

資安星際指南

資安制度全攻略



— 前言 —

讓制度成為引路的光 走向穩定與安全

對許多中小企業或非營利組織而言，嚴謹的資安制度常被視為工作效率的絆腳石，因此在人力有限的團隊中，「默契」往往成了最直覺的行事準則。雖然團隊成員憑經驗也能把事情完成，但隨著時間累積、人員異動，甚至組織規模擴大，責任不清或標準不一致的問題便會逐漸浮現。

或許我們能換個角度思考：是否存在一套制度，既能守護資通安全，又能成為提升效率的助力？

當制度設計得宜，不僅不會成為日常工作的負擔，反而能減少不確定性、帶來安心，幫助組織在穩定中走得更快、更遠。這本《資安星際指南：資安制度全攻略》將透過情境與實務案例，引導您把管理思維從繁瑣轉化為清晰，並找到一條安心可循的路徑。 ▽



國家資通安全研究院
National Institute of Cyber Security

本手冊會帶您認識以下主題

- ① 為什麼需要資安政策與制度？
- ② 如何盤點資訊資產、分析價值並計算出風險值？
- ③ 制度可以透過什麼方式，落實在日常工作中？
- ④ 自我檢驗、桌上推演與 BCP 可以怎麼協助組織測試制度的有效性？
- ⑤ 若發現制度出現問題，該如何修正及持續改善？

資安制度常被視為冰冷的規範，但當它融入日常工作中，便能成為支撐組織長久穩定運作的基礎。而要踏上這條路，首要任務是識別出與組織相關的利害關係者；滿足利害關係者的需求與期望，是組織確保未來可以持續發展的關鍵。

從利害關係者的需求與期望出發，達到政策有依據、制度規畫有方向，不只是在作業效率與品質上思考如何「把事情做對」，更是在策略層級關注是否在「做對的事」，避免有限的資源浪費在錯誤的方向上。



本書主角



龜龜

海湧觀光管理局的新進助理，個性熱血、積極，但偶爾迷糊出包。剛接觸資安世界，努力學習中！

海豬仔

冷靜聰明的白海豚，在海湧觀光管理局擔任資安管理師，負責系統設計與風險分析，是後輩們最信賴的靠山。

使用指南

🗨️ **故事劇情：**和海豬仔與龜龜深入資安情境題，破解各式挑戰

★ **資安知識：**快速掌握防禦重點，並可留意 📌 小提醒的秘訣

✍️ **龜龜筆記本：**以清單快速確認自身與組織的資安完備狀態

前言

讓制度成為引路的光，走向穩定與安全

Chapter1

1 守護從這裡開始——建立願景與資安政策

關鍵字 資安政策、ISMS、PDCA

新進人員龜龜原本以為，只要把電腦設備顧好就算完成任務，沒想到光是「誰能看資料？」、「備份怎麼做？」這些問題，就讓他焦頭爛額。

Chapter2

9 築起防護根基——資訊資產的總盤點

關鍵字 資訊資產、資產價值、盤點清冊

龜龜在檔案室，發現遊客的個資、舊硬碟與研究報告，全都混在一起，誰能存取也不清楚。他焦急地問：「要怎麼知道哪些東西最重要？」

Chapter3

16 從盤點到應變——風險評鑑與制度落實

關鍵字 風險評鑑、四階文件、程序書

某天，龜龜收到遊客的投訴：「照片下載頁面怎麼變成奇怪的廣告？」原來是同事忘了更新外掛程式，讓駭客有機可乘。

Chapter4

27 多管齊查——模擬各種風浪考驗防線

關鍵字 內部稽核、成效追蹤、BCP、桌上推演

查核日到了，龜龜自信滿滿，拿著漂亮的紀錄表格向海豬仔報告：「我們都有做啊！」沒想到海豬仔卻拋出問題：「如果今天星球全斷網，還能繼續營運嗎？」

Chapter5

37 調整再出航——修正並迎向下個挑戰

關鍵字 問題回溯、流程修訂、持續改善

桌上推演結束後，龜龜鬆了一大口氣，慶幸這只是一場模擬演練。他跟海豬仔將問題逐條記下，準備展開後續的修正與強化。

附錄

海豬仔的百寶箱

結語

制度落地，星球穩行

Chapter 1

守護從這裡開始—— 建立願景與資安政策

關鍵字 資安政策、ISMS、PDCA

海湧觀光星球是宇宙間頗負盛名的觀光聖地。官方網站作為各項服務的核心平台，遊客會透過它預約潛水活動、選購特色商品，甚至上傳自拍照與美食評論。

這些互動不僅留下無數珍貴回憶，也讓遊客之間建立起熱鬧的交流氛圍。然而，對海湧觀光管理局來說，歡樂背後潛藏的卻是龐大的個資與金流風險；一旦資料外洩，後果不堪設想。

一個炎熱的中午，海湧觀光管理局的資訊處緊急發出了一則威脅通報訊息：「偵測到多起來自境外的異常登入嘗試，目標直指本局官方網站後台，請各單位立即提高警戒！」消息一出，整個辦公室頓時陷入兵荒馬亂，龜龜則是嚇得從座位上跳起來，心想：「怎麼辦？是不是因為我太常用公司網路逛網拍害系統中毒了？」

事後，局長找來海豬仔和龜龜：「大家不熟悉流程不是偶發狀況，是長期問題。這次的通報，很多人一開始都沒反應過來，甚至還有人沒收到，這顯示我們的資安制度還不成熟，得從根本解決。這個重責大任就交給你們了！」局長說完便匆匆離去，只留下一片緊繃的空氣。

從願景出發，形成政策與制度

龜龜一臉緊張地看向海豬仔：「怎麼辦呀學長？我們明明都有訂制度呀！可是照局長的意思，好像我們還是像一盤散沙一樣。」

海豬仔也嘆了口氣：「看來是時候做一個全面的檢視與修正了。我前幾天才剛去其他星球稽核，正好有一點心得，或許可以用它來試試看。」

「首先呢，我們要來釐清——資安管理有四個層次：願景、政策、目標與制度。制度不是孤立存在的，唯有了解這四個層次的關聯，才能讓制度真正落地運作。」



✦ 願景、政策、目標與制度的四層架構

	定位說明	案例
願景	長遠方向與理想狀態， 為所有行動的最高指引	<ul style="list-style-type: none"> 符合大眾的期待 建立安全可信賴的旅遊環境 確保旅客個資受到嚴密保護
政策	原則與方向，不涉及細節操作，可作為內部準則與外部承諾	<ul style="list-style-type: none"> 保護旅客個資 維持營運不中斷
目標	可衡量的資安指標，支援政策落實與持續改善	<ul style="list-style-type: none"> 提升資安防護成熟度 縮短事件處理時效
制度	工作規範，將政策具體化為操作細節與流程，確保能落地執行	<ul style="list-style-type: none"> 離職帳號三日內停用 資安事件兩小時內通報 系統更新，需經內部審核後上線

龜龜瞬間開竅：「之前都沒有調查過旅客最關心的事情是什麼，等於組織願景是我們空想出來的；政策也沒有跟願景扣合，制度還是針對個案分別訂立！導致這些制度一直都很零碎，沒有清楚的脈絡與章法。」

海豬仔同時打開了他的筆記本：「沒錯！一套正確的政策與制度，除了對內管理時，可以讓我們的運作更有秩序；對外也應該能展現我們的價值與責任，透過政策與制度，建立顧客與我們之間的信任關係。給你看看我的筆記。」

✦ 海豬仔的筆記

制度對內的效果

- ➔ **流程一致性**：不同部門能依循共同規範，不再各自為政
- ➔ **資訊可追溯**：保留每次異動紀錄，發生問題能快速找到根源
- ➔ **責任更清楚**：權限與角色劃分明確，避免互相推託
- ➔ **風險可控制**：降低人為操作差異所導致的失誤，強化組織運作的穩定

