系統防護需求分級，直接以該規定之分級結果，做為該資通系統的風險評鑑等級
- 依風險評鑑等級選擇安全控制措施參考指引所建議適當之安全控制措施
- 採用ISO 31010企業衝擊分析，評鑑對於機關之衝擊程度，並考量其發生之可能性（亦可視為衝擊發生是必然的），以評定資通系統之安全等級

# 高階風險評鑑優點

- 較**簡單**之評鑑作法，容易獲得風險評鑑參與人員之**接受**。
- 可做為**良好之輔助規劃**，以建構**機關資安之策略藍圖**。
- 可將資源及預算運用於**最有利**之處。

採高階風險評鑑，**評鑑結果潛存在不精確或未能識別營運過程或系統**，針對**高安全**等級之資產



## 詳細風險評鑑

# 資通系統防護需求分級原則



# 資通安全管理法 (資安法)

105/8/31  
完成草案修訂

資通安全管理法  
草案

辦理座談會

刪除爭議條文

105/10/13公  
布

個人資料保護法  
調修版

辦理子法草案座談會

107/5/11  
立法院三讀通過

資通安全管理法

107/11/21 行政院訂定發布相關子法

107/6/6  
總統府正式公布

資通安全管理法

《資通安全管理法施行細則》

《資通安全責任等級分級辦法》

《資通安全事件通報及應變辦法》

《特定非公務機關資通安全維護計畫實施情形稽核辦法》

《資通安全情資分享辦法》

《公務機關所屬人員資通安全事項獎懲辦法》

108/1/1  
行政院公告  
正式實施

資通安全管理法  
及相關子法

# 資通安全管理法 (資安法)

資通安全管理法

資通安全管理法施行細則

資通安全責任等  
級分級辦法

資通安全事件通  
報及應變辦法

特定非公務機關  
資通安全維護計  
畫實施情形稽核  
辦法

資通安全情資分  
享辦法

公務機關所屬人  
員資通安全事項  
獎懲辦法

資安維護計畫範本

公務機關資通安全  
事件通報應變程序  
範本

特定非公務機關資  
通安全事件通報應  
變程序範本

# 資通安全責任等級分級原則

## A級

### 全國性

- 全國性民眾或公務員個人資料檔案
- 外交、國防或國土安全事項
- 公務機關涉全國性之能源、水、通訊傳播、交通、銀行與金融、緊急救援
- 關鍵基礎設施提供者
- 全國性民眾服務資通系統之維運
- 全國性跨公務機關共用性資通系統之維運
- 公立醫學中心

### 區域或地區性

- 區域性或地區性民眾個人資料檔案
- 公務機關所捐助或研發之敏感科學
- 技術資訊安全維護管理
- 公務機關涉及區域性或地區性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援事項
- 關鍵基礎設施提供者
- 區域性或地區性民眾服務資通系統維運
- 區域性或地區性跨公務機關共用性資通系統維運
- 公立區域醫院

## B級



# 資通安全責任等級分級原則

---

C級

自行或委外發資訊系統並設置伺服器者

D級

未自行或委外開發資訊系統，  
未設置伺服器

E級

全部資訊業務由其他機關兼辦或代辦

# 資通安全責任等級分級辦法

---

- A、B、C級公務機關
  - 初次受核定或等級變更後之**一年內**，針對**自行或委外開發之資通系統**，**依附表九完成資通系統分級**
  - 其後應**每年至少檢視一次資通系統分級妥適性**；並應於初次受核定或等級變更後之**二年內完成附表十之控制措施**。
  - **套裝軟體、上級機關提供之應用服務**不須進行附表九及附表十之作業。

# 資通安全責任等級分級辦法

---

- 第十一條

各機關辦理附表一至附表八所定事項或執行附表十所定控制措施，因**技術限制、個別資通系統之設計、結構或性質**等因素，就特定事項或 控制措施之辦理或執行顯有困難者，得經第三條第二項至第四項**所定其等級提交機關**或同條第五項**所定其等級核定機關同意**，**並報請主管 機關備查**後，免執行該事項或控制措施；其為主管機關者，經其同意後，免予執行。

# 資通系統防護需求分級原則

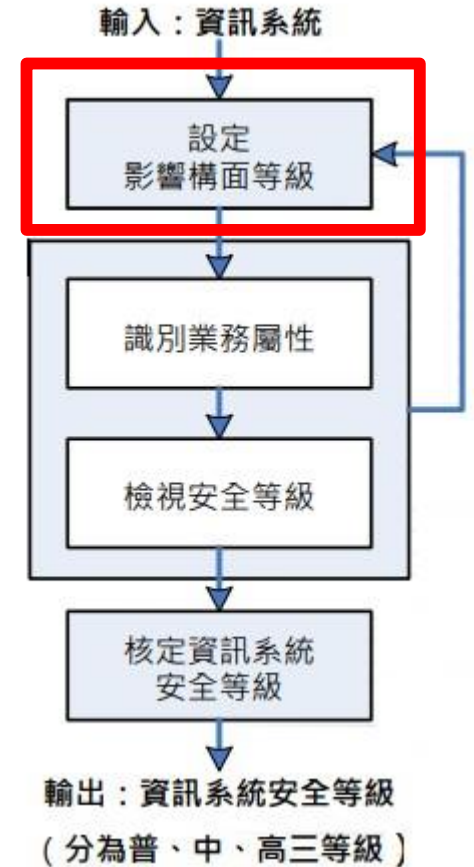
- 各資訊系統均須依循處理程序，填寫「安全等級評估表」

- 步驟1：

依機密性、完整性、可用性及法律遵循性四大構面

分別評估對各資訊系統(不含共同性系統)之影響衝擊構面等級

依資訊系統填寫「安全等級評估表」



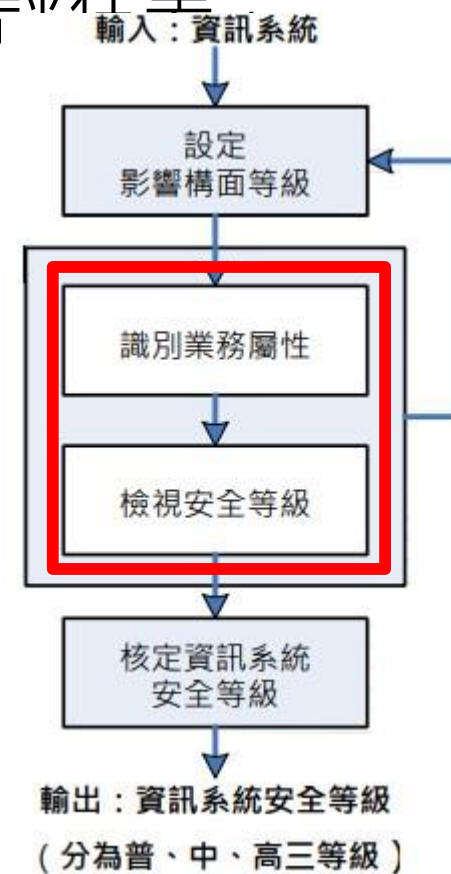
# 資通系統防護需求分級原則

- 各資訊系統均須依循處理程序，填寫「安全等級評估表」

- 步驟2：

依據資訊系統支援之業務屬性  
( 分為**行政**與**業務**二類 )

