資安弱掃標準放寬之風險揭露與責任承擔說明書

一、核心問題

是否應放寬弱點掃描標準，允許系統在未完全修補漏洞的情況下通過驗收？

二、風險總覽

危害類型	風險內容	影響程度
法遵風險	弱點未修補即上線、驗收，恐涉及違反《資通安全管理法》及政府資通系統防護基準要求。 ● 資安法第十二條 → 公務機關應置資通安全長，負責推動及監督機關內資安相關事務。 ● 資通安全責任等級分級辦法及其附表防護基準 → 資通系統應完成弱點掃描並改善弱點。	🔴 高
技術風險	弱點未修補→遭駭客利用、系統被入侵、資料外洩、網站遭植入惡意程式。	🔴 高
營運風險	資通系統遭攻擊→服務中斷、登入異常、資料損毀，造成校務作業受影響。	🟠 中高
名譽風險	資安事件曝光→媒體報導、家長與學生信任下降，影響校譽。	🔴 高
外包風險	弱掃未通過仍允許驗收→廠商責任減弱、安全品質下降、維護成本增加。	🟠 中

三、攻擊統計

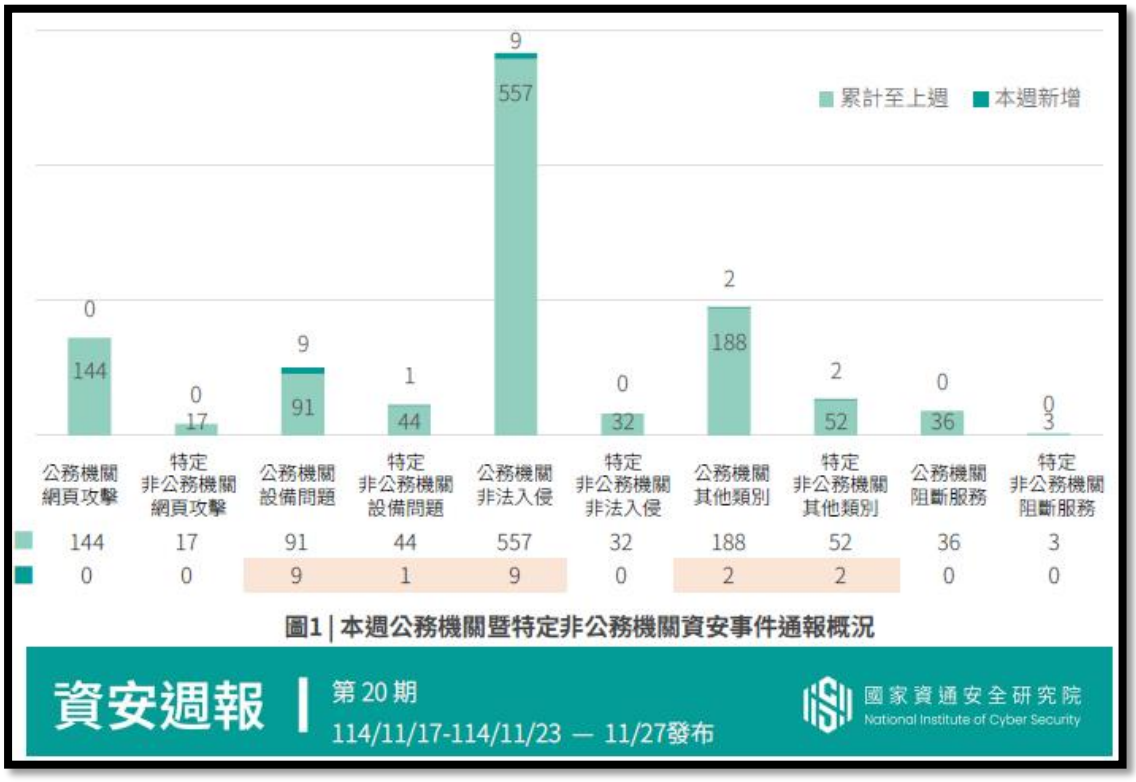

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

四、放寬弱點掃描標準之直接後果

- 弱點未全數修補亦可驗收 → 廠商可在安全修補尚未完成的情況下交付成果，降低其安全責任。
- 風險將由學校、承辦單位主管及系統承辦人員承擔，包括：
  - 系統遭入侵，資料遭竊取、外洩的後果。
  - 系統遭入侵且被利用作為跳板主機，攻擊校內、外應用系統或主機，導致其他方之損失。
  - 對承辦單位主管、承辦人員的行政責任與外界問責。
  - 後續事件處理所需的人力、時間與成本。

一旦發生資安事件，將難以再追究廠商責任，責任多由承辦單位自行承擔。

五、建議作法

1. 維持既有弱點掃描驗收標準

- 弱掃要求為法律遵循事項，並非技術單位單方面的堅持。
- 可避免主管、承辦人因系統弱點而承擔後續行政責任。
- 確保廠商依約完成系統安全加固，維持系統品質與可持續維運性。

2. 若承辦單位仍需申請放寬→請填寫「弱點處理報告單」並承擔風險

- **承辦單位須提出放寬申請，填寫「弱點處理報告單」**（含理由與必要性）。
- **「弱點處理報告單」必須由承辦單位主管親簽**，確認願意承擔弱點未修補所伴隨的法律、營運與資安風險。
- **資訊中心提供技術意見，但不承擔弱點未修補的後續責任**。

六、結語

弱點掃描標準為國家資安法規的強制要求，其目的在於降低資料外洩與系統入侵的風險，亦是保護承辦單位、主管及學校整體資訊安全的重要防線。若選擇放寬標準，需以書面方式確認風險與責任歸屬，以確保流程透明並保障相關人員。