114 年度資安稽核概況報告

數位發展部

中華民國 115 年 1 月

目 次

圖 目 次

表 目 次

壹、 依據及目的

數位發展部（以下稱本部）自 111 年 8 月 27 日成立，賡續辦理行政院國家資通安全會報資通安全稽核（以下稱行政院資安稽核），協助各機關發掘潛在的資安風險，持續精進資安整體防護水準。

鑒於資安法於 114 年 9 月 24 日修法通過，並於同年 12 月正式施行，為有效落實納管機關的資安管理與防護，並供各機關參考改進，本部依修正後同法第 6 條規定，公布「114 年度資安稽核概況報告」，並送立法院備查。惟 114 年度稽核計畫係於修法前核定並執行，故本報告稽核內容係依據修法前之法遵事項；針對新法增修內容，本部將納入後續年度稽核計畫辦理，以持續精進資安防護韌性。

114 年度行政院資安稽核延續以策略、管理及技術等 3 大構面辦理實地稽核作業，並關注當前資安威脅情勢，滾動調修稽核作業程序及稽核重點。由具備資安專業及實務經驗之產官學研稽核團隊，協同檢視各機關資通系統之各項資通安全管理政策、程序及整體防護作為，並對資通安全責任等級（以下稱資安責任等級）A 級公務機關於實地稽核前實施技術檢測；及對有維運工控系統或運營科技（OT）之受稽機關，額外辦理工控系統或運營科技（OT）實地稽核。期經由行政院資安稽核，持續完備各機關資通安全管理機制，以建構國家資通安全環境。

本報告綜整 114 年度資安稽核執行結果，分析各機關法遵符合情形及待改善事項，說明較具指標性的稽核發現，供納管機關作為借鏡參考，並提出對應之建議，俾利落實改善機制，以精進機關整體資安意識，降低國家整體資安風險。

貳、114 年度資安稽核作業辦理情形

一、 稽核重點

依當前國際資安發展、資安威脅趨勢及我國資安業務推動現況，持續滾動調修稽核作業程序及稽核重點，114 年資安稽核重點為業務持續運作規劃及演練、委外廠商管理及稽核、落實弱點修補情形、危害國家資通安全產品之禁用管控、雲端服務資安防護及控制措施、資安事件通報應處及聯防等項目，期敦促加強落實相關因應對策，持續強化公務機關及特定非公務機關整體資安防護。

二、 受稽機關遴選原則

依 114 年資通安全稽核計畫奉准規劃，114 年受稽核機關原則為 112 年受稽核之行政院所屬二級及獨立機關，並依過去稽核頻率、稽核結果及政策推動情形等綜整考量分配調整。

三、 稽核分組及稽核方式

考量稽核實務，將受稽機關依資安責任等級等條件進行分類，並分別適用不同之稽核類別及評分方式如表 1。

表 1　稽核類別及評分方式

類別	技術檢測	工控系統或運營科技（OT）	總成績計算方式
1			實地稽核得分×100%
2	V		1. A 級公務機關：技術檢測得分×30％＋實地稽核得分×70% 2. 非 A 級公務機關：實地稽核得分×100%
3		V	實地稽核得分（資訊系統稽核得分×70%+工控系統或運營科技（OT）稽核得分×30%）×100%
4	V	V	1. A 級公務機關：技術檢測得分×30％＋實地稽核得分（資訊系統稽核得分×70%+工控系統或運營科技（OT）稽核得分×30%）×70% 2. 非 A 級公務機關：實地稽核得分（資訊系統稽核得分×70% ＋ 工控系統或運營科技（OT）稽核得分×30%）×100%

受稽核公務機關之資安責任等級如為 A 級，於實地稽核前先行辦理技術檢測，主要對受稽機關之核心資通系統、網域主機、資料庫、使用者電腦、網路架構、物聯網設備、組態設定及網路惡意活動等進行安全檢測，為期 3 個工作日，其他非 A 級公務機關如經稽核團隊指定為受技術檢測機關，則不納入計分；實地稽核作業由行政院國家資通安全會報組成稽核團隊，至受稽機關進行實地查核，為期 1 個工作日。