檢視安全等級之合理性



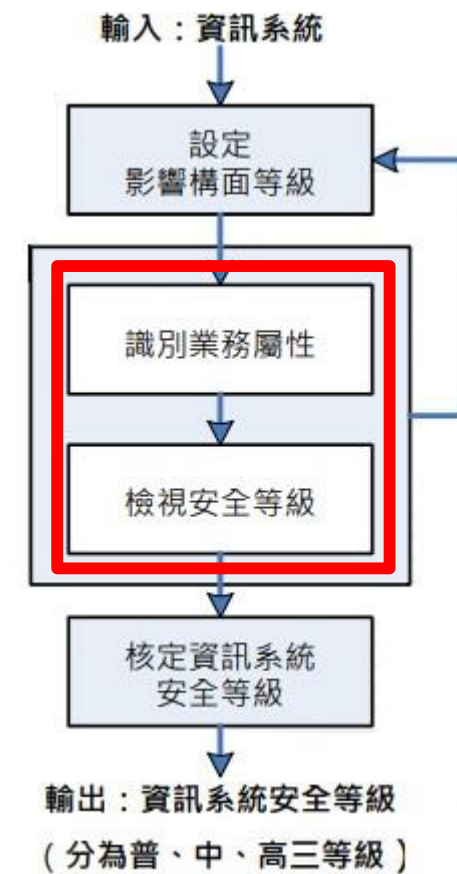
# 資通系統防護需求分級原則

- 續步驟2：

資通系統依其支援之單位及業務屬性，分為 **行政** 與 **業務** 二類：

**行政類**：指機關內部輔助單位之業務（如：人事、薪資等），惟若輔助單位工作與機關職掌相同或兼具業務單位性質，機關得視情形調整其類別。

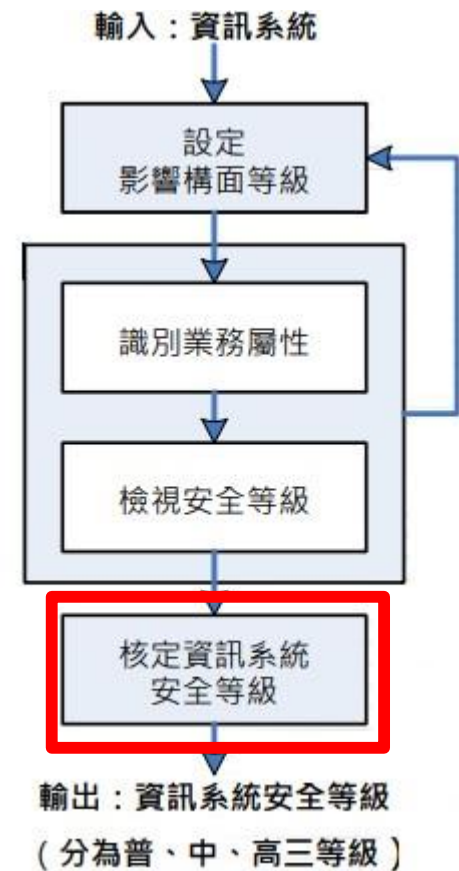
**業務類**：指機關內部業務單位之業務（如：交通監理、便民服務等）。



# 資通系統防護需求分級原則

- 步驟3：

由資訊單位將各資訊系統「**安全等級評估表**」中資訊，彙整至「**資訊系統清冊**」，資訊系統安全等級經相關主管確認後，由**資訊安全長核定**。共同性系統之分級，統一由開發管理之機關進行評估與鑑別。



# 資通系統防護需求分級原則

防護需求等級依據該系統相關之機密性、完整性、可用性及法律遵循性四個構面中之**最高者定之**。

防護需求 等級 構面	普	中	高
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 <b>有限之影響</b> 。	發生資通安全事件致資通系統受影響時，可能造成 <b>未經授權之資訊揭露</b> ，對機關之營運、資產或信譽等方面將產生 <b>嚴重之影響</b> 。	發生資通安全事件致資通系統受影響時，可能造成 <b>未經授權之資訊揭露</b> ，對機關之營運、資產或信譽等方面將產生 <b>非常嚴重或災難性之影響</b> 。



# 資通系統防護需求分級原則

## 機密性判斷舉例：

普	中	高
一般性資料；資料外洩 <b>不致影響</b> 機關權益或導致機關權益 <b>輕微受損</b> 。	敏感性資料；資料外洩將導致機關權益 <b>嚴重受損</b> 。 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。	機密性資料； <b>資料外洩將危及國家安全、導致機關權益非常嚴重受損</b> 。 凡涉及國家安全之外交、情報、國境安全、財稅、經濟、金融、醫療等重要機敏系統。特殊屬性之個人資料（如：臥底警員、受保護證人、被害人等資料），資料外洩可能會使相關個人身心受到危害、社會地位受到損害、或衍生財物損失等情形。 <b>極大規模（如：全國性）之涉及識別個人之資料。</b> <b>例如：戶役政資訊系統、護照管理系統等。</b>

# 資通系統防護需求分級原則

防護需求 等級 構面	普	中	高
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 <b>有限</b> 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 <b>嚴重</b> 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 <b>非常嚴重或災難性</b> 之影響。

完整性判斷舉例：

普	中	高
資料遭竄改 <b>不致影響</b> 機關權益或僅導致機關權益 <b>輕微受損</b> 。	資料遭竄改將導致機關權益 <b>嚴重受損</b> 。	資料遭竄改將 <b>危及國家安全、導致機關權益非常嚴重受損</b> 。

# 資通系統防護需求分級原則

防護需求 等級 構面	普	中	高
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 <b>有限</b> 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 <b>嚴重</b> 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 <b>非常嚴重或災難性</b> 之影響。

# 資通系統防護需求分級原則

可用性判斷舉例：

普	中	高
<ol style="list-style-type: none"><li>1. 系統容許中斷時間較長 (如：8小時以上)。</li><li>2. 系統故障對社會秩序、民生體系運作不造成影響或僅有輕微影響。</li><li>3. 系統故障造成機關業務執行效能輕微降低。</li></ol>	<ol style="list-style-type: none"><li>1. 系統容許中斷時間短 (如：4~8小時)。</li><li>2. 系統故障對社會秩序、民生體系運作將造成嚴重影響。</li><li>3. 系統故障造成機關業務執行效能嚴重降低。</li></ol>	<ol style="list-style-type: none"><li>1. 系統容許中斷時間非常短 (如：4小時以下或更短)。</li><li>2. 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。</li><li>3. 系統故障造成機關業務執行效能非常嚴重降低，甚至業務停頓。</li></ol>

# 資通系統防護需求分級原則

防護需求 等級 構面	普	中	高
法律 遵循性	其他資通系統設置或運作於法令有相關規範之情形。其他資通系統設置或運作於法令有相關規範之情形。	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。	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。

# 資通系統防護需求分級原則

法遵性判斷舉例：

普	中	高
各機關全球資訊網：必須符合智慧財產權相關法令尊重他人智慧結晶，並遵守兒童及少年福利與權益保障法進行資訊內容管理，否則將涉及違反法律之遵循性。	政府電子採購網：依「政府採購法」第27條規定，機關辦理公開招標或選擇性招標，應將招標公告或辦理資格審查之公告刊登於政府採購公報或公開於資訊網路。因此，若系統資料遭竄改導致公告資料錯誤，將影響採購作業透明化。	機密性資料：依「國家機密保護法施行細則」第28條第4款規定，國家機密之保管方式直接儲存於資訊系統者，須將資料以政府權責主管機關認可之加密技術處理，該資訊系統並不得與外界連線。  因此，機關若未依循規定儲存資料，將涉及從根本上違反法律之遵循性。



