科 技 部 推 動 SSDLC 經 驗 分 享

資訊處　何昇龍　副處長

中華民國科技部
Ministry of Science and Technology, R.O.C.

簡報大綱

一 SSDLC 概要

二 案例分享

三 建議與討論

一、SSDLC概要



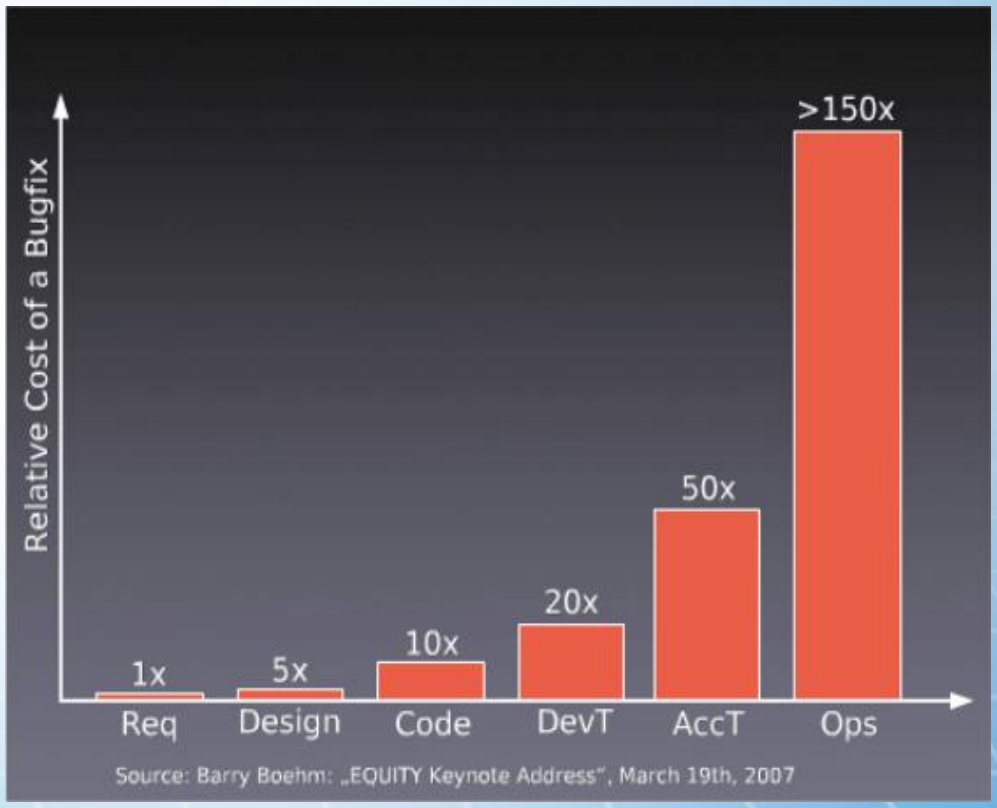

軟體發展生命週期 (SDLC)