制度對外的價值

- ➔ **對客戶**：確保服務穩定與資料安全，建立信任感，讓對方願意長期使用或合作
- ➔ **對合作夥伴**：讓彼此在合作過程中能放心交換資訊或資源，降低協作風險
- ➔ **對主管機關或審查單位**：符合相關法規與標準，必要時能提供完整紀錄，避免違規或裁罰
- ➔ **對投資人或董事會**：展現組織治理能力，證明風險有被妥善控管，提升長期經營的信心

海豬仔說：「所以制度不只是內部規範，還是我們對外的安全保證，能不能回應這些來自外部的期待，是評量『願景』成功與否的關鍵。」

龜龜用力點頭：「我終於懂了，原來資安制度不只是技術問題，還事關整個組織共同的承諾跟形象！可是聽起來好複雜喔，要寫政策、訂制度，還得設計流程。真的有必要搞得這麼正式嗎？」

海豬仔突然回想起一段陳年往事：「記得以前我在另一家公司時，有位資深技術員突然離職。結果沒人知道主控系統的密碼怎麼重設，整個營運就這樣停擺了 3 個小時。」

「那時我們才意識到，關鍵工作依賴特定人員，且**沒有文件化、系統化及制度化的作業程序，是多麼危險的一件事**。一旦負責的人不在，整個公司就會陷入癱瘓的風險之中。」

「那學長，我們該怎麼開始建立有系統的制度呢？」

海豬仔回答道：「好問題！讓我們一起來看看什麼是 ISMS 跟 PDCA！」

資安制度的架構與循環：ISMS 與 PDCA

✧ 什麼是 ISMS ？

資通安全管理系統 (Information Security Management System, ISMS) 是一套可以幫助我們把願景、政策、目標、制度串連起來的框架。

它不是單一的技術工具，而是一整套依循國際標準（如 ISO 27001）所設計的管理體系，幫助組織建立一套有文件依據、可驗證、能持續改進的管理制度，確保資訊的**機密性、完整性與可用性**，都能被制度化地維護。

龜龜聽完後恍然大悟：「所以 ISMS 不是一個電腦系統，而是一種讓組織用制度來維護資安的方式？」

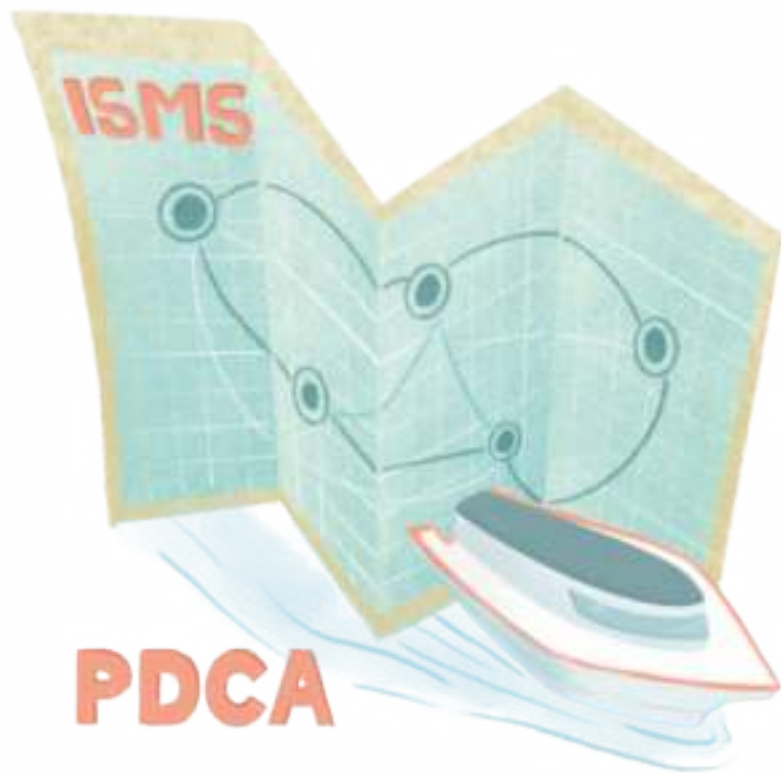
海豬仔笑著點頭：「沒錯，它就像一張星際航行地圖，把政策、規範和流程都標得清清楚楚，指引大家共同前行。」

✧ 什麼是 PDCA ？

PDCA 循環是一種持續改善的管理方法。透過 Plan（規劃）、Do（執行）、Check（檢查）、Act（改善）四個步驟，執行過程中不斷地檢視與修正，讓制度與流程能逐步貼近既定目標，並且確保制度不是一次性的措施，而是能隨組織環境變化長期演進的治理信念。

PDCA 循環在資安管理中的應用可以參考以下表格：

階段	任務	具體工作
Plan 規劃	擬定願景、政策、目標及制度	<ul style="list-style-type: none"> 制定資安政策 擬定資安目標 撰寫程序及制度文件
Do 執行	依照規劃落實制度	<ul style="list-style-type: none"> 資訊資產盤點與風險評鑑 建立帳號設定規範 執行異常通報 進行員工訓練
Check 檢查	檢視組織資安願景與目標是否達成，制度是否一致	<ul style="list-style-type: none"> 定期內部稽核 審查制度落實程度 考核內部教育訓練成效
Act 改善	根據結果修正流程並改善制度	<ul style="list-style-type: none"> 根據稽核結果調整規範 更新日常維運工具 簡化作業流程

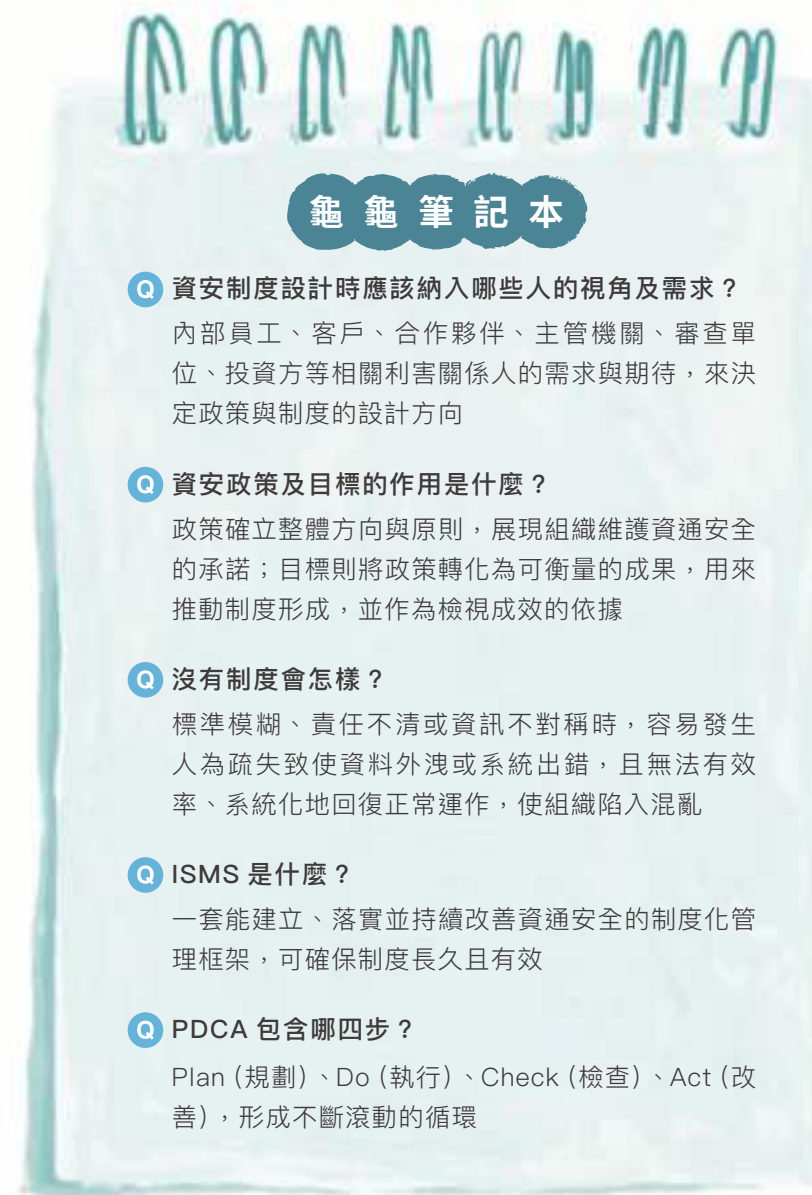


龜龜說：「我懂了，如果 ISMS 是地圖，那 **PDCA 就是在實踐 ISMS 時的導航輔助系統**。地圖能夠指引方向，但導航系統可以隨時偵測天候、修正航線，確保船隻在最佳航道上！」