# 設定資通系統影響構面等級(附表九)

- 「全球資訊網(參考範例)」安全等級評估表

功能說明：機關官方網站，提供機關簡介及政策措施介紹，並無提供線上申辦等服務。

業務屬性：■業務 □行政性業務 日期：\_\_\_\_年\_\_月\_\_日

影響構面				資訊系統安全等級
1.機密性	2.完整性	3.可用性	4.法律遵循性	
普	普	普	普	普
資訊系統安全等級：				普

影響構面		安全等級	原因說明
1.機密性	初估	普	網站資訊均為可公開之一般性資料
	異動		
2.完整性	初估	普	本網站主要提供資訊公告
	異動		
3.可用性	初估	普	本網站提供一般性資料瀏覽
	異動		
4.法律遵循性	初估	普	本網站必須符合智慧財產權相關法令，並遵守兒童及少年福利與權益保障法及其相關規定、電腦網路內容分級處理辦法，惟不涉及從根本上違反法律之可能性，也不致因違反規範導致嚴重不良後果
	異動		

# 資通系統防護需求分級原則

---

- 資通安全法施行細則第四條：

- 各機關依本法第九條規定委外辦理資通系統之建置、維運或資通服務之提供（以下簡稱受託業務），選任及監督受託者時，應注意下列事項：

五. 受託業務包括客製化資通系統開發者，**受託者應提供該資通系統之安全性檢測證明**；

該資通系統**屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者**，委託機關應**自行或另行委託第三方進行**安全性檢測；涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。



# 資通系統防護需求分級原則

---

- 資通安全法施行細則第七條：
  - 前條第一項第六款所稱**核心資通系統**，指**支持核心業務持續運作必要之系統**，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其**防護需求等級為高者**。

# 資通系統防護基準



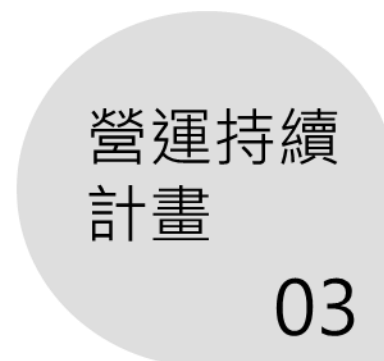
# 資通系統防護基準構面



A.9



A.12



A.17



A.13



A.14



A.13



A.12

# 資通系統防護基準類別

構面	控制措施
存取控制	帳號管理 最小權限 遠端管理
事件日誌與可歸責性	紀錄事件 日誌紀錄內容 日誌儲存容量 日誌處理失效之回應 時戳及校時 日誌資訊之保護
持續營運計畫	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

# 資通系統防護基準類別 (續)

構面	控制措施
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

# 資通系統防護基準控制措施(附表十)

機關名稱↵

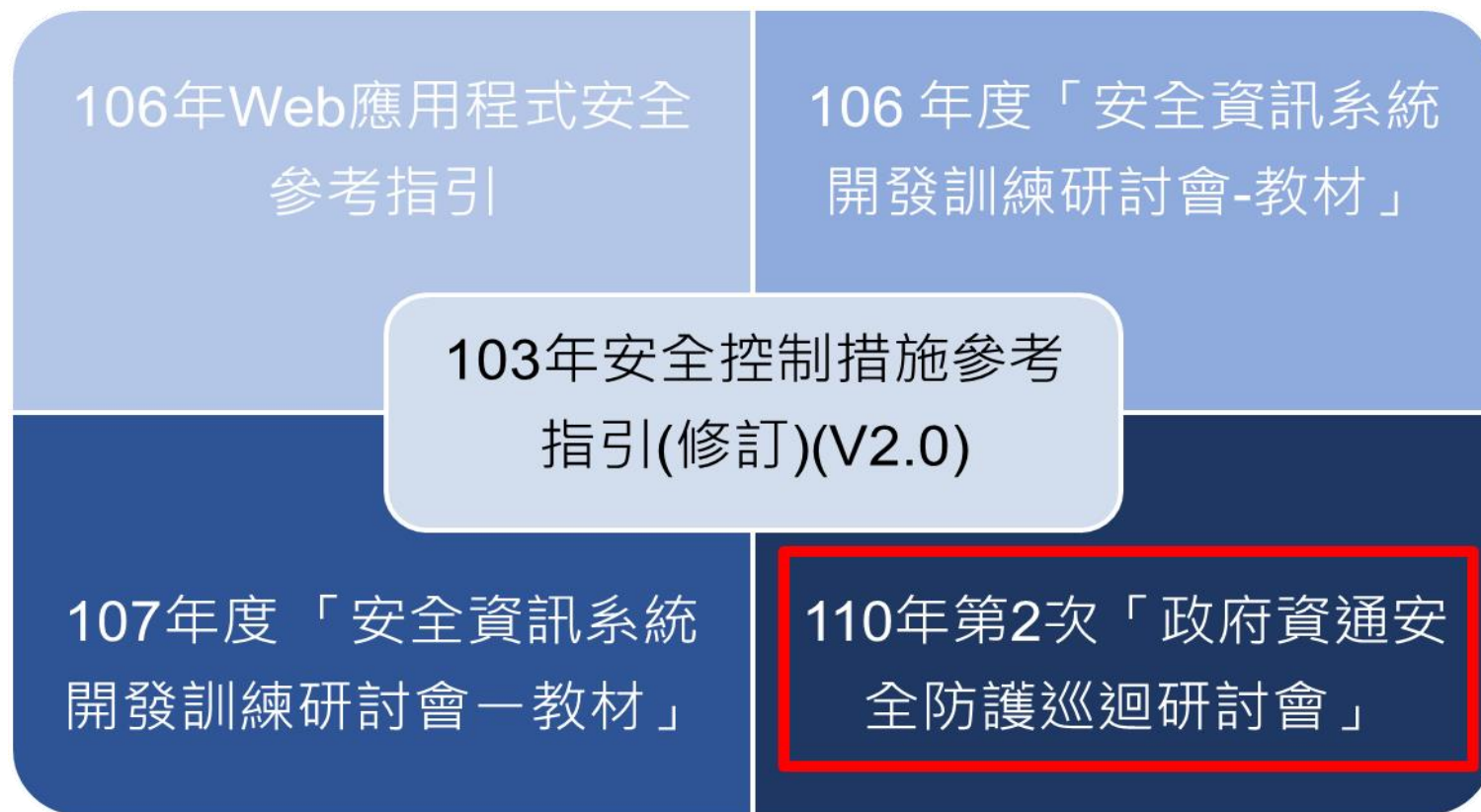
附表十、資通系統防護基準控制措施查檢表↵

單位(處/科)↵	↵	管理人↵	↵	填表日期↵	↵
系統名稱↵	↵			防護需求等級↵	□普□中□高↵
建置廠商↵	↵		維護廠商↵	↵	
系統版本↵ 類別↵	<input type="checkbox"/> 共用 <sup>1</sup> <input type="checkbox"/> 公版 <sup>2</sup> ↓ <input type="checkbox"/> 機關自用 <input type="checkbox"/> 其他 _____↓ <small>註 1：共用：2 個以上機關共同使用之系統 (如戶政、地政、財政、人事差勤系統)。↓</small> <small>註 2：公版：各機關依特定版本自行維運使用(如公務出國報告資訊網、電子公文系統)。↵</small>				是否還有維護合約？↵ <input type="checkbox"/> 無↓ <input type="checkbox"/> 有，至_____為止↵
系統建置↵ 方式↵	<input type="checkbox"/> 自行委外 <input type="checkbox"/> 租用服務 ↓ <input type="checkbox"/> 自行開發 <input type="checkbox"/> 主管/上級機關提供↓ <input type="checkbox"/> 其他 _____↵				