四、 受稽機關及稽核日期

114 年度各受稽核機關實地稽核日期如表 2，其中特定非公務機關涉及關鍵基礎設施資訊，爰以代碼表示。

表 2　114 年各受稽機關稽核日期

編號	受稽機關	實地稽核日期
1	特定非公務機關 A	4 月 14 日
2	特定非公務機關 B	4 月 25 日
3	特定非公務機關 C	5 月 2 日
4	特定非公務機關 D	5 月 9 日
5	特定非公務機關 E	5 月 15 日
6	衛生福利部金門醫院	5 月 19 日
7	特定非公務機關 F	5 月 22 日
8	衛生福利部澎湖醫院	5 月 26 日
9	特定非公務機關 G	6 月 2 日
10	特定非公務機關 H	6 月 12 日
11	特定非公務機關 I	6 月 16 日
12	特定非公務機關 J	6 月 18 日
13	特定非公務機關 K	6 月 23 日
14	特定非公務機關 L	6 月 26 日
15	特定非公務機關 M	6 月 30 日
16	特定非公務機關 N	7 月 2 日
17	臺灣高等檢察署	7 月 17 日
18	行政院公共工程委員會	7 月 24 日
19	交通部中央氣象署	7 月 31 日
20	特定非公務機關 O	8 月 4 日

編號	受稽機關	實地稽核日期
21	大陸委員會	8月7日
22	僑務委員會	8月15日
23	外交部	8月25日
24	經濟部	8月27日
25	國家太空中心	9月3日
26	特定非公務機關P	9月5日
27	衛生福利部臺東醫院	9月8日
28	國家中山科學研究院	9月10日
29	特定非公務機關Q	9月19日
30	原住民族委員會	9月24日
31	衛生福利部	9月26日
32	國家資通安全研究院	10月1日
33	特定非公務機關R	10月3日
34	文化部	10月8日
35	特定非公務機關S	10月16日
36	環境部	10月22日
37	特定非公務機關T	10月29日
38	勞動部	10月31日
39	交通部	11月5日
40	農業部	11月12日

五、 稽核團隊

稽核團隊主要由稽核領隊、稽核委員、技術檢測人員組成，共同執行資安稽核作業；另為培訓政府機關稽核種子人員，設置觀察員，並由稽核委員輔導觀察員參與實地稽核，稽核團隊人員組成與其資格如下，本部並得視實際情況及受稽機關之屬性、規模、查檢場域及系統等因素進行有關調整。

(一)稽核領隊：

由行政院國家資通安全會報副召集人、協同副召集人、其他經其授權之人員，或由行政院國家資通安全會報幕僚單位：本部之正副首長及資通安全署（以下簡稱資安署）之正副首長、主任秘書擔任，並得由國家安全會議國家資通安全辦公室主任、資安署各組組長或策略面委員代理。

(二)稽核委員：

1、 遴選標準

(1) 由本部考量稽核實際需求，邀請具備資通安全政策、管理、技術、法律專業或具實務經驗之公務機關代表或產、學、研等專家學者擔任團隊成員，各場次除策略面委員由政府機關委員擔任外，管理面及技術面公務機關委員以 3 分之 1 為原則。

(2) 稽核委員如有涉及特定非公務機關資通安全維護計畫實施情形稽核辦法第 6 條第 4 項各款之情形，應通知資安署並主動迴避擔任該場次稽核委員。

(3) 稽核委員如於 114 年已受其他上級或中央目的事業主管機關邀約擔任同一受稽機關稽核委員，亦應通知資安署及迴避擔任該場次稽核之稽核委員。

2、 分配原則

每個稽核場次以安排 8 位稽核委員為原則，包括策略面

2 名、管理面 3 名及技術面 3 名。如受稽機關有維運工控系統或運營科技（OT），則額外配置 2 名工控（OT）稽核委員進行工控系統或運營科技（OT）實地稽核作業。