海豬仔拍了拍龜龜：「ISMS 的核心理念，除了將作業流程標準化、文件化以外，更重要的是成員是否有將規範落實在每天的工作中。」

龜龜說：「所以我們下一步，應該是先釐清有哪些資訊資產、要面對哪些風險，才能規劃後續制度跟管理措施，對嗎？」

海豬仔很高興自己終於有個腦袋靈活的助理，他說：「很有概念喔！資安制度的第一步就是從盤點資產開始。走吧，我們去看看有什麼靈感！」



龜龜筆記本

- Q 資安制度設計時應該納入哪些人的視角及需求？**
內部員工、客戶、合作夥伴、主管機關、審查單位、投資方等相關利害關係人的需求與期待，來決定政策與制度的設計方向
- Q 資安政策及目標的作用是什麼？**
政策確立整體方向與原則，展現組織維護資通安全的承諾；目標則將政策轉化為可衡量的成果，用來推動制度形成，並作為檢視成效的依據
- Q 沒有制度會怎樣？**
標準模糊、責任不清或資訊不對稱時，容易發生人為疏失致使資料外洩或系統出錯，且無法有效率、系統化地回復正常運作，使組織陷入混亂
- Q ISMS 是什麼？**
一套能建立、落實並持續改善資通安全的制度化管理框架，可確保制度長久且有效
- Q PDCA 包含哪四步？**
Plan (規劃)、Do (執行)、Check (檢查)、Act (改善)，形成不斷滾動的循環

Chapter 2

築起防護根基—— 資訊資產的總盤點

關鍵字 資訊資產、資產價值、盤點清冊

海豬仔和龜龜開始在海湧觀光管理局裡四處巡視。

龜龜邊走邊數著：「電腦、攝影機、預約系統等，這些一定要保護吧？」

然而光是想到要把這些東西一一盤點並記錄下來，他就覺得頭暈目眩，忍不住大嘆一口氣：「唉！這麼多東西要顧，我根本不知道要從哪裡開始！」

海豬仔看向龜龜：「這還只是冰山一角呢，你可別這麼早就喊累。資訊資產的種類可不僅限於電子設備，我們得先把範圍看清楚，才知道自己要保護什麼。」



資產識別——資訊資產有哪些？

龜龜接著從口袋掏出一張小紙條：「我剛剛從前輩那邊問到的，你看，這些都是我們等等要盤點的**資訊資產類別**！原來不只人員，連個人資料也算資產？這對我們來說，到底有什麼價值呢？」

✦ 常見的資訊資產類別

- ☑ **文件**：公文、報表、紙本紀錄、表單、計畫書
- ☑ **軟體**：作業系統、應用程式、自行開發或委外的系統、租賃軟體
- ☑ **網通設備**：路由器、防火牆、AP 分享器、網路線路
- ☑ **硬體**：電腦、伺服器、印表機、監視器
- ☑ **資料**：個人資料、金流紀錄、研究數據、備份檔案
- ☑ **環境**：機房、電力、消防設備
- ☑ **人員**：管理維護這些系統、設備的負責人員及委外服務廠商

海豬仔耐心解釋：「資安所講的『資產』，不只是摸得到的硬體設備，而是**所有對組織有價值、或是需要守護的東西**。旅客的個人資料當然不是我們『擁有』的財產，但我們依賴這些資料來維持業務運作，依法也該對旅客的資料有保護的義務。」

海豬仔繼續補充：「所以啊，如果我們連自己擁有什麼都不清楚，就無法判斷每項資產的重要性，這就是為什麼第一步要做資產盤點。既然已經知道資產類別跟範圍了，就來看看各項資產的價值要怎麼計算吧。」

資產分級——重要性及價值計算

龜龜聽到計算兩個字，馬上縮回自己的龜殼裡：「不是只需要判斷哪些資產比較重要就好了嗎？為什麼還要計算呀？」

海豬仔又好氣又好笑地說：「如果公司人力與經費可以無上限支援資安工作，當然可以略過風險管理，但你覺得有可能嗎？而且資產是否重要，不是嘴巴說了就算數！**如果沒有一套標準或決策的方法，就無法判斷哪些資產最需要優先保護。**」

海豬仔接著安慰龜龜：「放心，接下來的步驟很簡單，只要問問自己這幾個問題，就能看出資產的價值！」

✦ 資產價值計算的四個指標

➔ 機密性 Confidentiality

這份資產是可以公開的嗎？如果不是的話，機密程度多高？

➔ 完整性 Integrity

這份資產如果被破壞或竄改，會對組織造成傷害，甚至造成業務終止嗎？

➔ 可用性 Availability

這份資產能容許失效或停擺的時間是多久？是 4 小時或一整天？

➔ 法遵性 Compliance

這份資產有受法律或規範要求嗎？如果違反是否會被罰款或損害名譽？

✦ 資產價值計分範例

	1 分	2 分	3 分
機密性	一般資料 可對外公開	敏感資料 僅限內部使用	機密資料 外洩會造成重大損害
完整性	完整性被破壞 不會對組織 造成傷害	完整性被破壞 會對組織造成傷害 但不至於太嚴重	完整性被破壞 會對組織造成傷害 甚至使業務終止
可用性	資產可容許 中斷 3 天以上	資產可容許 中斷 8 小時至 3 天	資產僅容許 中斷 8 小時以內
法遵性	未受法律 或規範限制	有內部規範 或業界慣例 無法律罰則	受法律規範要求 違反有罰則 或聲譽損害

海豬仔補充說：「最後，資產價值的計算方式有兩種可以參考。」

➔ **總合法**：把四個指標加總，得到一個完整分數。這樣能反映多方面的特性，但有時會淡化高分項目的重要性。

➔ **最大值法**：取四個指標裡的最高分作為資產價值。能凸顯最危險的那一項，避免關鍵價值被忽略，但容易低估其他指標的分數、忽略整體分數組合。

他眨了眨眼：「不論用哪一種算法，只要能清楚呈現資產之間的價值差異，幫助組織衡量哪些資產更關鍵，就能依此給它們不同的保護措施！」

資訊資產盤點清冊

龜龜看著手上的筆記本：「所以，我們已經識別完所有資產，也打好資產價值分數了，把分數寫在便條紙，貼在那項資產上就好了吧？」

海豬仔回答：「接下來我們要把所有分數整合在**資訊資產盤點清冊**上。清冊的目的就是把剛剛識別到的資產，連同它們的價值評估分數，一併整理在同份文件，形成一份可管理的清單。來吧，現在就由你動筆，寫出我們的第一份盤點清冊！」