# 資通系統防護基準(委外廠商)

- 依據行政院國家資通安全會報技術服務中心，訂定之共通規範；109年政府資訊作業**委外資安參考**指引(修訂)v6.2所示：
  - 其中系統發展類規範明定：**系統開發與系統維護**需於規劃系統開發類專案時，機關應先參考「資通安全責任等級分級辦法」附表9 所訂之資通系統防護需求分級原則，以資通系統之機密性、完整性、可用性及法律遵循性等 4 大構面，評估該資通系統之防護需求等級。接續機關應依「資通安全責任等級分級辦法」附表 10 所訂**資通系統防護基準列示之控制措施**，**識別應落實之資安相關事項**，並載明於RFP。

# 資通系統防護基準參考來源



資安防護訊息



共同規範



# 資通系統防護基準構面-存取控制

## • 帳號管理

等級	控制措施	控制說明
普	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。	資通系統之帳號應透過正式的帳號申請程序所建立，完成開通審核程序始能使用，因此系統應具備帳號管理機制，可對系統帳號進行申請、開通、停用或刪除之行為。
中	已逾期之臨時或緊急帳號應刪除或禁用。	若具有臨時帳號或緊急帳號時，應實作已逾期之系統帳號檢查機制，於帳號逾期時自動停用或刪除，以避免帳號遭有心人士盜用。
中	資通系統閒置帳號應禁用。	宜記錄系統帳號最後登入時間，可透過工作排程，檢查是否有持續一段時間(如半年等)未登入系統之帳號，並實作自動停用該帳號之功能。
中	定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。	定期審核資通系統帳號使用現況，檢視是否存在帳號被異常建立、竄改或啟用等行為，並停用或刪除閒置帳號與臨時帳號。
高	機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。	會談(Session)機制目的為管理使用者與伺服器之間的連線狀態，應定義允許使用者於系統中未進行活動之時間，並應定義資通系統之使用情況及條件(如特定時間或指定IP來源等)。
高	逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。	使用者於系統中若一段時間未進行活動，系統應有自動機制將該使用者的會談階段設為失效而登出系統，以降低資安風險。
高	應依機關規定之情況及條件，使用資通系統。	應依據機關規定之情況及條件，限制系統使用行為(如僅開放平時上班時間使用系統、特定功能或機敏資訊僅允許透過內部網路存取等)。
高	監控資通系統帳號，如發現帳號違常使用時回報管理者。	應具備監控及通知機制，向系統管理者回報帳號異常使用行為(如短期內大量帳號登入失敗或存取未經授權之資源等)。

# 資通系統防護基準構面-存取控制

## • 最小權限

等級	控制措施	控制說明
中	採用最小權限原則，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。	使用者(或代表使用者行為之程序)應以完成該工作所需的最小權限操作系統功能，避免過度授權而增加系統資源被不當存取的風險。因此在進行授權決定時應考量該使用者(或代表使用者行為之程序)之業務性質與範圍，限制其所能存取的系統功能及資料。

# 資通系統防護基準構面-存取控制

## • 遠端存取

等級	控制措施	控制說明
普	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。	機關應明確訂定資通系統之存取限制、組態需求、連線需求，並將這些資訊文件化，以供日後查檢。
普	使用者之權限檢查作業應於伺服器端完成。	應於伺服器端實作權限檢查機制，並預設禁止任何未通過權限檢查之存取行為，以避免被使用者繞過。
普	應監控遠端存取機關內部網段或資通系統後臺之連線。	資通系統所允許之遠端連線活動，應使用監控設備或其他可偵測未經授權使用的設備，在發現異常連線或存取行為時提出警告，以防止資通系統被不當使用。
普	應採用加密機制。	遠端存取資通系統時，應以加密機制保護機敏資料傳輸時之機密性。常見作法如採用HTTPS加密傳輸等，並選擇高強度之協定版本及演算法。
中	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。	遠端存取行為應經過適當授權後始可放行，若有必要允許外部遠端存取之系統功能，應限制資通系統遠端存取之來源(如機器、網路位址等)，預先定義合法來源並進行管理，避免全面性開放存取。

# 資通系統防護基準構面-事件日誌與可歸責性

## • 記錄事件

等級	控制措施	控制說明
普	訂定日誌之記錄時間週期及留存政策，並保留日誌 至少六個月。	應依機關規定之時間週期及日誌留存政策，保留系統日誌(Log)，目的包含程式除錯、行為歸責、日誌取證及法規要求等。
普	確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。	資通系統應實作記錄特定事件之功能，如身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等。
普	應記錄資通系統管理者帳號所執行之各項功能。	系統管理者為資通系統內具有最高權限之帳號，對系統及資料極具影響力，記錄所有管理者帳號執行之各項功能，有助於定期稽核系統行為及資安事件追查。
中	應定期審查機關所保留資通系統產生之日誌。	機關應訂定日誌審查時程，由負責人員檢視日誌紀錄內容，以掌握是否在期間內曾發生重要的資安事件，如異常的存取行為、重大的系統錯誤等。

# 資通系統防護基準構面-事件日誌與可歸責性

## • 日誌紀錄內容

等級	控制措施	控制說明
普	資通系統產生之日誌應包含事件類型、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，並採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。	日誌應詳細描述所觸發的事件，包含人、事、時、地、物等關鍵資訊，宜包含：使用者帳號(避免個資類型)、時間、執行之功能或存取之資源名稱、事件類型或優先等級、執行結果或事件描述、事件發生當下相關物件資訊、網路來源與目的位址，以及錯誤代碼等。盡可能採用單一的Log機制，如同一伺服器軟體應產出相同格式之日誌等，以便於事件比對與追查。日誌應依據法律政策或業務使用等需求，納入其他相關資訊，如憑證資訊、會談識別碼等。

# 資通系統防護基準構面-事件日誌與可歸責性

- 日誌儲存容量

等級	控制措施	控制說明
普	依據日誌儲存需求，配置所需之儲存容量。	資通系統應配置日誌所需之儲存容量(如磁碟或資料庫空間等)，避免因儲存容量不足造成日誌處理失效。



# 資通系統防護基準構面-事件日誌與可歸責性

## • 日誌處理失效之回應

等級	控制措施	控制說明
普	依據日誌儲存需求，配置所需之儲存容量。	資通系統應配置日誌所需之儲存容量(如磁碟或資料庫空間等)，避免因儲存容量不足造成日誌處理失效。
高	機關規定需要即時通報之日誌失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。	應定義需要即時通報的特定日誌失效事件、即時通報的時效以及特定通知對象，並實作通知機制，以利及早釐清事件發生原因並進行故障排除。如當日誌紀錄無法正常寫入資料庫時，以信件或簡訊通知系統維護人員。