SDLC (Software Development Life Cycle)：

軟體發展生命週期(也有稱系統發展生命週期)，進行階段分為：需求->設計->開發->測試->佈署維運 ，

- 整個過程以功能性導向，求最短時間完成開發與系統上線。
- 缺乏內建資訊安全之考量及特別要求，難以面對日新月異的攻擊手法。

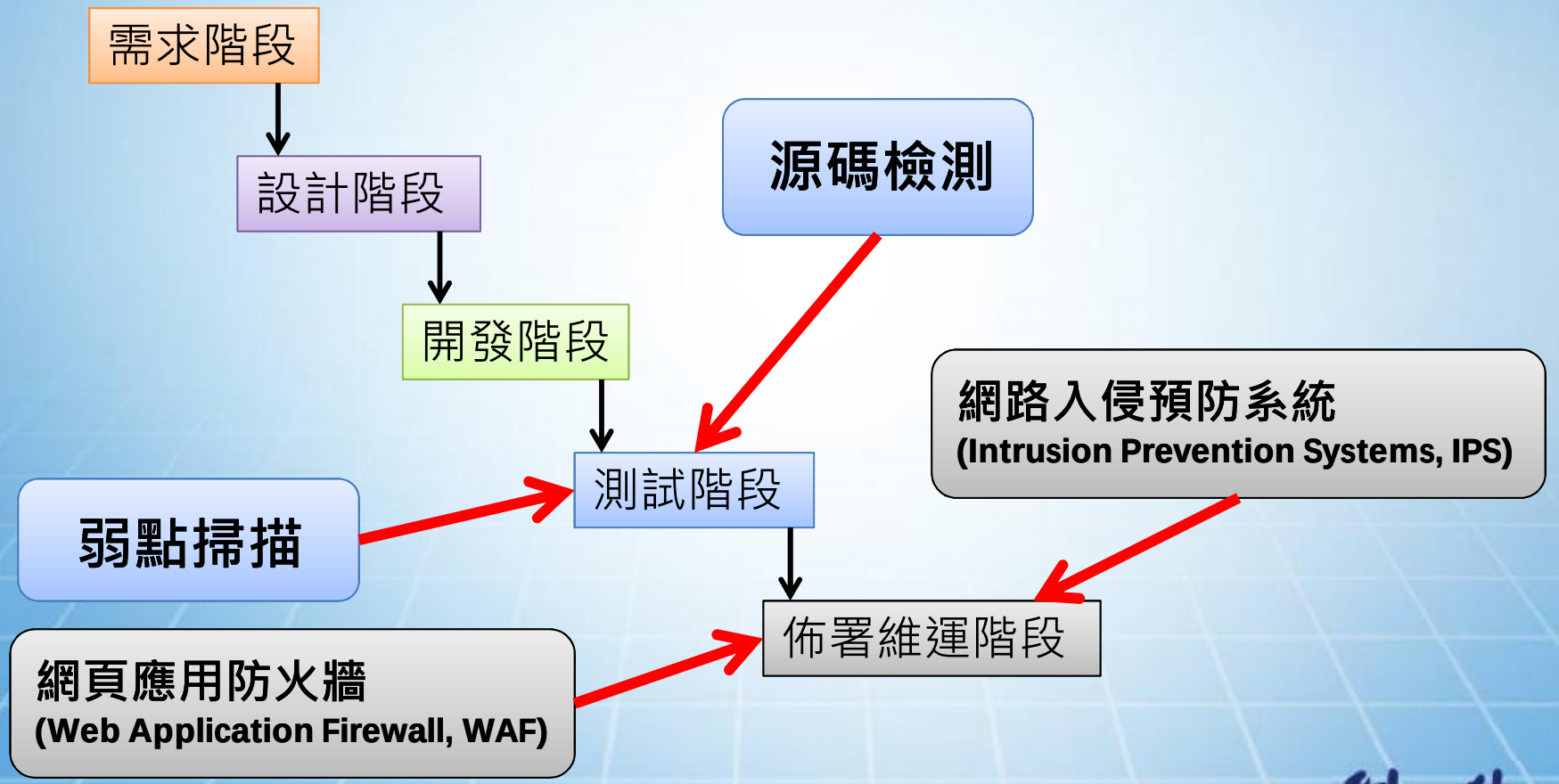
越晚修補，成本越高、風險也越大。



科技部 Ministry of Science and Technology

SDLC 資安風險常用補救措施

- 處理問題的方法
  - 集中後期處理、被動反應問題
- 無法解決系統設計、邏輯層次的安全瑕疵及缺點
  - 近年越來越多的漏洞，危害程度高複雜度卻較低，漏洞多出現於**應用系統程式**中

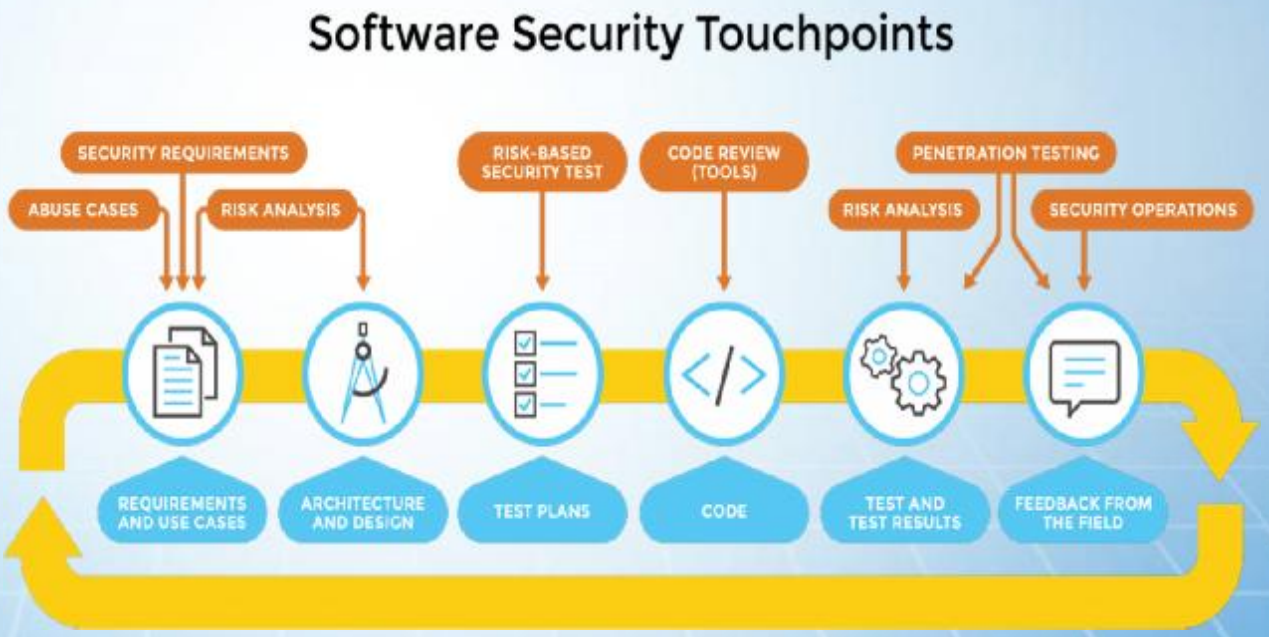


安全的軟體發展生命週期 (SSDLC)

❙ SSDLC (Secure Software Development Life Cycle)：

安全的軟體發展生命週期(Secure SDLC 或 S-SDLC)，
從專案開始的各階段(需求->設計->開發->測試->佈署維運)
就進行各項必要的安全防護措施(以 Cigital-Touchpoint Model 為例)。