他指著表格上的幾個欄位，耐心說明：

☑ **資產名稱**：寫清楚哪個資產，如「活動網站」、「個人電腦」等

☑ **資產類別**：屬於文件、硬體、軟體、資料、人員等等

☑ **所在位置**：實體位置如「機房 A 區」，或系統位置、路徑
例如「:\fileserver\2025」

☑ **權責單位及負責人**：誰要對這個資產負維護管理責任

☑ **各項指標分數及最終資產價值**：機密性、完整性、可用性及法遵性個別分數及最終評估的資產價值

海豬仔看著龜龜寫好的清冊，語氣嚴肅起來：「別以為盤點到這裡就能收工了喔！資產盤點只是第一步，真正的挑戰才正要開始。」

★ R-AM-001 資訊資產盤點清冊

盤點者：龜龜

序	資產名稱	資產類型	所在位置	權責單位及負責人	機密性	完整性	可用性	法遵性	資產價值
1	Microsoft Office 2019	軟體 _ 套裝軟體 或作業系統	DB_Cluster_Prod_A 雲端資料庫 A 區	資訊處 / 老螺	1	2	2	1	6
2	活動官方網站	軟體 _ 應用系統	AWS EC2 —ap-northeast-1	資訊處 / 魷姐	2	3	3	2	10
3	公務筆電	硬體 _ 實體設備	辦公室 2F	資訊處 / 海豬仔	2	2	2	2	8
4	財務報表	資料 _ 電子	\fileserver \Finance\2025	財會部 / 魷哥	3	3	2	3	11
5	帝雉手工餅乾合作契約	資料 _ 紙本	辦公室 1F	資訊處 / 龜龜	2	2	1	2	7

** 總合法



龜龜筆記本

Q 什麼是資訊資產？

所有對業務有價值或需保護的標的，包含：文件、資料、軟體、硬體、環境、人員、個資等等

Q 為什麼要評估資產價值？

資產價值的高低會影響風險排序，評估資產價值可以幫助判斷哪些東西最重要、需要優先投入資源及保護

Q 怎麼評估？

可參考常用的四個指標：機密性、完整性、可用性、法遵性，計算方法採總合法或最大值法計分皆可

Q 資產盤點清冊要包含什麼？

需包含資產名稱、類型、所在位置、權責單位 / 負責人、四個指標分數、最終資產價值等資訊

「知道有哪些資產、價值多高，只是幫我們建立資產全貌。但要保護得當，我們還得更進一步計算這些資產可能面臨的風險值，如此才能判斷後續該怎麼保護、怎麼分配資源，以及什麼時候要調整。」

龜龜緊張地問：「風險值？那要怎麼算？該不會又是數學題？」

海豬仔笑著說：「別怕，對你來說也是小菜一碟而已。下一步我們來看看風險評鑑該怎麼做吧！」

Chapter 3 從盤點到應變—— 風險評鑑與制度落實

關鍵字 風險評鑑、四階文件、程序書

海豬仔指著白板說：「在風險評鑑的工作中，除了剛剛已經算好的**資產價值**之外，還有兩個必須一起考慮的數字：**威脅等級**和**脆弱性等級**。常見是將這三個數字相乘，得出最後的風險值。」

龜龜皺著眉頭：「咦？為什麼這麼麻煩？不能直接把資產價值當作風險值就好嗎？」

海豬仔耐心解釋：「**因為資產的價值不等於資產的風險。**」



盤點之後的風險評鑑作業

「即便是高價值資產，如果不太可能遭遇威脅，或是本身的防護很完善，那風險不會真的那麼高；換句話說，中等價值的資產，如果每天都被駭客虎視眈眈地盯著，時刻暴露在危險中，且軟體還使用未更新的老舊版本，那風險就會非常高。所以，我們必須同時考量三個面向。」

- ☑ **資產價值**：這個資產有多重要？
若發生資安事件，對組織的衝擊程度？
- ☑ **威脅等級**：外部危害發生的可能性？
- ☑ **脆弱性等級**：資產的防護狀態與被利用的容易程度？

威脅等級 Threat Level

說明

舉例

1分
低風險

幾乎不會發生
或發生頻率極低

- 當地罕見的自然災害
- 極少見的攻擊手法
- 平均 1 至 5 年發生 1 次或從未發生過

2分
中等風險

偶爾會發生
存在一定的可能性

- 設備偶爾故障
- 常見釣魚郵件
- 每年發生 1 次以上

3分
高風險

經常發生
可能性極高

- 地區常有淹水停電
- 未授權的掃描頻率高
- 每季發生 1 次以上



風險值公式：風險值 = 資產價值 × 威脅等級 × 脆弱性等級

以龜龜先前盤點的公務筆電為範例：

- ☑ **資產價值**：8 分——屬法務部門所有，且會用來操作技術專利管理系統，為日常作業必需品
- ☑ **威脅等級**：2 分——偶爾會遇到釣魚郵件、外出攜帶有遺失風險
- ☑ **脆弱性等級**：2 分——已設密碼並加密，但員工偶爾延遲更新系統

將三個面向的積分依公式相乘，風險值就是： $8 \times 2 \times 2 = 32$ 分

脆弱性等級 Vulnerability Level

說明

舉例

1分
低風險

幾乎沒有可被利用的弱點
已有完善防護

- 系統及時更新
- 權限嚴格
- 異地備份完整

2分
中等風險

存在部分弱點
可能被利用但有部分保護

- 系統部分漏洞未修補
- 員工訓練不足

3分
高風險

弱點明顯
容易被利用，缺乏防護措施

- 預設密碼未更改
- 沒有備份
- 監控不足

龜龜算完數字，驚呼：「哇，竟然有 32 分！那是不是代表我馬上要把筆電鎖進保險箱？」

海豬仔忍不住笑了：「先別急著嚇自己。風險評鑑的目的，不是要我們什麼都害怕，而是要判斷**哪些風險需要處理、該怎麼處理、處理的優先順序**。帶你看看風險處置常見的四種做法。」

✧ 風險處置的四種做法

定義	範例
降低 Mitigate 減少風險發生的機會或衝擊 加密、權限控管、異地備援	
避免 Avoid 停止會帶來高風險的活動 停用不安全的舊系統	
轉移 Transfer 把風險轉給第三方 買保險、維運委外處理	
接受 Accept 在可承受範圍內選擇接受 承擔小額損失	

龜龜恍然大悟：「原來重點不在害怕，而是在選擇合適的方式，把風險控制在能接受的範圍內。」

海豬仔收起白板：「所以你看，盤點只是個起點，接下來還要一步步往下走。從資產識別盤點、價值計算、分級到評估風險，後續還要依組織經費與人力等資源，規劃控管措施、分配預算和人力，每年都還要回頭檢查，隨著環境變化去調整風險值分數。」

龜龜眨眨眼：「原來清冊只是開始，後續還有那麼多功課要做啊！」

海豬仔點頭笑道：「沒錯，要讓制度真正落實，就得把這些做法寫進程序書裡。清冊只是提供了制度運作的根據，而風險的變化則提醒我們，制度也要跟著修正。」

制度的起點：文件化

海豬仔收起白板筆，指著桌上的一疊資料夾：「光是會算風險還不夠喔。如果大家各寫各的筆記，最後一定亂成一團，誰也看不懂別人在做什麼。」

他接著說：「ISMS 的精神，不只是在盤點資產和評估風險，還要把制度文件化，並依架構分成四個層級。」

✧ 四階文件

功能定位	範例
第一階文件 政策性宣言 ，說明 ISMS 的目標、方向與執行原則	ISMS-01-001 資通安全政策
第二階文件 程序書 ，制定各類管理與控制程序，作為各類作業執行的指導	ISMS-02-003 營運持續管理程序書
第三階文件 作業說明、指引、辦法 ，針對具體領域詳細描述作業方式與規範	ISMS-03-007 備份管理作業說明書
第四階文件 表單或紀錄 ，保存執行成果與證據，作為查核依據	03-015-01 備份磁帶異地存放紀錄表

龜龜撓撓頭：「我們不是已經有清冊了嗎？為什麼還要分層？」

海豬仔說：「分層最大的好處，就是能讓文件架構分明、確保新舊人員都能一致遵循，萬一出問題也能沿著紀錄往上追溯到源頭。」

「原來如此！所以清冊只是起點，文件分層才是讓制度真正站穩的方法！」

海豬仔點點頭：「在 ISMS 的四階文件架構裡，程序書就是第二階文件。政策已經定下了方向，但要讓規範能被真正執行，就得靠程序書把流程、角色、責任，以及該流程應產出的結果、紀錄清楚敘明。」