(三)觀察員：

自總統府與中央一級機關含所屬機關、直轄市政府與各縣市政府及所屬一級機關之公務人員遴選，每場次至多 6 名觀察員。

(四)工作人員：

辦理現場幕僚或行政作業之人員，負責啟始會議、委員意見交換、結束會議簡報及其他行政庶務作業，人數視實際需求配置 3 至 6 名。

(五)技術檢測人員：

由國家資通安全研究院及資安署中具備惡意程式檢測、系統滲透測試及網路檢測等資安檢測能力及經驗之技術檢測人員擔任，每場技術檢測人員至多 12 名。

(六)觀摩人員：

觀摩現場實地稽核作業，不參與稽核問答過程，人數視實際需求而定。

六、 稽核基準、範圍與項目

依據資通安全管理法（108 年施行）及其子法（110 年施行）、國家資通安全發展方案（110 年至 113 年、114 年至 117 年）、資訊安全管理系統國家標準 CNS 27001:2014、CNS 27001:2023 或資訊安全管理系統國際標準 ISO 27001:2013、ISO 27001:2022、服務管理系統國際標準 ISO 20000-1:2018、資通安全維護計畫、其他內部控制及資安相關規定。

工控系統或運營科技（OT）通用性防護建議係參考國際安全標準與主要國家防護文件，及中央目的事業主管機關依資通安全責任等級分級辦法第 11 條自行擬訂之防護基準等。

(一)稽核範圍

稽核範圍為受稽機關資通安全維護計畫所包括之全機關及資通系統之各項資安管理政策、程序等。

(二)稽核項目

1、 第 1 階段：技術檢測

技術檢測分為 8 大檢測項目，各檢測項目之執行內容及配分說明如表 3。

表 3　技術檢測項目及配分

項次	檢測項目	檢測子項	配分
1	使用者電腦安全檢測	使用者電腦弱點掃描	10
		使用者電腦安全防護檢測	10
2	物聯網設備檢測		10
3	網域主機安全防護檢測	防毒軟體檢測	5
		安全性更新檢測	
		惡意程式檢測	
4	資料庫安全檢測		10
5	核心資通系統安全檢測	核心資通系統內網滲透測試	20
		核心資通系統防護基準檢測	5
6	網路架構檢測		10
7	組態設定安全檢測	作業系統組態檢測	10
		瀏覽器組態檢測	
		網通設備組態檢測	
		應用程式組態檢測	
8	網路惡意活動檢視	惡意中繼站連線阻擋檢測	5
		APT 網路流量檢測	5
合計：			100

2、 第 2 階段：資訊系統及工控系統或運營科技（OT）實地稽核

資訊系統實地稽核分策略面、管理面及技術面等 3 個構面共 9 個稽核項目，各構面之稽核項目與配分如表 4。

表 4　資訊系統各構面稽核項目及配分

構面	稽核項目	配分
策略面	一、核心業務及其重要性	10
	二、資通安全政策及推動組織	10
	三、專責人力及經費配置	10
管理面	四、資訊及資通系統盤點及風險評估	10
	五、資通系統或服務委外辦理之管理措施	10
	六、資通安全維護計畫與實施情形之持續精進及績效管理機制	10
技術面	七、資通安全防護及控制措施	20
	八、資通系統發展及維護安全	10
	九、資通安全事件通報應變及情資評估因應	10
	合計：	100

針對有維運工控系統或運營科技（OT）之受稽機關，就擇定之核心系統（OT）等，依據10大稽核項目（分管理面及技術面等 2 個構面）額外辦理（OT）實地稽核，各構面之稽核項目及配分說明如表 5。

表 5　工控系統或運營科技（OT）各構面稽核項目及配分

構面	稽核項目	配分
管理面	一、事件日誌與可歸責性	10
	二、營運持續計畫	10
	三、系統與服務獲得	10
技術面	四、ICS（OT）網路架構	10
	五、存取控制	10
	六、識別與鑑別	10
	七、系統與通訊防護	10
	八、實體與環境防護	10
	九、系統與資訊完整性	10
	十、組態管理	10
	合計：	100

參、114 年稽核結果

114 年受稽機關計有 40 個，依稽核階段分以技術檢測、實地稽核及稽核總成績說明如下。

一、 技術檢測

技術檢測機關共 9 個，8 個檢測項目之平均分數經標準化後，檢視個別項目得分情形，其中「網域主機安全防護檢測」、「資料庫安全檢測」、「網路惡意活動檢視」等 3 個項目表現較佳，各項目得分情形詳見圖 1。