Ø 可以降低後續系統維護的成本，及遭受攻擊的營運損失。



** 行政院國家資通安全會報技術服務中心

科技部 Ministry of Science and Technology

Secure SDLC 方法論比較

	Cigital – TouchPoint Model	MS - SDL	OWASP - CLASP
1	• External Review	• 安全教育訓練	• 安全意識宣導方案
2	• Define Security Requirements • High Level Risk Assessments • Define Use & Misuse Cases	• 考量安全需求 • 進行風險評鑑 • 使用品質關卡	• 捕捉安全軟體需求 • 施行應用程式評鑑
3	• Secure Architecture & Design Patterns • Threat Modeling • Security Architecture Review • Security Test Planning • Technical Risk Assessment	• 減少攻擊面 • 威脅建模 • 檢視安全設計	
4	• Peer Code Review • Automated Code Review • Security Unit Tests	• 採用通過檢驗工具 • 源碼靜態分析 • 拒用不安全函式	• 實作安全開發實務
5	• White Box Testing • Black Box Testing	• 重新審視威脅模型與攻擊面 • 源碼動態分析	• 建置漏洞修補程序
6	• Secure Configuration • Secure Deployment • Incident Management • Vulnerability Management	• 最終安全審查 • 事故應變計畫	• 定義監測安全評量 • 發布作業安全指引

行政院國家資通安全會報技術服務中心

- 網址：http://www.nccst.nat.gov.tw/
- 點選：資安防護訊息/共通規範

參考指引：

104年度政府資訊作業委外安全參考指引(修訂)(V4.0).rar
104年度無線網路安全參考指引(V3.0).rar
103年政府行動化安全防護規劃報告(V1.0).rar
103年資訊系統風險評鑑參考指引(修訂)(V3.0).rar
103年安全軟體設計參考指引.pdf
103年安全軟體測試參考指引.pdf
103年安全軟體發展流程指引.pdf
103年安全控制措施參考指引(修訂)(V2.0).rar
102年我國電腦機房異地備援機制參考指引.pdf
102年行動裝置資通安全注意事項.pdf
101年電子資料保護參考指引.rar
101年度行動裝置資安防護參考指引.pdf
100年個人資料保護參考指引.pdf
100年度Web應用程式安全參考指引與實作手冊.rar
100年度營運持續管理參考指引.rar
99年度政府資訊改造資安參考指引V1.2.rar
99年度Web應用程式安全參考指引(修訂).rar
97年度電子郵件安全參考指引v.2.rar
97年度資安產品選擇參考指引V.1.2.rar
97年度防火牆安全參考指引v.2.rar
96年度電子身分認證參考指引v.1.rar
96年度VPN安全參考指引V1.rar

- **S-SDLC強調如何將安全納入軟體發展生命週期各階段。**
- **在SDLC的每個階段都強調安全，並結合S-SDLC到一個組織的框架中有很多好處，以確保安全的產品。**

科技部 Ministry of Science and Technology

行政院 資訊系統分級與資安防護基準作業規定

Ⅰ 資訊系統分級與資安防護基準作業規定

- 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。

輸入：資訊系統

1. 設定影響構面等級

2. 識別業務屬性、檢視安全等級

3. 設定資訊系統安全等級

輸出：資訊系統安全等級

Œ：由業務承辦人依機密性、完整性、可用性及法律遵循性四大影響構面，分別評估對各資訊系統之影響衝擊，並據以設定影響構面等級。

•：識別資訊系統所支援之業務屬性，並由承辦單位主管檢視業務承辦人所設定安全等級之合理性。

Ž：資訊系統安全等級經承辦單位主管、資訊主管確認後，最後由資訊安全長核定。

** 資訊系統分級與資安防護基準作業規定

科技部 Ministry of Science and Technology

步驟說明 (1/2)

1. 設定影響構面等級 (安全等級：普、中、高)

步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估		
	異動		
2. 完整性	初估		
	異動		
3. 可用性	初估		
	異動		
4. 法律遵循性	初估		
	異動		

2. 識別業務屬性 (業務屬性：行政類、業務類 …)、檢視安全等級

步驟❷：識別業務屬性

項目		業務屬性	原因說明
識別業務屬性	初估		
	異動		

備註	

步驟說明 (2/2)

3. 設定資訊系統安全等級

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	
		資訊系統安全等級：		

機關之資訊系統清冊

資訊系統清冊

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	共同性系統(Y/N)	承辦(管理)單位	備註
1						
2						
3						

軟體專案導入 SSDLC

- **專案管理目標：**
  - 如期、如質、在預算內完成軟體專案 (On Time, On Quality, On Budget)
- **軟體建置案，導入 S-SDLC，可以思考之議題：**
  - 機關資訊系統安全等級評估。
  - 多是委外(廠商)開發。
  - 考量安全性需求，預算是否需適度增加？
  - 加入安全性需求，是否會影響專案期程？
  - 在專案各階段如何控管安全性需求之執行品質？
- **導入 S-SDLC 重點：**
  - 每一階段(規劃->需求->設計->開發->測試->佈署維運)，均要導入安全性的思維及相關措施。
  - 加強人員安全教育訓練，特別是廠商開發團隊。