制度的落實：程序書

正當大家以為一切都步上軌道時，某個週末深夜，官網突然響起異常警報。管理局隨即接到投訴：「官網下載活動照片的頁面怎麼變成廣告？還有人說電腦被植入病毒！」

龜龜嚇得臉色發白：「糟了！難道我們真的被駭客入侵了嗎？」

海豬仔立刻登入後台檢查，他說：「原來是網站的一個外掛程式漏洞被利用了。按照程序書，這個外掛應該每個月更新一次，但負責的同仁上個月太忙忘了更新，讓駭客有機可乘，在下載頁面偷偷塞入惡意連結。」

他嚴肅地說：「這就是制度沒有落實的後果。程序書寫得再完整，如果沒人照做，風險還是會爆發。這次只是頁面被竄改，要是捐款金流被動手腳，後果可就不是嚇一跳這麼簡單了。」

✧ 程序書是什麼？

程序書與作業規範主要功能在於**確保制度可操作化與一致性**，使組織內不同人員在相同情境下，能依照同一套標準流程執行，降低依賴個人經驗或記憶，並避免作業結果因人而異。程序書的內容通常包含：

- ➔ 執行方式：業務要求與流程
- ➔ 責任角色：由誰負責、誰審核、誰執行
- ➔ 時機要求：何時啟動、多久檢查一次
- ➔ 驗證標準：產出什麼成果或條件才算完成

✧ 什麼時候會用到程序書？

情境	為什麼需要程序書？
員工離職後帳號須停用	確保交接完整，帳號停用有依循步驟，不會遺漏
活動前要備份網站資料	建立固定流程，讓備份成為例行公事，避免憑記憶行事
接到可疑 Email 要通報	提供明確通報管道與流程，縮短反應時間、即時阻擋攻擊

海豬仔說：「**程序書看似簡單好寫，但還是有幾點核心原則是需要遵守的**。第一，要把誰負責講清楚；第二，要讓流程標準化，大家照同一套做事才不會亂；最後，就是要針對正常運作、異常警示、緊急狀況等，設計不同層級的應變措施。」

✧ 程序書內容範例：

情境	指令流程	負責角色	時間要求
● 正常運作	系統每日備份 → 安全日誌記錄 → 稽核報告	系統管理員 老螺	每日例行 任務
● 異常警示	偵測異常登入 → 通報主管 → 啟動調查程序	資訊人員 魷姐	30 分鐘 以內回應
● 緊急狀況	資料外洩 → 啟動應變小組 → 暫停外部連線	應變指揮官 海豬仔	立即執行

幾週後，海湧觀光星球的資安制度已有初步成果，不僅訂定了資訊資產管理程序、風險評鑑與處理方法，連其他運作相關程序書初稿也差不多就緒了。

海豬仔拍拍龜龜的肩膀說：「看在你最近這麼辛苦的份上，晚點請你吃海藻飯糰吧。但制度寫出來只是第一步，真正的挑戰是讓它們變成大家的日常工作。」

資安危機的救星——通報應變流程

龜龜一邊吃著海豬仔買回來的海藻飯糰、一邊反省：「上次官網被駭時，我們根本沒有一套完整的事件通報流程，難怪大家會亂成一團！」

於是，他決定趁著記憶猶新，起草一份**資安事件應變程序書**。

	目標	行動	案例
1 通報	第一時間 掌握狀況	<ul style="list-style-type: none">通知主管與資安人員建立事件紀錄	週六 20:45，遊客服務中心回報：照片下載頁面被竄改投放廣告，影響約 200 人
2 隔離	阻止 事件擴大	<ul style="list-style-type: none">關閉受影響系統封鎖可疑 IP暫停外掛服務	立即關閉照片下載功能，避免更多遊客受害
3 調查	找出破口 與影響範圍	<ul style="list-style-type: none">檢查日誌比對異動確認外洩情況	發現外掛程式未更新，駭客利用漏洞植入惡意連結
4 修補	漏洞修補 清除威脅 恢復服務	<ul style="list-style-type: none">安裝更新清除惡意程式建立監控通知使用者	更新外掛，移除惡意碼，寄送信件給 200 位遊客，告知發生資安事件並提醒留意
5 回報	總結與 改進制度	<ul style="list-style-type: none">撰寫報告提出改善建議調整流程	事件報告： 原因是未落實程序書，未確實更新系統 改進措施： 建立自動更新排程、交叉覆核

【海湧觀光星球資安事件處理流程】

① 發現異常

看到可疑狀況（如網站跳轉、系統異常、帳號異動、釣魚信）
不要自行處理！

💡 例如：龜龜發現照片下載頁面被竄改成其他資訊。

② 立即通報

馬上透過指定管道（內部系統報告表單 / 資安專線 / 緊急群組）通知主管與資安人員。

💡 記得提供：時間、地點、狀況描述、受影響範圍。

③ 隔離現場

在等待資安人員接手前，先阻止進一步損害。

💡 例如：暫停受影響系統、斷線可疑設備、提醒同仁先別使用。

④ 配合調查

保存證據，不要刪檔案或清除紀錄。

💡 工程師會查看日誌、備份資料，確認問題來源。

⑤ 修補漏洞

由技術團隊安裝更新、修補問題、恢復服務。

💡 必要時發出對外通知，提醒用戶防範。

⑥ 回報與改善

資安人員撰寫事件報告，提出改善措施。

💡 例如：建立自動更新排程、安排加強教育訓練。

龜龜筆記本

Q 盤點清冊完成後還要做什麼？

- 評估資產風險
- 制定相應的控管措施
- 考量資源怎麼分配投入保護
- 持續檢視並修正

Q 面對風險有哪四種處理作法？

降低、避免、轉移、接受

Q 程序書與應變流程的價值是什麼？

危機發生時，有清楚依循的步驟，避免手忙腳亂

Q 為什麼制度一定要落實？

有程序書卻未確實執行，一樣可能導致資安事件

海豬仔看著龜龜主動發現、解決問題，心裡感到很驕傲，但他不改嚴肅形象地對龜龜說：「程序書不是寫完就可以一勞永逸，必須隨著環境和需求調整，才能真正發揮保護作用。當發生資安事件，就是檢驗制度是否真的有效的最好時機。」

Chapter 4

多管齊查—— 模擬各種風浪考驗防線

關鍵字 內部稽核、成效追蹤、BCP、桌上推演

龜龜躺在甲板上，仰望著星空，滿臉自豪地對海豬仔說：「經過這幾個月，我們的資安制度都落實了耶！大家都有專屬帳號、系統更新也有人在做，還有備份流程。我覺得我們的防線已經沒問題了！」

海豬仔卻沒有馬上回話，只是拿起一張舊照片，照片裡是他以前買下的一艘漂亮遊艇，在出港前看起來狀態完美，卻因為沒檢查到船底的小裂縫，最後在風浪中沉沒了。

「龜龜，你知道嗎？很多災難不是因為沒有制度，而是因為**我們以為有制度就夠了，卻忘了確認它們是不是真的有發揮作用**，也常常忘了在執行之餘，順手留下紀錄。」

龜龜愣了一下，慢慢坐起來：「那該怎麼辦？還是我們來做沙盤推演！」

海豬仔點頭：「沒錯，我們需要模擬各種風浪，看防線能不能撐得住。這樣，等真正的駭客來襲或系統故障時，我們才不會手忙腳亂。」

日常制度落實——從紀錄開始！

某天，龜龜在整理檔案時，發現一大疊「系統更新日誌」和「備份紀錄表」。他趕緊跑去找海豬仔：「為什麼要留這麼多紀錄？這些不能丟掉嗎？」

海豬仔翻開其中一份備份紀錄，上面寫著：114 年 9 月 23 日 / 自動備份完成並還原測試成功。

他向龜龜解釋道：「你看，這些你看不順眼的雜亂表單，就是制度落實的證據。制度不是寫在紙上就算了，還需要透過紀錄來證明它真的有被執行！」

龜龜恍然大悟：「對耶，有保留記錄才能溯源，也才有回頭比對跟修正的機會！」

海豬仔點點頭：「沒錯。**紀錄就是制度的生命軌跡**，沒有紀錄，制度就只是紙上的規則；有了紀錄，才能證明它確實在日常運作中發揮作用。」



✧ 從紀錄檢視制度是否被落實

制度	紀錄	能證明什麼
帳號管理	<ul style="list-style-type: none"> 新增 / 刪除帳號申請單 權限變更紀錄 	一人一帳號，且權限各異
系統更新	<ul style="list-style-type: none"> 更新日誌 更新安裝紀錄 	系統有依循規定定期更新
資料備份	<ul style="list-style-type: none"> 備份報告 還原測試紀錄 	資料有備份並能成功復原