# 資通系統防護基準構面-事件日誌與可歸責性

## • 時戳及校時

等級	控制措施	控制說明
普	資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。	使用系統內部時鐘產生日誌所需時戳，採用全系統一致的時間標準，有助於彙整資安事件所發生的各種事件時間點，進而分析資安事件可能發生的原因。
中	系統內部時鐘應定期與基準時間源進行同步。	日誌必須維持使用精確的時間，以利事件追蹤及日誌取證等用途，實務上，可使用網路時間協定(Network Time Protocol, NTP)，讓機關內各個系統及網路設備與校時伺服器進行同步，如國家標準時間伺服器(time.stdtime.gov.tw)或使用機關自建之伺服器。

# 資通系統防護基準構面-事件日誌與可歸責性

## • 日誌資訊之保護

等級	控制措施	控制說明
普	對日誌之存取管理，僅限於有權限之使用者。	應施行日誌存取控管，避免未經授權使用者惡意讀取、竄改或刪除日誌。
中	應運用雜湊或其他適當方式之完整性確保機制。	日誌資訊以安全雜湊演算法產生，並留存其雜湊值，後續可對資料再次產生雜湊值並與原先結果進行比對，以確保資料未遭到異動竄改。
高	定期備份日誌至原系統外之其他實體系統。	定期將日誌備份至與原系統不同之實體系統，如建置Log伺服器或設定系統排程等方式，集中管理及保存日誌之備份，可降低因系統損毀或人為惡意刪除而無法取用日誌之風險。

# 資通系統防護基準構面-營運持續計畫

## • 系統備份

等級	控制措施	控制說明
普	訂定系統可容忍資料損失之時間要求。	機關應訂定可容忍資料損失之時間要求，若資安事件發生造成資料損失時，需使用最接近的備份資料進行復原，資料損失與備份資料之間的時間間隔，亦稱為復原點目標(Recovery Point Objective, RPO)。RPO一旦訂定完成，則可協助系統維護人員選擇適合的備份機制及頻率。如若訂定為1小時，則至少每小時必須進行一次資料備份，所選擇的儲存媒體可能為磁碟；但若RPO訂定為一週(168小時)，則至少每週進行一次資料備份，使用磁帶或光碟片等媒體即可滿足備份需求。
普	執行系統源碼與資料備份。	應備份系統源碼與資料，備份時機如廠商交付或內容變更時，或依機關規定定期備份。
中	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。	常見之儲存媒體如磁碟、磁帶、光碟等，因使用方式及保存環境之差異，可能影響儲存媒體壽命而造成備份資料損毀。機關應訂定週期性測試時間表，並依時間表進行備份資料還原測試，以確保備份資料處於可用狀態。
高	應將備份還原，作為營運持續計畫測試之一部分。	災害復原是營運持續計畫中相當重要之環節，其目的是為了在發生天災、人為疏失或惡意破壞造成資通系統損害時，能快速回復至正常或可接受的營運水準。營運持續計畫應定期完整測試、演練，以驗證計畫之適切性及有效性，在災害復原過程中應使用備份資料，以驗證備份機制是否正確可靠。
高	應在與運作系統不同地點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。	備份資料應有適當的實體(如防火櫃等)及環境保護，且不可儲存於運作系統處，以避免因系統損毀造成無法取用備份資料之情況。將備份資料異地存放於離運作系統有一段距離之場所，則可減少災害(如火災等)發生時，同時傷害正式資料與備份資料的風險。

# 資通系統防護基準構面-營運持續計畫

## • 系統備援

等級	控制措施	控制說明
中	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。	機關應考量服務需求、使用現況、相關資源項目，以及資安事件發生之風險，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，亦可稱為復原時間目標(Recovery Time Objective, RTO)。
中	原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。	機關應準備適當及足夠的備援設備或其他方式，以便在發生災害時，可於所訂定之容忍時間內讓服務回復正常運作。

# 資通系統防護基準構面-識別與鑑別

## • 內部使用者之識別與鑑別

等級	控制措施	控制說明
普	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。	資通系統應具備唯一識別及鑑別機關使用者之功能，如替內部使用者建立個別帳號，以強化系統之可歸責性(Accountability)。若多人共用同一個帳號登入系統，則難以從日誌識別確切的使用者身分。
高	對資通系統之存取採取多重認證技術。	系統身分驗證或重要交易行為，可採用多重因素身分驗證以強化安全性。多重因素身分驗證係指具備兩種以上驗證類型，驗證類型一般區分為所知之事(如密碼、特定問題之答案、簡訊、電子郵件)、所持之物(如晶片卡、憑證、TOKEN、OTP)及所具之形(如指紋、虹膜辨識等生物特徵)。



# 資通系統防護基準構面-識別與鑑別

## • 身分驗證管理

等級	控制措施	控制說明
普	使用預設密碼登入系統時，應於登入後要求立即變更。	使用者註冊時係由資通系統或人工配發預設密碼者，於使用者首次登入時，應強制其變更預設密碼。
普	身分驗證相關資訊不以明文傳輸。	系統傳輸身分驗證相關資訊(如帳號密碼等)時，採用加密傳輸可降低機敏資訊外洩之風險。
普	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。	系統應實作帳戶鎖定機制，並建議以電子郵件通知使用者。於鎖定期間禁止該帳號所有登入嘗試，超過鎖定時間則重新計次。
普	使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。	應強制最低密碼複雜度，包含密碼長度限制及組成字元種類，目的在避免因使用安全性不足之密碼而被人輕易破解。強制密碼最短效期目的在防止使用者規避3次密碼歷程之限制，而於短期內頻繁變換密碼後又改回原始密碼。強制最長之效期之目的在避免固定使用同一組密碼。實務上，可參考政府組態基準(Government Configuration Baseline, <b>GCB</b> )之建議值，設定密碼複雜度及密碼使用效期限制。
普	密碼變更時，至少不可以與前三次使用過之密碼相同。	使用者前3次舊密碼應被保留(以雜湊值形式)，於設定新密碼時，比對新密碼與舊密碼之雜湊值，若雜湊值相同則拒絕此次密碼設定。

# 資通系統防護基準構面-識別與鑑別

## • 身分驗證管理

等級	控制措施	控制說明
中	身分驗證機制應防範自動化程式之登入或密碼更換嘗試。	系統若採用帳號密碼進行身分驗證，往往可能遭受到自動化程式以暴力破解方式嘗試登入。如圖形驗證碼(CAPTCHA)為常見的防範方式，透過將驗證碼以圖形方式呈現於頁面上，並要求使用者辨別該圖形中文字之方式，或以其他足以辨識人為動作之方式(如勾選特定選項等)，防堵自動化程式之嘗試行為。
中	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。	密碼重設機制設計不良可能造成安全問題，常見錯誤是系統自行產生隨機密碼後以電子郵件寄送給使用者，此問題在於無法確保傳輸過程經過加密保護，故提高資安風險。使用者忘記密碼並啟動密碼重設機制時，應以使用者其他留存於系統的聯絡資訊，如電子郵件或手機號碼等，先要求使用者輸入該資訊，比對正確無誤後，發送一次性及具有時效性符記(如簡訊驗證碼、電子郵件驗證連結等)，一般會由亂數產生的英數字所組成，使用者接收後須於時效內進行輸入回傳動作，系統檢查回傳符記之有效性後，才允許使用者進行重設密碼動作。