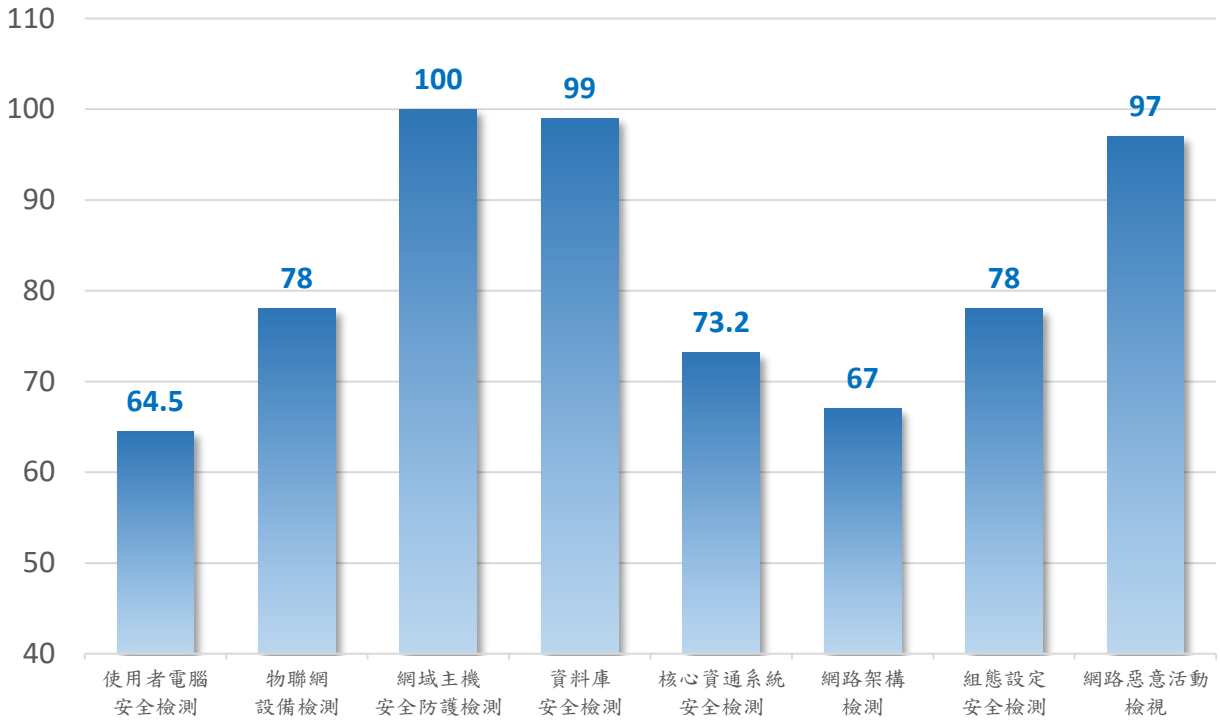

圖 1　技術檢測各項目得分情形

二、 實地稽核

實地稽核 9 個項目之平均得分經標準化後，檢視個別項目得分情形，其中「專責人力及經費配置」得分最高，「資通安全政策及推動組織」次之，各項目得分情形詳見圖 2。

圖 2　實地稽核各項目得分情形

三、 稽核總成績

114 年受稽機關平均總成績為 71.56 分，公務機關及特定非公務機關得分，詳見圖 3。

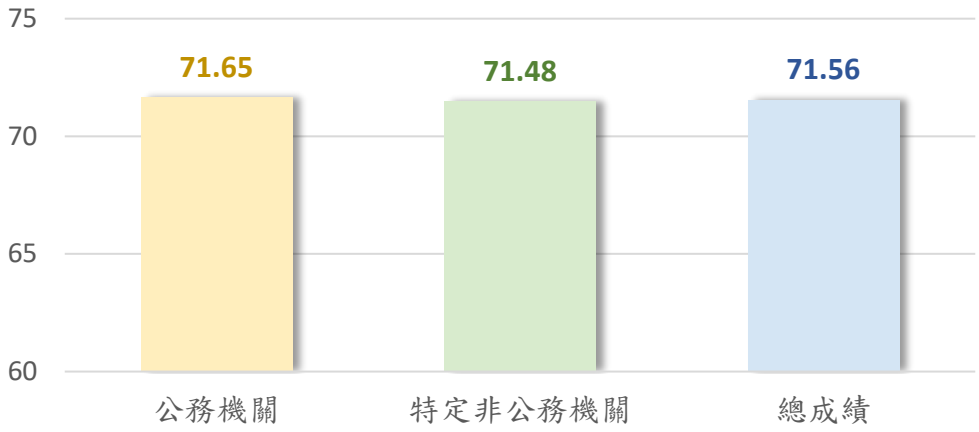

圖 3　公務機關及特定非公務機關得分比較

本次受稽機關其中 22 個機關在 108 年資安法施行後曾受行政院資安稽核、18 個機關為首次受行政院資安稽核，分別統計各階段稽核結果，曾受行政院資安稽核機關在實地稽核表現，資訊系統及工控系統或運營科技（OT）領域均優於首次受稽核機關。114 年度執行結果持續呈現曾受稽核機關之資安防護有效提升，顯示經由行政院資安稽核