二、案例分享




專案導入 SSDLC 概述

	安全需求 相關作業	[1]案	[2]案	[3]案	[4]案	[5]案
0. 招標階段	資訊系統安全等級評估表 RFP_資訊安全規範 RFP_SSDLC查檢表 廠商建議書與簡報					V
1. 規劃階段	專案工作計畫書 SSDLC查檢表				V	V
2. 需求分析階段	SRS 需求追溯表(RTM) 工作或訪談會議				V	V
3. 設計階段	SDS 系統測試計劃書 SSDLC測試個案查驗表				V	V
4. 開發階段	程式開發規範 源碼檢測報告 弱點掃描報告	V	V	V	V	V
5. 測試階段	驗證_SSDLC測試個案 SSDLC 測試報告	V	V	V	V	V
6. 佈署維運階段	強化組態安全 元件定期更新	V	V	V	V	V

建議書徵求文件-納入安全需求

- **以科技部民國105年進行之五大專案為例進行說明，包括：**
  - [1]案、[2]案、[3]案、[4]案、[5]案
- **哪些專案將資訊安全規範加入RFP？**
  - 各案RFP已要求須配合資訊安全管理系統(ISMS)規範，及設計開發測試需納入資訊軟體安全之考量等資安要求。
- **SSDLC查檢表：**
  - 各案RFP皆未加入SSDLC查檢表。
- **僅[5]案在投標簡報加入SSDLC說明。**

[建議事項：]

- **建議書徵求文件 (RFP)：**
  - RFP是機關對外招標之契約文件。
  - 將 SSDLC規範、SSDLC查檢表 列入RFP 。

廠商投標簡報 ([5]案)

遵循SSDLC全程落實系統資訊安全

OWASP Top 10 – 2013 (New)
A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control
A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards

存取控制
- 帳號管理
- 最小權限
- 遠端存取

稽核與可規則性
- 稽核事件
- 稽核紀錄內容
- 稽核儲存容量
- 稽核處理失效之回應
- 時戳
- 稽核資訊之保護

營運持續計畫
- 資訊系統備份
- 資訊系統備援

識別與鑑別
- 使用者
- 裝置
- 資訊管理
- 資訊回饋
- 加密模組鑑別

二、1.規劃階段




規劃階段-納入安全需求

- **於專案工作計畫書或分工結構圖(WBS)加入SSDLC之說明：**
  - 加入SSDLC說明之專案：[4]案、[5]案。
  - WBS加入SSDLC之專案： [5]案。

- **僅[5]案於啟動會議說明SSDLC執行規劃。**

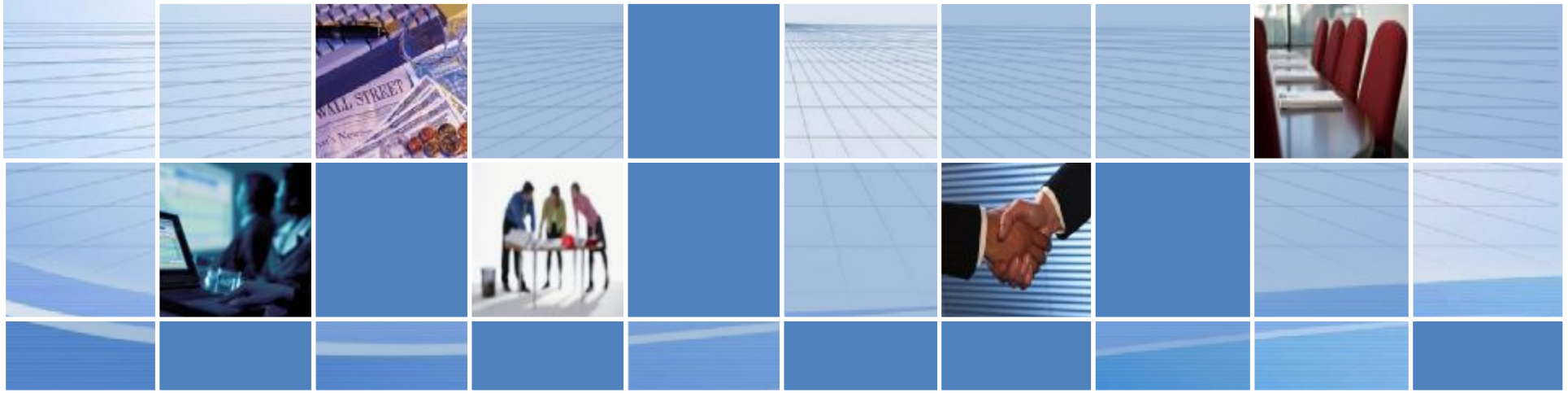
[建議事項：]

- **專案工作計畫書之製作：**
  - 規範廠商將SSDLC軟體安全需求列入計畫書內容，說明 SSDLC 在各階段之工作內容。
  - 規範廠商將SSDLC軟體安全相關工作列入分工結構圖(WBS)中。

- **專案啟動會議說明事項：**
  - 確定得標廠商後，需請廠商說明 SSDLC軟體安全需求如何執行與規劃。

**科技部-專案工作計畫書，P.38 (黃色背景文字)

二、2.需求分析階段



需求階段-納入安全需求

- **將RFP資安要求、SSDLC查檢表加入需求追溯表(RTM)：**
  - 各專案均已要求廠商將RFP所列資安要求及SSDLC查檢表納入需求追溯表(RTM)。
  - 有納入RTM，表示已訂定驗收標準，及列入各階段持續追縱項目。