# 資通系統防護基準構面-識別與鑑別

- 鑑別資訊回饋

等級	控制措施	控制說明
普	資通系統應遮蔽鑑別過程中之資訊。	資通系統身分鑑別頁面中，資料輸入欄位(如密碼等)應設定不以明文顯示方式，如以*取代真實輸入字元，以避免他人從旁窺視而盜取密碼。

# 資通系統防護基準構面-識別與鑑別

## • 加密模組鑑別

等級	控制措施	控制說明
中	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。	密碼不可以明文方式儲存，應經過加密或雜湊處理，使得系統管理者或是惡意入侵的攻擊者皆無法輕易取得使用者原始密碼，以降低密碼外洩風險。實務上，當使用者設定密碼時，應針對該帳號產生一個亂數值(Salt)，將密碼結合亂數值再以雜湊函式處理產生雜湊值後，分別於不同欄位儲存亂數值及雜湊值。後續使用者輸入密碼時，以輸入值添加當初設定密碼時產生的亂數，再次以雜湊函式處理，若產出結果同當初設定密碼時的雜湊值，則表示輸入密碼正確。

# 資通系統防護基準構面-識別與鑑別

- 非內部使用者之識別與鑑別

等級	控制措施	控制說明
普	資通系統應識別及鑑非機關使用者(或代表機關使用者行為之程序)。	資通系統若開放給外部使用者(含其他機關、委外開發與維護廠商、臨僱人員及一般民眾等)存取使用，應具備識別及鑑別之能力，如利用帳號、憑證或來源IP位址等方式，識別與鑑別使用者。

# 資通系統防護基準構面-系統與服務取得

## • 系統發展生命週期設計階段

等級	控制措施	控制說明
中	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。	可參照「 <a href="#">安全軟體設計參考指引</a> 」之第3章安全軟體設計階段實務活動，包含「安全設計原則」，進行系統設計時應參考使用的設計原則；「執行攻擊面分析」，進行攻擊面的定義、識別與對應方式，包含如何進行攻擊面的衡量與評估，並進行管理等；「執行風險分析」，軟體設計過程中，如何透過使用威脅建模與架構風險分析，進行系統架構與威脅的分析，並使用通用性的安全設計原則與控制措施，提供軟體安全風險分析與控制；「安全設計審查」，在進行一連安全軟體設計的實務活動之後，應確保安全設計符合需求階段提出的相關安全需求及安全設計，以符合軟體安全的基準線。
中	將風險評估結果回饋需求階段的檢核項目，並提出安全需求修正。	系統發展生命週期需求階段發展之安全需求檢核項目，可能未能充分符合系統之所有安全需求，故應依據風險評估結果進行修正。

# 資通系統防護基準構面-系統與服務取得

## • 系統發展生命週期開發階段

等級	控制措施	控制說明
普	應針對安全需求實作必要控制措施。	應於系統開發階段，針對安全需求實作必要之控制措施，輔以檢核表方式進行確認，可減少遺漏之可能。
普	應注意避免軟體常見漏洞及實作必要控制措施。	軟體開發時應避免常見漏洞，如OWASP TOP 10或CWE/SANS TOP 25等，這些錯誤容易被惡意攻擊者利用，造成資料被竊取、竄改或使軟體無法運作，故需實作必要控制措施，以降低資安風險。
普	發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。	系統應設計錯誤處理機制，當系統發生錯誤時，儘可能採取錯誤代碼或簡短訊息呈現，避免將詳細或除錯用訊息直接顯示於使用者頁面，以防被攻擊者用來刺探系統內部資訊，或根據錯誤訊息推測出系統可能之弱點。確保系統所有功能的程式碼，在程式的進入點之後，儘可能採用程式語言的try-catch陳述，捕捉可能發生的錯誤與例外狀況。另外，採用程式語言的finally陳述，確保將該段功能程式碼所使用的資源正確釋放。
高	執行「源碼掃描」安全檢測。	源碼檢測可於程式開發及測試階段進行，以及早發現源碼之安全實作問題，並進行修補。實務上，常使用自動化檢測工具以提高檢測效率，輔以有經驗之軟體開發人員進行檢測結果檢視及分析，檢測工具可參考OWASP組織整理之免費及商業化工具列表。
高	系統應具備發生嚴重錯誤時之通知機制。	系統應區分錯誤等級，若發生嚴重等級錯誤時，採用電子郵件或簡訊等通知機制，使系統管理員或相關人員可及時掌握狀況，以利進行後續處理。

# 資通系統防護基準構面-系統與服務取得

- 系統發展生命週期測試階段

等級	控制措施	控制說明
普	執行「弱點掃描」安全檢測。	弱點掃描係利用自動化工具，對受測目標進行安全性掃描，以找出系統潛在弱點。
高	執行「滲透測試」安全檢測。	滲透測試係在取得合法授權後，對受測目標進行安全探測，由專業人士模擬駭客的攻擊行為，以人工及自動化掃描工具或攻擊程式等方式，尋找並利用系統弱點入侵系統，並於檢測作業完畢後提供完整的評估報告。



# 資通系統防護基準構面-系統與服務取得

## • 系統發展生命週期部署與維運階段

等級	控制措施	控制說明
普	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。	就作業系統或平台之安全更新，定期評估、測試與更新。系統上線前，就作業系統或平台預設開啟的服務與埠口(Port)進行檢視與評估，正面表列需要開啟該服務及埠口之理由，並關閉不必要之項目。
普	資通系統不使用預設密碼。	使用者註冊時係由資通系統或人工配發預設密碼者，於使用者首次登入時，應強制其變更預設密碼。
中	於系統發展生命週期之維運階段，應執行版本控制與變更管理。	在維運階段可能因需求變更、系統除錯、功能精進等原因而需要變更系統組態，而版本控制之目的，即在記錄系統組態在某段時間內的變更行為，使得使用者在需要時可取回特定的版本，嚴謹的版本控制與變更管理可強化系統的安全性與可用性。



# 資通系統防護基準構面-系統與服務取得

- 系統發展生命週期委外階段

等級	控制措施	控制說明
普	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。	機關委外開發資通系統時，可參考本文件之內容，並依據不同之安全等級(高、中、普)制定適用之安全需求，明確納入委外契約以做為驗收時之依據。

# 資通系統防護基準構面-系統與服務取得

- 獲得程序

等級	控制措施	控制說明
中	開發、測試以及正式作業環境應為區隔。	開發環境、測試環境與正式作業環境可區隔成不同的設備及網段，限制所能存取的應用程式及資料庫，以保護正式作業環境系統及資料。實務上，開發人員常以本機電腦為開發環境，並連結使用本機端之資料庫進行應用程式開發。俟開發完畢則將應用程式部署至測試主機，並連結至測試用資料庫，供測試人員進行測試使用。俟測試完畢，再將應用程式部署至正式環境，並連結至正式資料庫提供上線服務。

# 資通系統防護基準構面-系統與服務取得

- 資訊系統文件

等級	控制措施	控制說明
普	應儲存與管理系統發展生命週期之相關文件。	系統發展生命週期之相關文件如系統需求書、系統規格書、系統發展計畫、系統測試計畫及測試報告等，應書面或電子化形式進行文件保存，並被納入管理程序。