✧ 紀錄文件保存要點

海豬仔接著強調：「**文件與紀錄的保存，不只是為了方便日後查找，更是內部稽核的基礎**。檔案一旦遺失、混淆或無法追溯，就等於失去證據，無法確認制度是否被正確執行。因此，紀錄保存需要遵循四個重點。」

- ➔ **統一命名**：用「事件類型－日期－編號」的規則，方便追查
- ➔ **集中管理**：放在專屬資料夾，並設好存取權限
- ➔ **版本控管**：每次修改都保留舊版本與修改原因
- ➔ **留存期限**：至少保存一年（或法規要求之期限），到期前必須經審查才能刪除或歸檔

✧ 為什麼要自我檢驗？

「就像船要定期檢查船體、測試防水，我們的制度也要定期驗證，才能確保在真正需要的時候發揮作用。」海豬仔說。

龜龜說：「喔！我知道！是類似資安制度的健康檢查嗎？」

海豬仔打開他的小手冊：「沒錯！我嘗試過四種內部驗證的工具，從日常遵循到災難演練都包含在內，讓我來跟你好好聊聊。」

驗證方式	說明	範例
內部稽核	定期檢查資安政策、制度是否被遵守	<ul style="list-style-type: none"> 檢查是否有人共用帳號 備份紀錄是否完整
成效追蹤	檢視制度的執行成果是否符合預期	<ul style="list-style-type: none"> 釣魚信測驗通過率是否提高 通報速度是否縮短
BCP 檢核	確認在災難情境之下，核心業務能否持續運作	<ul style="list-style-type: none"> 模擬資料中心後，備援系統啟動時間是否達標
演練測試	模擬資安事件驗證應變流程的有效性	<ul style="list-style-type: none"> 模擬釣魚信事件 聯合不同部門舉辦桌上推演

營運持續計畫 BCP：確保危機中的穩定運作

某天，海豬仔帶著龜龜到會議室，桌上放著厚厚一疊稽核報告。

龜龜得意地說：「看，我們所有平時檢查紀錄都很漂亮！帳號有人管、備份也都有、教育訓練有紀錄，是不是代表我們可以安心了？」

海豬仔卻搖搖頭：「這些紀錄只能證明平時大家有照做，但災難發生時，能不能真的活下來，是另一回事。**假設今天星球所有網路斷線，你能撐多久？**」

龜龜嚇得直瞪眼：「哇！如果真的全斷網，我們的官網、預約、捐款都不能用了，那我們要怎麼辦？」

海豬仔說：「這就是為什麼要做演練，測試『災難來臨時，制度是否真的有用』。這種演練的核心，就是 **BCP**。」

✧ BCP 是什麼？

BCP (Business Continuity Plan, 營運持續計畫) 就是一套「當災難發生時，組織如何維持基本運作」的計畫。它不只檢查平時有沒有備份，更要能回應各種可能發生的危機事件，例如：

- ➡ 如果網路斷線，備援系統是否可自動切換？
- ➡ 資料毀損後，能在數小時內還原嗎？
- ➡ 金流中斷時，怎麼啟動人工機制以維持營運？
- ➡ 當遊客大排長龍時，誰負責對外溝通與發布訊息？

✧ 平時查核與 BCP 比較

檢查面向	平時查核重點	BCP 重點
資料備份	<ul style="list-style-type: none"> 備份是否完整？ 排程是否有跑？ 	系統能不能在故障 2 小時內還原備份資料？
系統運作	<ul style="list-style-type: none"> 系統是否按時更新？ 是否有備援機制？ 	系統突然故障時，有沒有異地備援？
教育訓練	<ul style="list-style-type: none"> 員工是否接受過訓練並通過測驗？ 	員工是否能在模擬事件中正確判定事件並通報？
對外溝通	<ul style="list-style-type: none"> 是否有公告草稿？ 公告的發布有無依據程序進行？ 	發生重大事故時，公關能否在 30 分鐘內發布新聞稿或公告於官網？

龜龜看著表格，吞了口口水：「原來不能只靠漂亮的日常紀錄，還要真槍實彈演練過，才知道危機來時能不能撐得住！」

海豬仔點點頭：「沒錯，**平時的檢查是基礎，但 BCP 的演練才是保命的關鍵。**」

桌上推演：模擬挑戰，驗證營運不中斷

為驗證 BCP 是否實用，海豬仔發起了第一次「模擬斷網日」。

「今天起，我們來做桌上推演，假設我們不幸發生資安事件，整個公司沒有網路、系統跟資料庫無法使用，在這樣的條件下來接待一日遊遊客！」

龜龜問：「桌上推演是什麼？」

海豬仔解釋：「**桌上推演 (Tabletop Exercise)** 是一種模擬演練，透過討論和假設情境，來驗證組織在面對突發事件時是否有清楚的應變流程與分工。它不需要真的中斷服務或造成損害，而是讓各單位成員在安全的環境下『演練思考』，當遇到資安事件或營運中斷時，大家能否照著計畫行動、找到問題並加以改進。」

「就像防災逃生演習，不是真的失火，但大家要知道出口在哪、誰帶人疏散、醫療包在哪。」

螢幕上跳出模擬情境：

- ➔ 官網、預約系統、捐款平台全面停擺
- ➔ 系統與資料庫無法連線
- ➔ 門口排滿遊客，要求退票或改期
- ➔ 合作的非營利組織研究報告無法即時上傳
- ➔ 財務金流暫停，捐款收不到

現場頓時七嘴八舌，開啟了各部門的演練對話：



行政部門

遊客大排長龍，我們要怎麼解釋？要不要印一份『系統暫停服務公告』貼在入口？



公關部門

媒體記者已經在外面等著，我們有沒有新聞稿範本？



資訊部門

若伺服器全斷，要不要立刻切換到異地備援系統？上次備份是什麼時候？



財務部門

捐款系統停擺了，要不要緊急開人工收單？

龜龜再次確認了文件後，驚訝的發現：「我們的 BCP 檢查表上，好像沒有寫到『人工收單』耶。」

海豬仔立刻指出：「很好，這就是桌推的價值——讓我們提前發現制度的缺口，讓我們模擬流程步驟，並將發現的問題記錄下來。」

桌上推演問題紀錄與改善方針

行政部門 如何安撫遊客？	目前狀況	口頭解釋不夠一致
	改進需求	制定標準公告模板
公關部門 如何對媒體說明？	目前狀況	有新聞稿草稿但未定稿
	改進需求	建立多版本公告模板，如：系統異常公告、資料外洩公告
資訊部門 是否有備援系統？	目前狀況	尚未建立異地備援
	改進需求	需建置異地機房或雲端備援
財務部門 如果捐款系統停擺怎麼辦？	目前狀況	沒有人工收單流程
	改進需求	制定人工收單 SOP
全體員工 是否每人都清楚知道通報窗口？	目前狀況	部分人不清楚
	改進需求	強化教育訓練，張貼通報流程海報