[建議事項：]

- **需求追溯表：**
  - 在工作或訪談會議確認 SSDLC查檢表 相關安全性需求，並列入需求清單，作為需求階段交付項目之附件。
  - 提早確認各階段之安全性需求與工作，必免因安全問題而影響專案期程。
  - 專案各階段均透過需求追溯表、SSDLC查檢表持續追蹤。

- **SSDLC軟體安全需求查檢表：**
  - 依據各機關情況客製化。
  - 定期檢討調整 (各專案執行情況回饋)。
  - 可請資訊安全方面的專家或顧問協助。

**科技部-SSDLC軟體安全需求查檢表

範例 – 採用客製化查檢表

附件 4　軟體安全需求查檢表

分類	評量指標	適用分級	評估結果 (Y/N)
機密性	機敏資料傳輸時，採用加密機制	普	
	使用公開、國際機構驗證且未遭破解的演算法	中	
	使用該演算法支援的最大金鑰長度	中	
	加密金鑰或憑證週期性更換	中	
	加密金鑰具有保護機制	高	
	機敏資料儲存時，評估採用加密機制	高	
完整性	機敏資料傳輸過程，使用防止竄改的協定	普	
	提供下載的資料，產生雜湊值供比對其完整性	中	
	重要系統資料留存雜湊值以確保完整性	高	

軟體安全特性分類

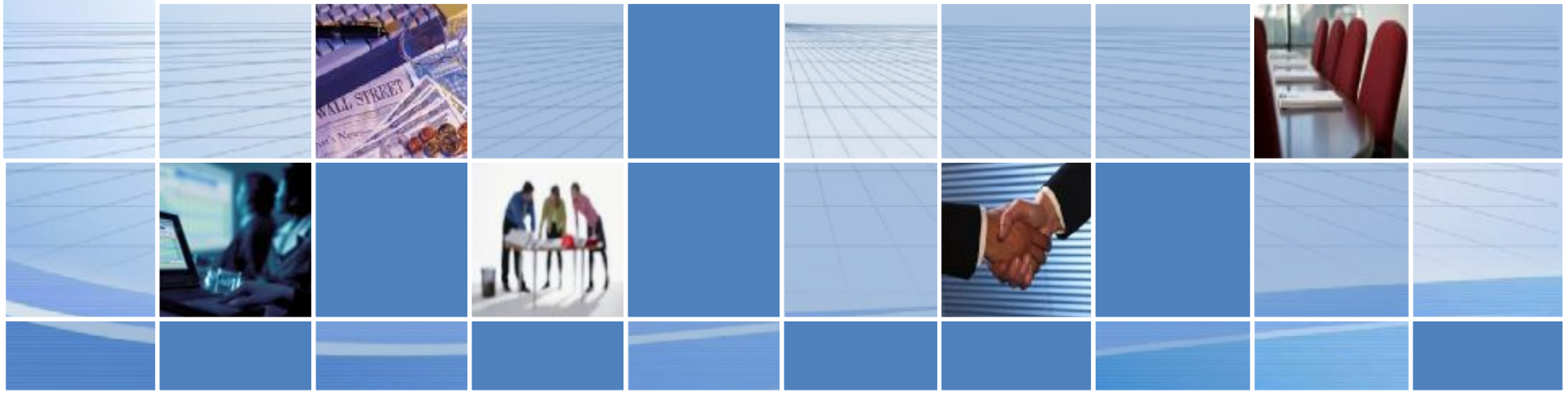
安全等級

（普、中、高）

軟體安全特性分類

- **C.I.A：(**須同時考量資料分級**)**
  - 機密性(Confidentiality)
  - 完整性(Integrity)
  - 可用性(Availability)
- **授權：**
  - 身分驗證(Authentication)
  - 授權(Authorization)
  - 稽核(Auditing)
- **其他：**
  - 會談管理(Session Management)
  - 錯誤及例外處理(Error and Exception Handling)
  - 組態管理(Configuration Management)

二、3.設計階段



設計階段-納入安全需求(1/2)

- **設計時納入SSDLC之考量：**
  - 廠商在設計時是否有納入SSDLC，實務上如何去檢核是很重要。
  - 設計前：RFP納入SSDLC相關要求。
  - 設計時：依據需求追溯表(RTM)，要求廠商於交付之文件需有對應設計說明。
  - 設計後：於測試階段，以檢測工具及測試個案進行驗證。
  - 僅[4]案、[5]案，
    有要求廠商在設計階段納入完整SSDLC之考量。
  - 僅[4]案、[5]案，
    測試階段有針對SSDLC查檢表要求廠商以測試個案進行驗證。

[建議事項(1/2)：]

- **請廠商檢視下列各項作業與軟體安全需求相關之設計：**
  - 軟硬體環境及佈署規劃。
  - 開發環境及系統開發規範(包括避免使用不安全之設計、元件或API)。
  - 程式設計所選用之框架及第三方元件。
  - 業務流程、權限、稽核、及各功能設計。
  - 資料庫設計。

設計階段-納入安全需求(2/2)

[建議事項(2/2)：]