# 資通系統防護基準構面-系統與通訊保護

## • 傳輸之機密性與完整性

等級	控制措施	控制說明
高	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。	資訊系統傳輸機敏資料時，應避免明文傳輸。實務上，常採用加密傳輸協定(如HTTPS等)，以確保機敏資料傳輸過程中的安全，並應採取較安全的傳輸協定(如TLS1.2以上)及加密演算法(Cipher)，以降低被破解之風險。亦可進一步於伺服器端設定強制使用加密傳輸協定(如啟用網站安全性標頭之HTTP Strict Transport Security強制安全傳輸技術等)，避免使用者透過非加密傳輸協定存取應用系統伺服器。
高	使用公開、國際機構驗證且未遭破解的演算法。	若使用自行創造的加密方式且未經過適當的驗證程序，可能存在設計瑕疵，增加被破解的風險。應採用公開、國際認可之演算法，如AES對稱式加密演算法、RSA非對稱式演算法及SHA安全雜湊演算法等。
高	支援演算法的最大長度金鑰。	系統若採用密碼學演算法時，應使用該演算法目前支援的最大金鑰長度，以減少被暴力破解解密之可能及弱點。
高	加密金鑰或憑證應定期更換。	產生網站HTTPS使用之憑證，應具備使用年限限制，並於到期前進行更換。系統若另行使用自行產生之加密金鑰，亦需定期更換。
高	伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。	伺服器端之金鑰一旦外洩，則加密機制視同無效，嚴重危害系統之機密性，故應訂定相關作業標準或管理規範，以妥善保護金鑰。如不將加密金鑰與加密資料存放於同一系統中，或對於加密金鑰的存取進行限制。

# 資通系統防護基準構面-系統與通訊保護

## • 資料儲存之安全

等級	控制措施	控制說明
高	資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。	資通系統重要組態設定檔案及機敏資料存於資料庫或其他儲存媒體時，應採用對稱式或其他加密方式，將機敏資料加密成密文後儲存，並於需要取得原文明文時解密還原，以減少機敏資料因儲存媒體有其他存取管道而洩漏的風險。

# 資通系統防護基準構面-系統與資訊完整性

## • 漏洞修復

等級	控制措施	控制說明
普	系統的漏洞修復應測試有效性及潛在影響，並定期更新。	針對系統所使用的外部元件與軟體進行表列，包含其版本資訊，定期關注元件版本更新訊息及安全漏洞通告，若有相關之安全漏洞，評估系統元件更新之必要性，並於系統測試環境進行更新測試驗證後，才於正式環境進行更新。
中	定期確認資訊系統相關漏洞修復之狀態。	注意相關之安全漏洞訊息(透過CVE 相關訊息網站、廠商安全通告等)，若發現採用之軟體或元件具有安全漏洞，應設法修復漏洞並定期追蹤修復之狀態。

# 資通系統防護基準構面-系統與資訊完整性

## • 資訊系統監控

等級	控制措施	控制說明
普	發現資通系統有被入侵跡象時，應通報機關特定人員。	應指派人員負責處理資通系統入侵攻擊相關資安事件，並於發現資通系統有被入侵跡象時，通報相關人員進行處理。
中	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。	機關應具備監控資通系統之能力，如指派專業人員或使用監控設備，用以偵測資通系統連線行為，當發現未授權之連線或存取行為應向系統維護人員提出告警。
高	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。	機關應透過多種工具及技術(如入侵偵測系統、入侵防禦系統、WEB應用程式防火牆、網路設備流量監控軟體等)達成監控能力，監控資通系統所有進出之通訊活動，以發現不尋常或未經授權之連線及存取行為，並進行資安事件分析。



# 資通系統防護基準構面-系統與資訊完整性

## • 軟體及資訊完整性

等級	控制措施	控制說明
中	使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。	提供完整性驗證工具以驗證軟體或資訊在儲存或傳輸過程中未被人惡意竄改，如網站可在檔案下載連結處，提供以安全雜湊演算法產生之雜湊值，並說明使用的雜湊演算法為何，供使用者取得資料後自行計算雜湊值進行比對。另外，為確保系統程式之完整性，可對系統程式檔案留存雜湊值，並進行監控比對，以偵測未授權之惡意變更。
中	使用者輸入資料合法性檢查應置放於應用系統伺服器端。	對於使用者輸入欄位資料應檢查是否符合預期之邏輯規則，實務上，以正規表示式(Regular Expression)驗證內容之合法性。檢查機制若於客戶端實作，容易被使用者繞過檢查機制，故應於應用系統伺服器端實作始視為有效。
中	當發現違反完整性時，資通系統應實施機關指定之安全保護措施。	機關應訂定相關安全保護措施，在發現資通系統完整性遭到破壞時採取適當之行動。如當發現資料庫或檔案被不當竄改、站台被植入惡意指令碼或元件等資安事件時，應通知系統管理者進行緊急應變處置，並依規定之通報流程進行資安事件通報作業。
高	應定期執行軟體與資訊完整性檢查。	重要資料或紀錄，以安全雜湊演算法產生並留存其雜湊值，後續可對資料再次產生雜湊值並與原先結果進行比對，以確保資料未遭異動竄改。

# 資安防禦策略探討



# 惡意攻擊入侵類型

## Hack Value 引起駭客的價值

對攻擊者而言有趣或**有意義(值得)**

## Vulnerability 弱點/脆弱性

存在**弱點**、**設計**或**配置錯誤**而導致事件發生危害系統的安全

## Exploit 利用

透過漏洞**破壞**資訊系統的安全

## Payload

利用**漏洞的程式碼**用以執行預設的惡意操作(如建立後門或刪除銷毀)