演練結束後，龜龜總算鬆了一口氣，他邊擦汗邊說：「還好這次只是模擬，要是真的全斷網，我一定慌到不會動。」

海豬仔拍拍牠的背：「這就是桌上推演的意義。平時查核是檢查制度有沒有做，桌上推演則是驗證災難來時能不能撐住。」

龜龜點點頭，把「人工收單 SOP」、「公告範本」及「異地備援」寫進筆記本。心想：希望自己下次能更快做出正確的反應。

龜龜筆記本

Q 為什麼要做查核？

制度寫了、也有人在做，但不查核就不知道是否真的有效

Q 日常制度成效怎麼查？

靠紀錄來證明，例如：帳號異動紀錄、備份日誌、還原測試結果。沒有紀錄就無法追蹤

Q 什麼是 BCP？

營運持續計畫，確保重大災難（斷網、系統故障）時，組織仍能維持基本運作

Q 為什麼要做桌上推演？

透過模擬資安事件發生可能對組織帶來的影響，驗證制度是否真的能運作，桌上推演可以幫助組織發現目前制度沒寫到的地方

Q 查核的最終目的是什麼？

找出漏洞並改善，而不是挑錯或咎責

海豬仔總結：「做完是第一步，確認做對、做足才是重點；下一步就該根據這些數據和演練結果，回過頭來修正制度，讓 PDCA 循環真正跑起來。」

👉 第五章：調整再出航——修正並迎向下個挑戰

Chapter 5

調整再出航 —— 修正並迎向下個挑戰

關鍵字 問題回溯、流程修訂、持續改善

在完成各項定期檢查與模擬桌推後，龜龜筋疲力盡地癱軟在辦公桌上。

「我們上次桌上推演後，不是已經更新公告範本了嗎？怎麼我在共用資料夾還是找不到？」海豬仔點開了無數個資料夾視窗，語氣帶著不耐煩。

龜龜不好意思地說：「啊，那份文件我上次改完，好像忘了同步上傳。」

海豬仔搖搖頭：「制度的改善不是改好一份文件就好，重點是要讓大家知道改了什麼，這才能真正落實修正呀！」

他想了想後，接著說：「不過發現問題是好事，看來我們需要建立『制度修正紀錄表』，記下每次變更的內容、修改人、日期與原因，還要統一命名方式，像『公告範本_v3_20250909』，讓大家一眼就可以掌握最新版本。」



重新檢視查核結果

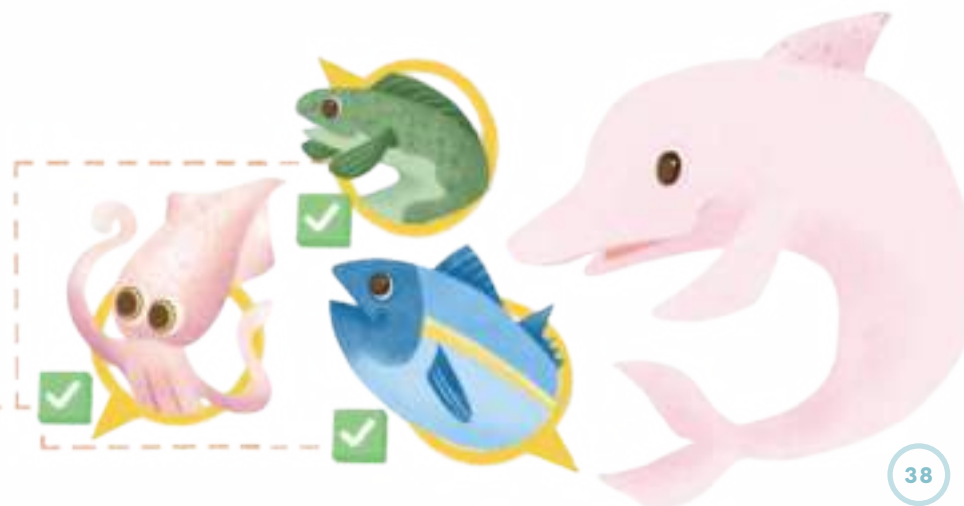
海豬仔說：「每一次自我查核、事件通報或桌上推演，都提醒我們制度可能潛藏漏洞。但光是發現問題是不夠的，只有將『發現』轉化為『行動』，才能真正補強制度、避免同樣的錯誤重演。」

龜龜苦著臉說：「你說得沒錯，我回頭盤點了上次推演的結果，發現有幾個共通性的問題。」

- ➔ 制度文件太複雜，導致實際執行時發生困難
- ➔ 表單欄位不完整，找不到流程中對應的窗口
- ➔ 文件修正後沒同步更新給所有人，各部門間資訊有落差

「問題又多又雜，全靠我一人負責，難道沒有什麼修正措施的 SOP 嗎？」

海豬仔：「算是沒白教你了，既然已經有了這些觀察，接下來可以把問題進行分析與改善！給你看看我之前整理的秘笈！」



改善流程步驟

✧ 第一階段：問題辨識

① 盤點問題

- 蒐集通報紀錄、員工回饋、查核報告等線索
- 判斷問題屬性：是制度設計缺陷、資源不足，還是人員操作偏差

② 問題回溯與根因分析

- 逐層追問原因，拼湊出問題的根因
- 比較理想做法與實際做法，找出落差的原因
- 蒐集第一線意見：納入第一線操作經驗，避免只停留在管理層的推測

✧ 第二階段：擬定對策並公告周知

③ 內部討論與確認

- 邀請相關人員共同釐清問題，分辨出需要修正的部份，以及實際做法為何

④ 修正制度文件

- 更新程序書、表單或流程圖，邀請使用者共同參與修正
- 檢視每個環節是否合理、可行，避免只做文字修補

⑤ 通知與教育

- 公告制度更新，並清楚說明修改原因
- 透過教育或簡報，確保人員理解並能正確執行

✧ 第三階段：記錄與持續修正

⑥ 修正紀錄與版本控管

- 記錄版本號、修改人、修改原因與日期
- 文件命名以版本加上日期為原則（例如：通報流程_v1.3_202508）
- 大幅修正需正式公告，並避免僅用電子郵件等一次性通知進行
- 若公告於雲端布告欄，設定檔案類型為唯讀，並留意權限設定，降低誤刪風險

⑦ 滾動式修訂

- 謹記「改善不是一次到位，而是持續循環」的大原則
- 每次發現問題就修正與記錄，讓制度隨組織成長、進化

— 小結 —

讓資安制度成為日常，而不是口號

海豬仔說：「資安制度不是用來寫報告的裝飾詞，也不是喊了就會實現的口號。它真正的價值，在於每天遇到問題時，我們會主動去想——要怎麼改善，才能做得更好。」

當團隊能以這樣的態度面對問題，制度就會從流程，轉化成一種習慣，再從習慣逐漸累積為組織文化。

龜龜點頭：「每次錯誤、每次學習，都能使我們一步步變得更強壯！」



龜龜筆記本

- Q 這次的修訂，真的解決了原本的問題嗎？**
大部分能解決，但缺乏驗證流程，效果未知
- Q 修改過程是否留下清楚的紀錄？**
已經加上版本號與簡要說明，但修改原因常寫得過於簡略
- Q 更新後的制度，大家真的理解並能執行嗎？**
已經公告，但缺乏統一說明，無法確認是否真正傳達給全公司
- Q 制度文件持續檢討與進步的可能？**
會依平時員工提出的改善意見修正，但沒有固定的回顧與檢討機制