機制檢視機關各項資安工作及防護措施落實情況，有助機關將稽核發現確實納入PDCA循環，強化機關整體資安防護韌性，平均得分成績詳見圖4。

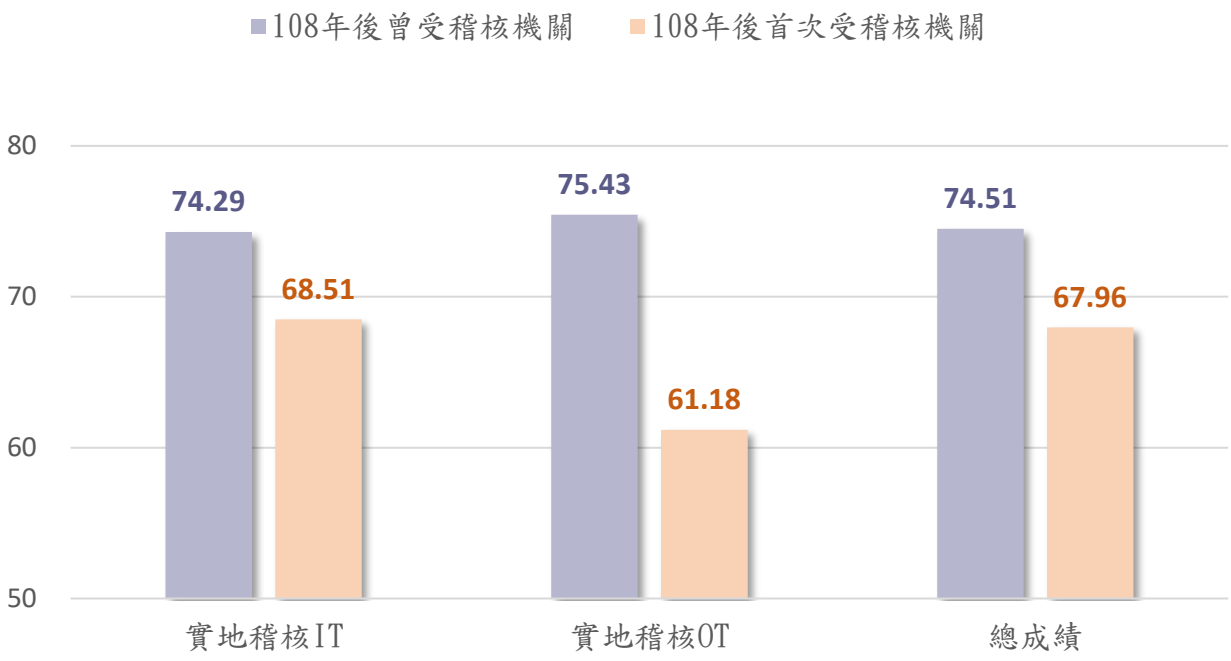

圖4　是否曾受稽核之平均得分成績比較

肆、 稽核共同發現

經綜整 114 年之稽核發現，就法遵符合情形及待改善事項，彙整較具重要性可提供各級機關借鏡之事項，分別就策略面、管理面、技術面及工控面分別說明如下。

一、 法遵符合情形

(一)策略面

1、依規定配置足額之資通安全專職(責)人員，並增加專職(責)辦理資安業務之人力外，另推動資安種子人員制度，提升各業務單位資安專業職能，有助推動機關資安作業。

2、機關導入資訊安全管理系統標準，並完成公正第三方驗證之範圍，除核心資通系統外，亦擴大至其他資通系統，部分機關已將驗證範圍涵蓋至全機關。

3、對辦理資通安全業務相關人員定期審核，並給予適度獎勵，顯示對機關資通安全之支持與重視。

(二)管理面

1、透過舉辦資安漏洞獎勵活動，與外界專家協力檢測資通系統，除提升公私協作關係外，更能有效識別潛在漏洞，進而強化資安防護能力。

2、妥適訂定第二方稽核之資通安全稽核計畫，確認稽核方式、範圍及頻率，並完備待改善事項之追蹤及陳核程序，落實資通安全維護計畫實施情形之持續精進機制。

3、定期提報系統異常事件分析統計表，並具體說明處理方式及後續預防措施，且有簽核程序，有效掌握系統異常情形。

(三)技術面

1、除提升資通系統安全性檢測頻率外，亦將源碼檢測、滲透測試等擴及至中、普等級資通系統，並確實落實修補漏洞。

2、透過即時情資彙整平臺進行自動化情資分析，並與上級機關

或中央目的事業主管機關進行情資分享，達資安聯防效果。

3、針對個資欄位，採用資料庫欄位加密機制，並導入安全憑證管理加密金鑰，有效強化個資保護。

(四)工控面

1、普等級控制系統亦納入機關故障分析機制，有效追蹤異常事件之潛在影響。

2、機關 OT 網路建置單向隔離措施，嚴格管控 OT 網路資料單向傳輸至 IT 網路。

3、機關將工控場域內系統、防火牆等系統日誌即時備份至實體主機。

二、待改善事項

(一)策略面

1、部分機關高等級資通系統未辦理異地備份，部分機關未定期驗證備份媒體可靠性與備份資訊完整性。

2、部分機關業務持續運作演練未納入新興資安威脅及複合式情境、無業務單位參與，或演練範圍未包含所有核心資通系統。

3、部分機關未依資通系統防護需求分級原則評估系統分級，或未建立客觀一致性之衡量標準。

(二)管理面

1、部分機關未定期稽核委外廠商執行情形，亦缺乏後續追蹤與改善機制，同時尚未建立系統第三方元件清單。

