建立證券商資通安全檢查機制-分級防護應辦事項附表

等級 應辦事項	第一級(A 級)證券商 實收資本額 200 億(含)以上	第二級(B 級)證券商 實收資本額 100 億(含)以上，未達 200 億	第三級(C 級)證券商 實收資本額 40 億(含)以上,未達 100 億	第四級(D 級)證券商 實收資本額未達 40 億	應辦事項完成日	對應項目
一、資訊安全管理系統之導入及通過公正第三方之驗證	初次受核定或等級變更後之二年內，全部核心資訊系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。	初次受核定或等級變更後之二年內，全部核心資訊系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。	初次受核定或等級變更後之二年內，全部核心資訊系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。	-	111 年 1 月底導入 112 年 1 月底通過驗證	2. 資訊安全政策(CC-12000)、(8)
二、資通安全專業證照	初次受核定或等級變更後之一年內，資通安全專責人員總計應持有四張以上，並持續維持證照之有效性。	初次受核定或等級變更後之一年內，資通安全專責人員總計應持有二張以上，並持續維持證照之有效性。	初次受核定或等級變更後之一年內，資通安全專責人員總計應持有一張以上，並持續維持證照之有效性。	-	112 年 1 月底	3. 安全組織(CC-13000)、(6)

等級 應辦事項	第一級(A 級)證券商 實收資本額 200 億(含)以上	第二級(B 級)證券商 實收資本額 100 億(含)以上，未達 200 億	第三級(C 級)證券商 實收資本額 40 億(含)以上,未達 100 億	第四級(D 級)證券商 實收資本額未達 40 億	應辦事項完成日	對應項目
三、資訊系統分級	初次受核定或等級變更後之一年內，針對自行或委外開發之資訊系統完成資訊系統分級；其後應每年至少檢視一次資訊系統分級妥適性。	初次受核定或等級變更後之一年內，針對自行或委外開發之資訊系統完成資訊系統分級；其後應每年至少檢視一次資訊系統分級妥適性。	初次受核定或等級變更後之一年內，針對自行或委外開發之資訊系統完成資訊系統分級；其後應每年至少檢視一次資訊系統分級妥適性。	初次受核定或等級變更後之一年內，針對自行或委外開發之資訊系統完成資訊系統分級；其後應每年至少檢視一次資訊系統分級妥適性。	111 年 1 月底	資產分類與控制(CC-14000)、(3)
四、網路防火牆	建置網路防火牆	建置網路防火牆	建置網路防火牆	建置網路防火牆	110 年 1 月底	7.通訊與作業管理 (1)網路安全管理(CC-17010)、b.
五、防毒軟體	導入防毒軟體	導入防毒軟體	導入防毒軟體	導入防毒軟體	110 年 1 月底	7.通訊與作業管理 (1)網路安全管理(CC-17010)、e.
六、電子郵件過濾機制	具有郵件伺服器者，應備電子郵件過濾機制	具有郵件伺服器者，應備電子郵件過濾機制	具有郵件伺服器者，應備電子郵件過濾機制	具有郵件伺服器者，應備電子郵件過濾機制	110 年 1 月底	7.通訊與作業管理 (1)網路安全管理(CC-17010)、e.(e)
七、系統滲透測試	全部核心資訊系統每年辦理一次。	全部核心資訊系統每二年辦理一次。	全部核心資訊系統每二年辦理一次。	-	111 年 1 月底	7.通訊與作業管理 (1)網路安全管理(CC-17010)、i.(a)

等級 應辦事項	第一級(A 級)證券商 實收資本額 200 億(含)以上	第二級(B 級)證券商 實收資本額 100 億(含)以上，未達 200 億	第三級(C 級)證券商 實收資本額 40 億(含)以上,未達 100 億	第四級(D 級)證券商 實收資本額未達 40 億	應辦事項完成日	對應項目
八、資通安全健診	每年辦理一次。	每二年辦理一次。	每二年辦理一次。	-	112 年 1 月底	7.通訊與作業管理 (1) 網路安全管理(CC-17010)、i.(b)
九、資通安全威脅偵測管理機制	建置資通安全威脅偵測管理機制。	建置資通安全威脅偵測管理機制。	-	-	112 年 1 月底	7.通訊與作業管理 (1) 網路安全管理(CC-17010)、 i.(c)
十、入侵偵測及防禦機制	建置入侵偵測及防禦機制	建置入侵偵測及防禦機制	-	-	112 年 1 月底	7.通訊與作業管理 (1) 網路安全管理(CC-17010)、i.(d)
十一、應用程式防火牆	具有對外服務之核心資訊系統者，應備應用程式防火牆。	具有對外服務之核心資訊系統者，應備應用程式防火牆。	-	-	112 年 1 月底	7.通訊與作業管理 (1) 網路安全管理(CC-17010)、i.(e)
十二、進階持續性威脅攻擊防禦措施	建置進階持續性威脅攻擊防禦措施		-	-	112 年 1 月底	7.通訊與作業管理 (1) 網路安全管理(CC-17010)、i.(f)
十三、公司交易相關網路直接連線之設備不得使用危害	與交易相關網路直接連線之設備不得使用危害國家資通安全產品。	與交易相關網路直接連線之設備不得使用危害國家資通安全產品。	與交易相關網路直接連線之設備不得使用危害國家資通安全產品。	與交易相關網路直接連線之設備不得使用危害國家資通安全產品。	110 年 1 月底	7.通訊與作業管理 (1)網路安全管理(CC-17010)、

等級 應辦事項	第一級(A 級)證券商 實收資本額 200 億(含)以上	第二級(B 級)證券商 實收資本額 100 億(含)以上，未達 200 億	第三級(C 級)證券商 實收資本額 40 億(含)以上,未達 100 億	第四級(D 級)證券商 實收資本額未達 40 億	應辦事項完成日	對應項目
國家資通安全產品。						b.(g)
十四、業務持續運作演練	全部核心資訊系統每年辦理一次。	全部核心資訊系統每二年辦理一次。	全部核心資訊系統每二年辦理一次。	依「建立證券商資通安全檢查機制」營運持續管理（CC-20000，半年查核）故障復原程序應週期性測試	111 年 1 月底	10. 營運持續管理(CC-20000)、(4)