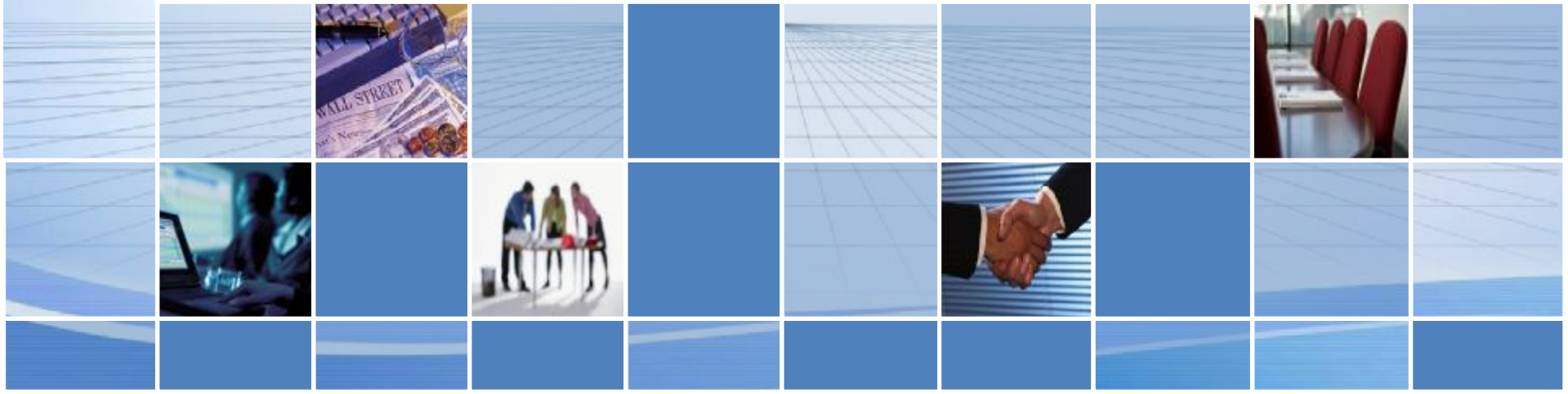
- **程式細部設計：**
  - 廠商須將與軟體安全需求相關的實作機制，融入細部設計說明中，確保後續程式撰寫人員能據以開發。
  - 與資安需求相關設計項目，須能對應到SSDLC查檢表。

- **準備測試個案：**
  - 在系統測試計畫書(或系統測試規格書)中，依據需求追溯表、及SSDLC查檢表，設計與軟體安全需求相關之測試個案，於測試階段據以驗證安全性相關需求。

常見威脅 - Microsoft STRIDE

	代表涵義	描述	軟體安全特性
S	偽冒 (Spoofing)	假冒為某人或某物	身分驗證 (Authentication)
T	竄改 (Tampering)	惡意的修改資料	完整性 (Integrity)
R	否認行為 (Repudiation)	使用者可以否認曾經進行某行為	不可否認性 (Non-Repudiation)
I	資訊洩漏 (Information Disclosure)	資訊被洩漏給不被預期可存取的個體	機密性 (Confidentiality)
D	拒絕存取服務 (Denial of service)	對使用者拒絕服務或降低服務水準	可用性 (Availability)
E	權限提升 (Elevation of privilege)	未正常授權取得權限能力	授權 (Authorization)

二、4.開發階段



開發階段-納入安全需求(1/2)

- **開發階段，廠商以工具方式檢測情況：**
  - 檢測到較多中、高風險之案例。

    源碼檢測安全性評估報告_案例一(20160623))

  - 在專案一開始就納入資安考量，就能呈現較佳之檢測結果，並配合每月定期檢測之案例。

    源碼檢測安全性評估報告_案例二(20160929)

    源碼檢測安全性評估報告_案例三(20161027)

開發階段-納入安全需求(2/2)

[建議事項：]

- **功能清單-掌握開發進度：**
  - 功能清單係指操作畫面、報表、介接、批次作業等各類功能。
  - 依據需求階段產出之功能清單，請廠商填報開發進度(已開發、未開發)。
  - 依據需求追溯表、SSDLC查檢表，
    監控軟體安全需求相關設計之開發進度。

- **避免常見弱點：**
  - 請廠商提交源碼檢測、弱點掃描報告 ，
    並至少須完成中、高等級之風險議題修正。
  - 檢測或掃描內容須包含主機弱點及OWASP最新發布之Top 10弱點等
  - 相關檢測掃描所用工具，及是否交第三方檢測或掃描，
    需先經相關專案會議確認。