2、部分機關未建立資產異動管理程序，或資產盤點範圍未涵蓋全機關，導致資產清冊與實際情形不符。

3、部分機關資安風險評估機制未臻妥適，未適當檢討可接受風險值及未針對委外業務項目進行風險評估。

(三)技術面

1、部分機關資安防護未臻完善，如未建立完善的網段區隔、實體機房未落實管制(如監視、消防、進出管制等)，且未落實無線基地台、雲端服務之防護控制措施。

2、部分機關未完成中高風險弱點之修補，亦未建立替代管控措施，另修補後未進行複測，無法確認修補有效性。

3、部分機關未於時限內完成資安事件通報，第 3 級與第 4 級事件未依規定由資安長召開會議研商；另部分機關相關通報應變程序書未完整包含法規要求，導致應變制度未臻完善。

(四)工控面

1、部分機關帳號密碼管理機制未完備，如 OT 系統管理者密碼為供應商持有、未定期審查帳號、未變更預設密碼及共用帳號且無其他監管措施等。

2、部分機關未完整盤點 OT 資產，或盤點分類方式不符合防護基準要求。

3、部分機關未落實執行 OT 資安防護控制措施，如重大漏洞未更新，缺乏校時機制，亦未完成 OT 網段隔離規劃與建置等。

三、 改善建議

(一)策略面

1、依資通安全責任等級分級辦法防護基準規定，防護需求等級為高之資通系統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，另防護需求等級為中以上之系統，應定期測試備份資料，驗證備份媒體之可靠性及資訊完整性，以確認資料備份還原機制正常運作。

2、依資通安全責任等級分級辦法應辦事項規定，核心資通系統應辦理業務持續運作演練，建議納入新興資安威脅及複合式情境，以切合實際複雜情形，並落實各業務單位共同參與演

練，以驗證業務服務有效性及真實反映跨單位合作之整體韌性。

3、依資通安全責任等級分級辦法第 11 條規定，各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級。機關應對資通系統進行機密性、完整性、可用性、法律遵循性四個構面進行評估分級，並建議建立全機關客觀一致之評估標準，且應於每年定期檢視分級妥適性，以有效分配資安防護資源。

(二)管理面

1、依資通安全管理法施行細則第 4 條規定，委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務執行情形，機關宜建立後續追蹤與改善機制，以確保供應鏈安全；另機關應建立系統第三方元件清單，以確保能掌握元件來源、版本及授權證明，以利於接獲漏洞情資時盡速修補。