龜龜在這段旅程中學到，制度的每次修正、每次更新，都是讓整個組織更清楚方向、少走冤枉路的機會。只要願意回頭檢視、記錄與修正，制度就能陪著團隊不斷進化、越走越穩。

附錄 | 海豬仔的百寶箱 可參考的相關資料



數位發展部資通安全署

✎ 資通安全事件通報應變流程

明定我國政府與特定非公務機關通報資安事件的流程、層級與責任。



✎ 資通安全應變程序範本

提供完整的事件應變文件範例與表單格式，協助組織依據自身規模與業務特性設計可落地的制度與程序書。



TWCERT/CC 台灣電腦網路危機處理暨協調中心

✎ 企業資安事件應變處理指南

說明企業在發生資安事件時的通報、隔離、調查與復原流程，提供事件分級與通報時限參考。



衛生福利部

✎ 醫院面對勒索軟體攻擊的應變指南

專為醫療機構制定之應變指南，說明遭勒索攻擊時的分階段應變措施與溝通重點，強調關鍵服務持續運作與病患資料保護。



附錄 | 海豬仔的百寶箱 常見的程序書類型

為了確保資通安全管理制度能夠有效落實，並符合法規及主管機關的要求，組織可建立資安相關程序書，作為內部控制與執行的依據。

程序書的目的如下：

➔ 符合法規要求

滿足主管機關與相關標準（如 ISO 27001、個人資料保護法、資通安全管理法）對文件化流程的規定。

➔ 確保一致性

使全體人員依循統一的作業流程，避免個人理解差異造成資安漏洞。

➔ 保留可追溯性

保留制度修訂與操作紀錄，方便後續稽核與檢討。

➔ 強化執行力

將資安政策與規範轉化為具體可執行的步驟，確保制度真正運作於日常管理中。

以下列出常見的程序書類型及其功能說明：

✧ 常見的程序書

程序書名稱	功能說明
帳號與密碼管理程序書	規範帳號申請、停用程序、密碼長度與更換頻率等
存取控制管理程序書	規定如何申請 / 變更 / 移除系統權限等規範
系統更新與修補管理程序書	說明系統更新檔、漏洞修補作業的流程與紀錄要求等
備份與還原程序書	包含備份排程、儲存位置、測試還原流程等
資安事件通報與應變處理程序書	定義事件類型、通報流程、通報窗口、應變小組任務與處置時限等
資安事故調查與回報程序書	定義資安事件的後續追蹤、紀錄與報告格式等

- 結語 -

✦ 制度落地，星球穩行

在海湧觀光星球，每一次的預約、每一份紀錄、每一張照片，背後都連結著遊客的信任。只要有一個環節出現漏洞，整個系統都可能受到影響。

這本《資安星際指南：資安制度全攻略》，帶著大家跟隨海豬仔和龜龜，一步步走過 PDCA 循環，從規劃制度、落實操作、查核檢驗到持續改善，把資安真正融入日常工作。

☑ 海豬仔提醒我們：制度需要被實踐，也需要證據。

☑ 龜龜的經驗告訴我們：再小的行動，也能守住一分安全。

資安是一種團隊的默契

一份紀錄、一場演練、一張通報表單，都是累積信任的重要基石。當每個成員都清楚流程、養成習慣，星球的防線就會逐漸堅固。

✦ 讓我們從這些日常動作開始

💡 寫下清楚的程序書，確保所有人都能照著做。

💡 定期檢查備份與還原，確認系統能及時復原。

💡 安排演練與桌上推演，測試在災難中能否繼續營運。

💡 精簡通報流程，讓事件能在第一時間被處理。

💡 留下紀錄與改進，讓下一次應對更快更好。

就像海港裡的船隻要定期維修檢查，資安的 PDCA 也必須持續循環，才能確保航程安全；當規劃、執行、檢查、改善成為日常習慣，資安文化就會自然成形。讓我們攜手前行，把制度變成日常，迎向更穩定、更長久的未來。





《資安星際指南：資安制度全攻略》

出版單位 國家資通安全研究院

召 集 人 林盈達

主 編 許建榮

副 主 編 方耀宇

執行編輯 胡馨元

作 者 邱元貞、張恩鳳、陳思帆

審 訂 王弘儒、林珊珊、陳奕穎
鄭翔云、龔俐霏、魏鈞培

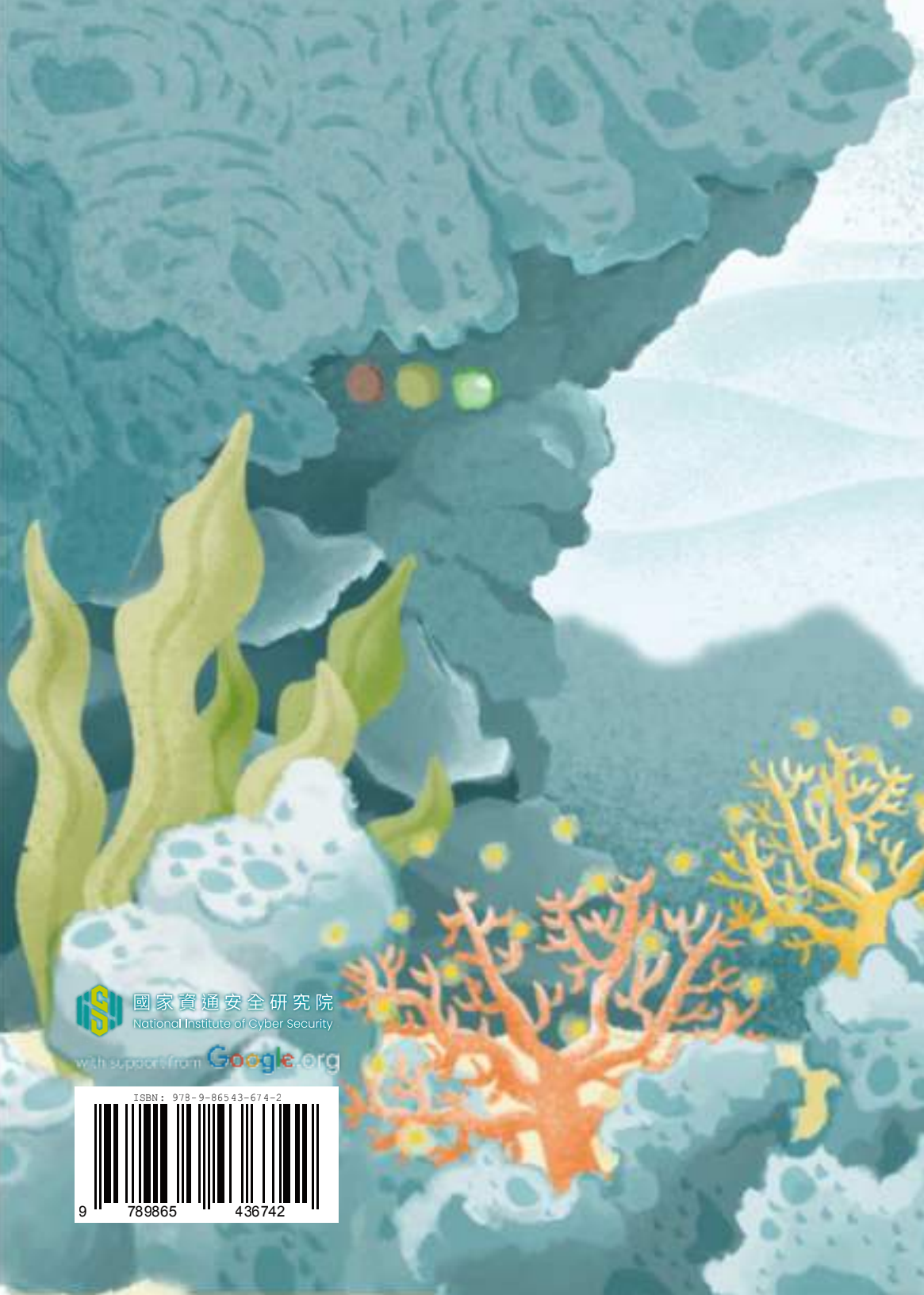
設 計 施逸青

出版日期 2025 年 11 月 初版一刷

ISBN 978-986-5436-74-2

本手冊出版來自 NICS 台灣資安計畫，由 Google.org 提供資金挹注。

本手冊中所提供的外部資訊及相關連結，其責任與權利歸屬於該媒體單位或作者所有。



國家資通安全研究院
National Institute of Cyber Security

with support from  Google.org

ISBN : 978-9-86543-674-2



9

789865

436742