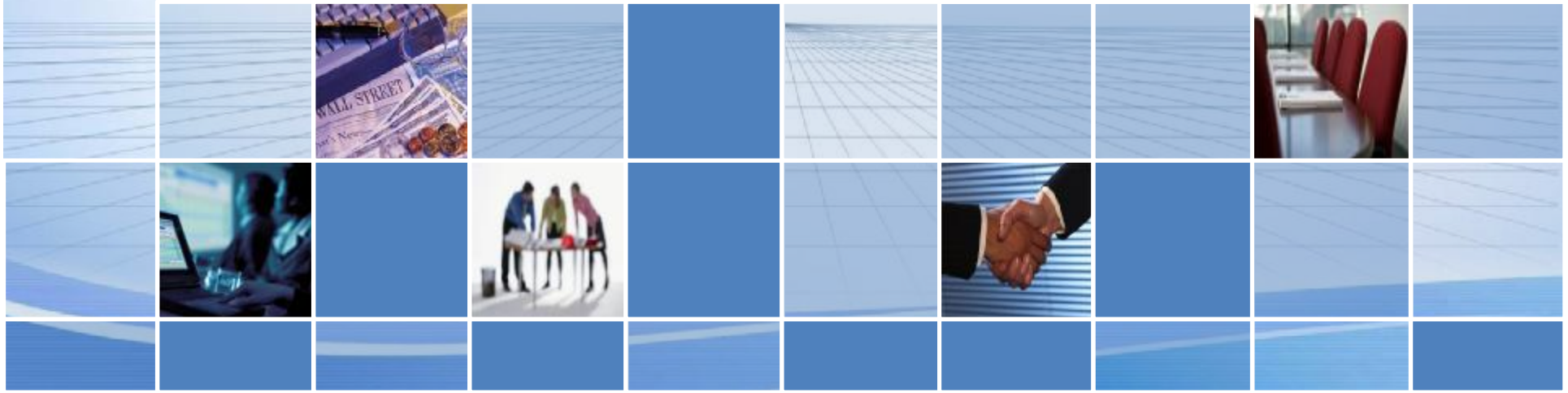
常見弱點 - OWASP Top 10 2013

	代表涵意	軟體安全特性
A1	Injection (注入攻擊)	機密性、完整性
A2	Broken Authentication and Session Management (失效的驗證與連線管理)	身分驗證、會話管理
A3	Cross-Site Scripting (XSS，跨腳本攻擊)	機密性、完整性
A4	Insecure Direct Object References (不安全的物件參考)	授權
A5	Security Misconfiguration (不當的安全組態設定)	組態管理
A6	Sensitive Data Exposure (敏感資料曝露)	機密性
A7	Missing Function Level Access Control (存取控制缺乏權限分級功能)	授權
A8	Cross-Site Request Forgery (CSRF，跨站冒名請求)	授權
A9	Using Components with Known Vulnerabilities (使用已知漏洞元件)	組態管理
A10	Unvalidated Redirects and Forwards (未經驗證的重新導向與轉送)	完整性

其他常見網頁程式漏洞

漏洞	舉例說明
B1 – 過度資訊揭露	登入頁面，貼心告訴使用者，帳號錯誤、密碼錯誤等錯誤細節。
B2 – Robots.txt 洩漏網站架構	有些網站會利用Robots.txt告訴網頁爬蟲程式相關目錄位置。
B3 – 檔案上傳機制	對上傳檔案未適當過濾及限制。
B4 – AJAX 機制	透過AJAX進行非同步請求處理，卻未啟用Session管理機制。
B5 – Cross Frame Scripting (XFS，跨頁框腳本攻擊)	當網站不存在XSS弱點時，藉由Javascript跨網域操作 iframe 的缺失。
B6 – 殘存備份檔或備份目錄	缺版本控管機制，將舊版備份檔以.BAK附檔名命名，而被視為一般檔案下載

二、5.測試階段



測試階段-納入安全需求(1/2)

- **機關於測試環境以工具檢測。**

- **在使用者驗證測試(UAT)是否納入資訊安全及SSDLC檢測：**
  - 透過設計階段所準備之資安測試個案進行驗測。
  - 經測試所有發現之問題均須修正。
  - 相關資安測試主要是由資訊單位負責進行。
  - 僅[4]案、[5]案有規劃相關資安測試個案。

使用者驗證測試-測試個案查驗表_SSDLC

SSDLC驗證報告

測試階段-納入安全需求(2/2)

[建議事項：]

- **使用者驗證測試(UAT)：**
  - 依據需求追溯表、SSDLC查檢表，按軟體安全需求相關之測試個案進行測試。
  - 測試所發現之問題單(含安全性問題)都全部解決後，使用者驗證測試才能通過。

- **於測試環境之資安測試：**
  - 廠商通過使用者驗證測試後，於測試環境進行源碼檢測、弱點掃描。
  - 由機關另行安排進行滲透測試。
  - 上線前於正式環境再次進行相關資訊安全檢測。

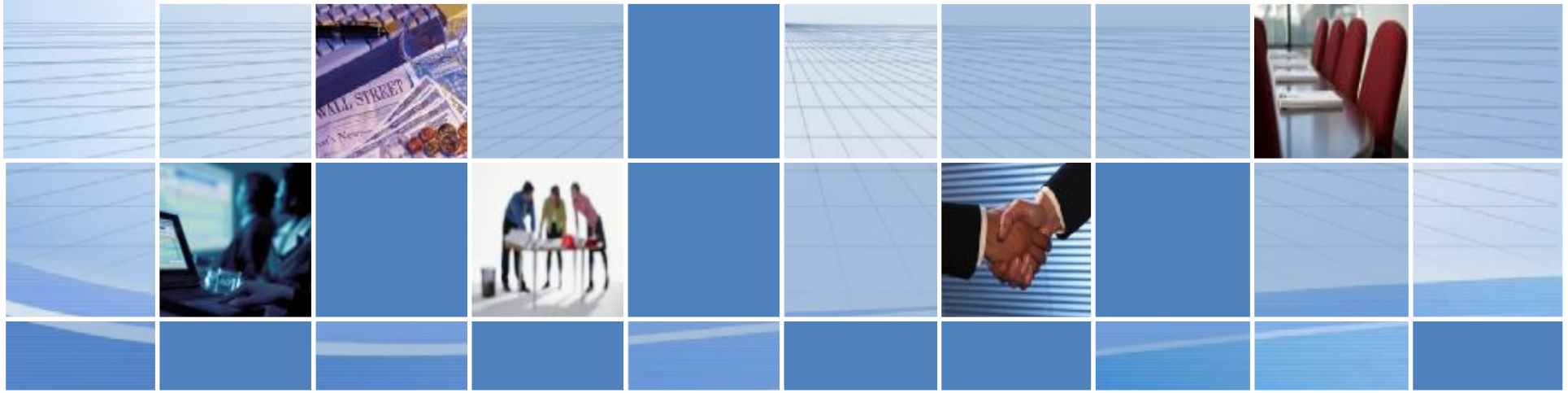
- **檢討執行專案所發現之資安議題：**
  - 測試過程，記錄所有與安全有關之bug。
  - 檢視：SSDLC相關規範、SSDLC查檢表，是否需調整。
  - 若須調整，更新後續專案RFP相關內容。