2、依資通安全管理法施行細則第 6 條規定，資通安全維護計畫應包含資訊及資通系統之盤點，並標示核心資通系統及相關資產，機關應落實全機關資產盤點，盤點範圍包含全部單位，及納入 IT、OT、IoT 相關設備等，並建立資產異動管理程序，包含各類資產異動管理，如實體設備回收、業務異動等，以完整掌握資產範圍，俾利進行後續風險評鑑及處理。

3、依資通安全管理法施行細則第 6 條規定，資通安全維護計畫應包含資通安全風險評估，建議機關建立相關風險準則、進行風險評鑑等，且風險評估成員應包含資訊、資安人員及業務相關人員，以利風險評估結果符合機關現況情形。另不可接受之風險評估等級及風險評估結果，應經機關管理層級審查並核定，適時檢討可接受風險值。

(三)技術面

1、依資通安全管理法施行細則第 6 條規定，資通安全維護計畫應包含資通安全防護及控制措施，建議機關網路架構應依網路服務需要區隔獨立的邏輯網域，如 DMZ、內部或外部網路等，另於提供無線網路、雲端服務時，應針對服務存取及應用訂定相關安全管控程序並落實執行防護控制措施，以減少潛在攻擊。

2、依資通安全責任等級分級辦法應辦事項及資通系統防護基準規定，應定期辦理安全性檢測、資安健診等，及確認資通系統相關漏洞修復之狀態及系統之漏洞修復應測試有效性及潛在影響，並定期更新，建議機關發現系統漏洞後，應執行漏洞修補，且測試漏洞修復之有效性及潛在影響，如未能及時完成修補，應建立替代緩解管控措施，並持續追蹤。

3、依資通安全事件通報及應變辦法第 4 條、第 7 條及第 9 條規定，公務機關知悉資通安全事件後，應於 1 小時內依主管機關指定之方式及對象，進行資通安全事件通報，知悉第 3 級或第 4 級資通安全事件後，其資通安全長應召開會議研商相關事宜，並得請相關機關提供協助，建議機關透過演練、宣導等方式確保相關人員熟悉資安事件通報、應處等程序等。

(四)工控面

1、工控系統或運營科技（OT）之防護基準應依中央目的事業主管機關擬定之防護基準或依資通安全責任等級分級辦法資通系統防護基準規定辦理，機關應定期審查工控系統或運營科技（OT）帳號、變更預設密碼、共用帳號應有其他監管措施等，並以最小權限為原則進行權限管理，落實 OT 設備之存取控制。。

2、 依資通安全管理法施行細則第 6 條及中央目的事業主管機關

擬定之防護基準規定，機關應完整盤點 OT 資產，另部分機關應依所屬領域之防護基準規定進行 OT 資產分類，以掌握設備資產並遵循其防護基準。

3、機關依各領域中央目的事業主管機關擬定之防護基準或資通安全責任等級分級辦法資通系統防護基準規定辦理相關控制措施，如因技術限制、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，得依資通安全責任等級分級辦法第 11 條規定，提交配套措施經等級提交機關或等級核定機關同意，報請主管機關備查後，免執行該事項或控制措施，並加強網段隔離規劃建置、實體與環境防護及漏洞修補控管

伍、結語

本部於 114 年度辦理行政院國家資通安全會報層級資通安全稽核作業，全面檢視公務機關及特定非公務機關資通安全維護計畫實施情形及相關資安防護強化措施之完整性及有效性，強化國家整體資通安全法制，協助機關逐步提升資安管理政策及落實防護控制措施。

114 年度稽核結果顯示，各受稽機關在遵循法規、調整內部資安政策、完善管理制度及強化防護基準方面持續精進，使各項法遵要求之落實程度穩健提升。為因應快速演變的資安威脅，本部已完成資安法修法工作，以期建立更為健全的國家資通安全法制，並持續強化國家整體資通訊安全及韌性。

展望未來，本部將持續運用資通安全作業管考系統，密切追蹤受稽機關的改善進度，並透過資安長會議及各項資安專職人員調訓加強宣導與輔導，確保稽核發現的待改善事項能徹底落實，共同建構各機關更安全、更具韌性的數位環境。