## Zero-Day Attack 零日攻擊

在軟體開發人員發布針對漏洞的修補前，利用此**程序漏洞**的攻擊

## Daisy Chaining 菊鏈/串聯傳輸

連結到一個網路環境或設備，利用相同訊息**連結其他網路或設備**

## Doxing 肉搜

由當事人**自行公布的社群網路或公開資訊**蒐集到的個人身分資訊

## Bot 機器人

Bot通常被用來**遠端控制**或**自動化執行預設任務**的應用程式

# 網路攻擊鏈(Cyber Kill Chain)

1.Reconnaissance 偵查弱點

2.Weaponization 製造武裝

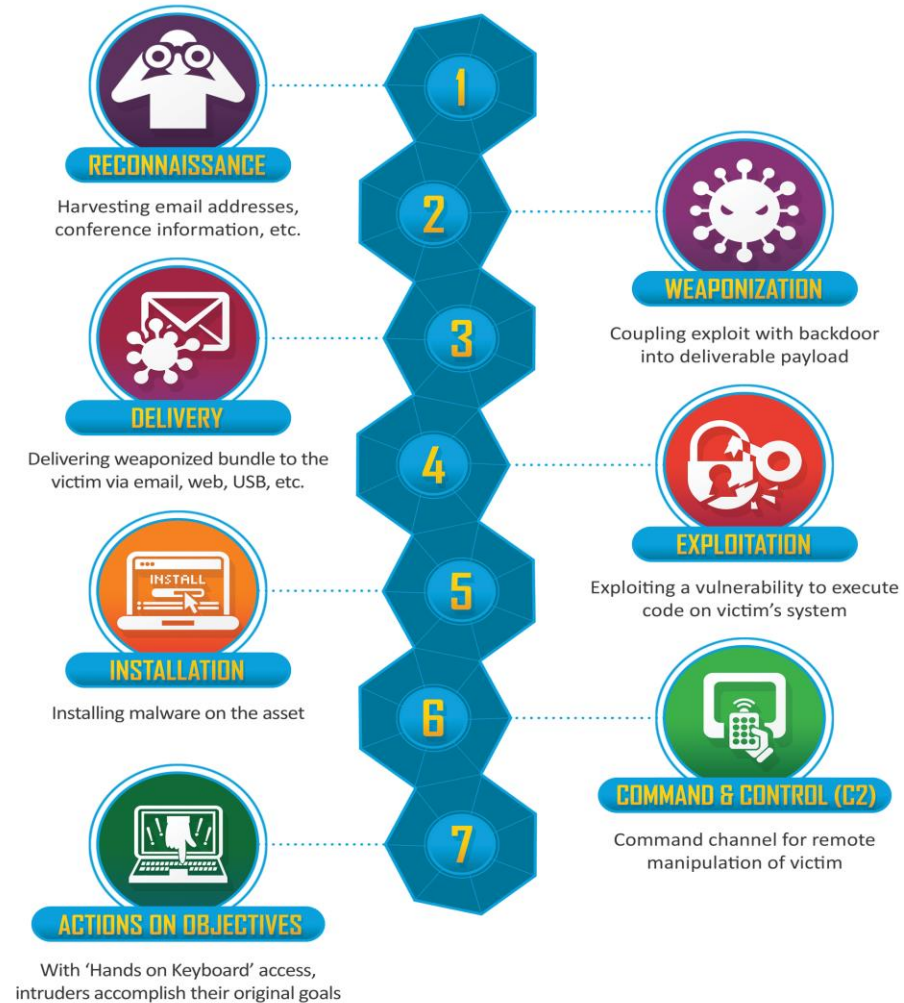
3.Delivery 傳送攻擊

4.Exploitation 觸發惡意程式(踩中陷阱)

5.Installation 安裝惡意程式(陷阱生效)

6.Control 控制系統與網路

7.Action 取得最高權限並發動攻擊



# 網路攻擊鏈(Cyber Kill Chain)(1)

- **Cyber Kill Chain**是目前驅使網路威脅趨勢/狩獵防禦常見的方法論，此方式可用來 識別和預防惡意的入侵活動。它亦可讓資安專業人員對於網路攻擊各階段有著深刻的體認，熟悉攻擊者的戰術、技術與程序的進行。
- **偵查(Reconnaissance)**：駭客研究、辨識及選擇目標，通常是代表搜尋網站上電子郵件地址、社交網路的關係或其他特定技術的資訊。因此此階段應針對開放性資訊與情報來源進行挖掘與分析，以發現可能的入侵企圖先期徵兆。
- **武裝(Weaponization)**：駭客通常是利用自動化的工具(weaponizer)，將木馬程式與弱點攻擊程式結合起來放在可傳遞的載具。常見的載具是使用者端應用程式的資料檔案，例如 Adobe PDF 或微軟 Office 文件。因此針對此階段應設法發展高準度的偵測碼。

# 網路攻擊鏈(Cyber Kill Chain)(2)

- **傳遞(Delivery)**：駭客將武器傳輸到攻擊目標環境。最普遍的武器載具運送的方法是電子郵件附件、網站及 USB 儲存媒體。**因此針對此階段應瞭解駭客會使用的載具，並發展攔截機制。**
- **弱點攻擊(Exploitation)**：當武器運送到受害者主機時，弱點攻擊就會觸發入侵者的程式。弱點攻擊通常是針對應用程式或作業系統的弱點，但也可以利用使用者本身或是作業系統自動執行程式的特性。**針對此階段可以利用弱點攻擊偵測技術來發現零時差攻擊。**
- **控制(Control)**：指在被駭系統上安裝可遠端存取的後門或木馬，讓入侵者可以在目標環境中維持存在。針對此階段可以布建入侵偵測機制以便發現新**安裝的後馬或木門**。



# 網路攻擊鏈(Cyber Kill Chain)(3)

---

- 執行(Execute)：指入侵者在目標環境中布建內部網路並進行資料竊取。因此針對此階段可以針對內部網路的行為進行偵測。
- 維持(Maintain)：指入侵者會在目標環境中維持存在，例如清除電腦或網路稽核軌跡(Audit Trail)。因此針對此階段可以佈建與稽核紀錄保持系統與先進的端點分析機制，以發現這些不正常的行為。





# MITRE ATT&CK 資安框架

---

- 基於真實世界觀察攻擊者的**戰術**(Tactics)和**技術**(Techniques)的通用知識庫框架。
- 作為私人企業、政府以及資安產品和社群中開發**特定威脅模型和方法**的基礎。
- 屬**開源框架**，任何人或組織都可以**免費**使用。
- 透過模擬駭客實際進行APT攻擊之網路攻擊鏈(Cyber Kill Chain)，來考驗**EDR**(Endpoint Detection and Response)與**資安產品**設備成效

# MITRE ATT&CK 資安框架(續)

- **TTP** :戰術(Tactic) 、技術(Technique) 、程序 (Procedure)

## 戰術(Tactic)

- 代表ATT&CK技術的「Why」，執行某項行動的戰術目標。如：入侵初期、執行、權限提升、防禦逃避、憑證存取、發現、橫向移動、收集、滲透、指揮與控制...等。

## 技術(Technique)

- 通過執行動作來「實現戰術目標」的「手法」。也可以代表對手通過執行一項行動而獲得的「收益」。可以顯示採取特定操作後要獲取的信息類型。

## 程序 (Procedure)

- 使用技術的過程，該過程是一個特定的使用實例或工具，可準確了解如何使用該技術以及使用對手模擬複製事件以及如何檢測案例。

# NIST網路安全框架(Cybersecurity Framework)

- 美國國家標準技術研究所 ( NIST ) 以現有的標準、指南以及實務所基礎所訂定的指南，用以解釋組織網路安全風險的指南，藉此強化網路安全。主要強化身分驗證與識別、資安風險的自我評估、管控供應鏈網路安全與弱點察覺

- 框架核心  
(Framework Core)
- 框架層級  
(Framework Tiers)
- 框架輪廓  
(Framework Profiles)



# NIST網路安全框架(Cybersecurity Framework)

識別( Identify ):建立組織規則以管理系統、人員、資產、資料和功能的網路安全風險

保護( Protect ):建立和實施適當的安全措施以確保重要服務的運行

偵測( Detect ):制定並實施適當的作為以識別網路安全事件的發生

回應( Respond ):對偵測到的網路安全事件，規劃並實施適當的行動

復原( Recover ):制定並實施適當的措施以修復因網路安全事件受損的功能和服務。

治理(Govern):組織如何制定和執行網路安全的明智決策

# NIST網路安全執行

- Step 1：確定優先級和範圍
- Step 2：確認組織目標與方向
- Step 3：描述當前資安狀況
- Step 4：進行風險評估
- Step 5：描述目標資安狀況
- Step 6：確定、分析差距並確定其優先級
- Step 7：實施行動計劃

關鍵基礎設施受到的網路威脅持續增加，是我們必須面對的最嚴重的國家安全挑戰之一。

面對這種威脅時，美國的國家和經濟安全仰賴國家基礎設施的可靠運作。

—摘自美國總統歐巴馬於 2013 年 2 月簽署的第 13636 號行政命令