範例 – Issues Tracking System

以問題追蹤系統之「自定義標籤」功能，設定安全標籤，支援安全需求或安全問題的追蹤

科技部 Ministry of Science and Technology

二、6.佈署維運階段



強化組態設定-納入安全需求

- **強化安全的組態設定：(參考)**
  - 服務最小化：關閉不使用的服務、功能及port。
  - 作業系統進行安全分析與掃描，譬如：
    - Bastille - Hardening program (Linux/UNIX)
    - Microsoft Baseline Security Analyzer (MBSA)
  - 伺服器設定檔，譬如：
    - 安全限制
    - 認證方法
    - 錯誤處理頁面
    - Session Timeout時間
  - 常見組態問題，譬如：
    - 使用預設安裝軟體之預設密碼
    - 不應開放瀏覽目錄清單
    - 不當的錯誤處理組態設定
      (預設錯誤訊息頁面、顯示詳細Debug訊息)
    - 過高的系統權限
    - 不安全的SSL設定

元件定期更新-納入安全需求

- **元件定期更新：(參考)**
  - 第三方元件弱點，譬如：
    - 基礎元件：OpenSSL
    - 開放框架：Struts、Spring (Java)
    - 第三方套件：Apache Commons
    - 網頁伺服器：Apache, Apache Tomcat
    - 執行環境：Java Runtime Environment
    - 作業系統：Windows, UNIX / Linux
  - 第三方元件更新，譬如：
    - 注意Security Alert網站：
      - Microsoft Security Alert - http://technet.microsoft.com/zh-tw/security/dn530791
      - CVE (http://cve.mitre.org/cve/)
      - Bugtraq
      - http://www.us-cert.gov/ncas/alerts/
    - 訂閱廠商的安全通告
    - 定期檢視評估元件更新之必要性，重要服務應於測試環境評估完畢後再行更新。

三、建議與討論




建議與討論 (1/3)

- **評估面：**

  進行機關資訊系統安全等級評估。

- **目標面：**

  專案目標調整，如期、如質、如預算、如安全。

- **準備面：**

  除非列入RFP，廠商不見得會配合或有能力配合，或知道要配合什麼。

  - RFP問題：
    - 確認RFP相關資訊安全需求內容 (RFP 修訂)；資訊安全需求應加入SSDLC需求
    - 專案預算應含資訊安全執行預算
  - 執行問題：建立執行方法與步驟。
  - 廠商問題：慎選有經驗的廠商或有能力的廠商

建議與討論 (2/3)

- **執行面：**
  - 建立SSDLC檢核表
  - 執行步驟：安全需求追溯 -> 確認安全需求 ->確認廠商架構設計 ->測試個案與驗證 ->工具掃描 (源碼檢測 -> 弱點掃描 ->滲透測試)
  - 督促廠商系統架構師，進行架構安全設計與開發規範、程式範例確立。
  - 開發過程要求廠商定期進行源碼檢測，即時修正；在專案會議報告。
  - 不同的源碼檢測與弱掃工具，結果可能不同；可考量兩種工具搭配。
  - 機關宜在專案結案前進行滲透測試。(或委請專業第三方進行)
- **廠商(督促)面：**
  - 確認廠商已準備好。
  - 廠商應預先進行程式架構檢核，底層框架與安全設計檢視。
  - 廠商應預先進行程式規範與程式範本的建立。
  - 第三方元件使用，應預先檢核。
  - 使用合格與驗證過的掃描工具，經機關確認。
  - 建立程式自動檢核與測試平台機制。

建議與討論 (3/3)

- **規劃階段：**
  - 請廠商將SSDLC軟體安全需求列入計畫書內容
- **需求階段：**
  - 萃取並追蹤安全需求 (軟體安全需求查檢表)
- **設計階段：**
  - 系統內外部安全控管 (架構設計)
- **開發階段：**
  - 發展控制措施
  - 避免常見弱點 (源碼檢測、弱點掃描報告等)
- **測試階段：**
  - 安全測試 (源碼檢測、弱點掃描、滲透測試等)
  - 驗證安全需求 (測試個案及測試結果)
- **佈署維運階段：**
  - 組態強化
  - 元件更新 (定期更新)

簡報完畢
敬請指教