項目	(九)資通安全事件通報應變及情資評估因應
9.1	是否訂定資安事件通報作業規範，包含判定事件等級之流程及權責、事件影響及損害評估、內部通報流程、通知其他受影響機關之方式、通報窗口及聯繫方式等，並規範於知悉資通安全事件後 1 小時內進行通報，若事件等級變更時應續行通報？相關人員是否熟悉相關程序，且落實執行？
9.2	是否訂定資安事件應變作業規範，包含應變小組組織、事前之演練作業、事中之損害控制機制，以及事後之復原、鑑識、調查及改善機制、相關紀錄保全等，且落實執行？
9.3	【參與行政院資通安全會報資通系統實兵演練機關適用】機關參與行政院資安會報對外資通系統實兵演練，是否就相關系統弱點訂定資安防護改善計畫，並落實執行？
9.4	是否建立資安事件相關證據資料保護措施，以作為問題分析及法律必要依據？
9.5	近 1 年所有資安事件及近 3 年第 3、4 級資安事件之通報時間、過程、因應處理及改善措施，是否依程序落實執行？
9.6	是否訂定資安事件處理過程之內部及外部溝通程序？
9.7	針對所有資安事件，是否保留完整紀錄，並與其他相關管理流程連結，應依自身機關資通安全責任等級保存日誌，詳各機關資通安全事件通報及應變處理作業程序表二，且落實執行後續檢討及改善？
9.8	【A、B 級機關適用】 是否建置資通安全威脅偵測管理(SOC)機制？監控範圍是否包括「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄？SOC 是否有委外供應商？SOC 供應商是否依契約規範(包含 SLA 水準)確實履約？
9.9	【A、B 級機關適用】 是否依指定方式提交 SOC 監控管理資料？

9.10	是否訂定應記錄之特定資通系統事件（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）、日誌內容、記錄時間週期及留存政策，且保留日誌至少 6 個月？是否有啟用 DNS 及內部網路之相關紀錄日誌日誌時戳是否對應世界協調時間（UTC）或格林威治標準時間（GMT）或相關校時主機?
9.11	是否依日誌儲存需求，配置所需之儲存容量，並於日誌處理失效時採取適當行動及提出告警？
9.12	針對日誌之是否進行存取控管，並有適當之保護控制措施？
9.13	是否監控資通系統以偵測攻擊與未授權之連線?是否辦理系統軟體及資訊完整性之控制措施?
9.14	知悉資通安全事件後，是否於規定時間內完成損害控制或復原作業，並持續進行調查及處理(包含根因分析、跡證保存及防範措施等)，於 1 個月內送交調查、處理及改善報告，且落實執行？（第一級或第二級事件：72 小時內完成損害控制或復原作業；第三級或第四級事件：36 小時內完成損害控制或復原作業）
9.15	知悉第三級或第四級資通安全事件後，是否由資通安全長召開會議研商相關事宜，並得請相關機關提供協助？
9.16	是否建立資通安全情資之評估及因應機制，針對所接受之情資(警訊)，辨識其來源之可靠性及時效性，及時進行威脅與弱點分析及研判潛在風險，並採取對應之預防或應變措施？
9.17	是否適時進行資通安全情資分享？分享哪些資訊？