

資通安全實地稽核之 因應分享

111年10月26日 V1.0

前置作業

*注意請勿填寫個人資料

問題1.今天日期?

答案:XX/XX

問題2.是否熟悉NMAP工具?

答案:是、否

<https://reurl.cc/dWNWZ2>

問題 回覆 設定

1111026

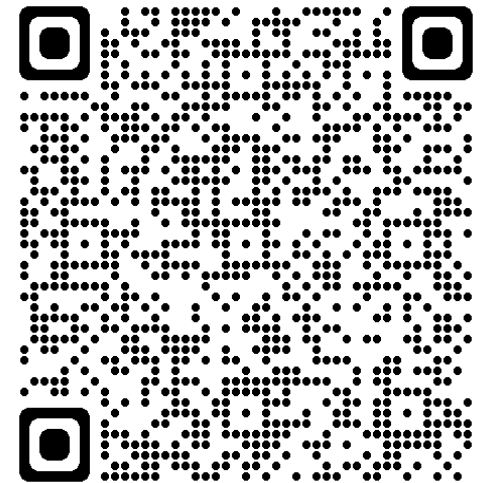
表單說明

問題1.

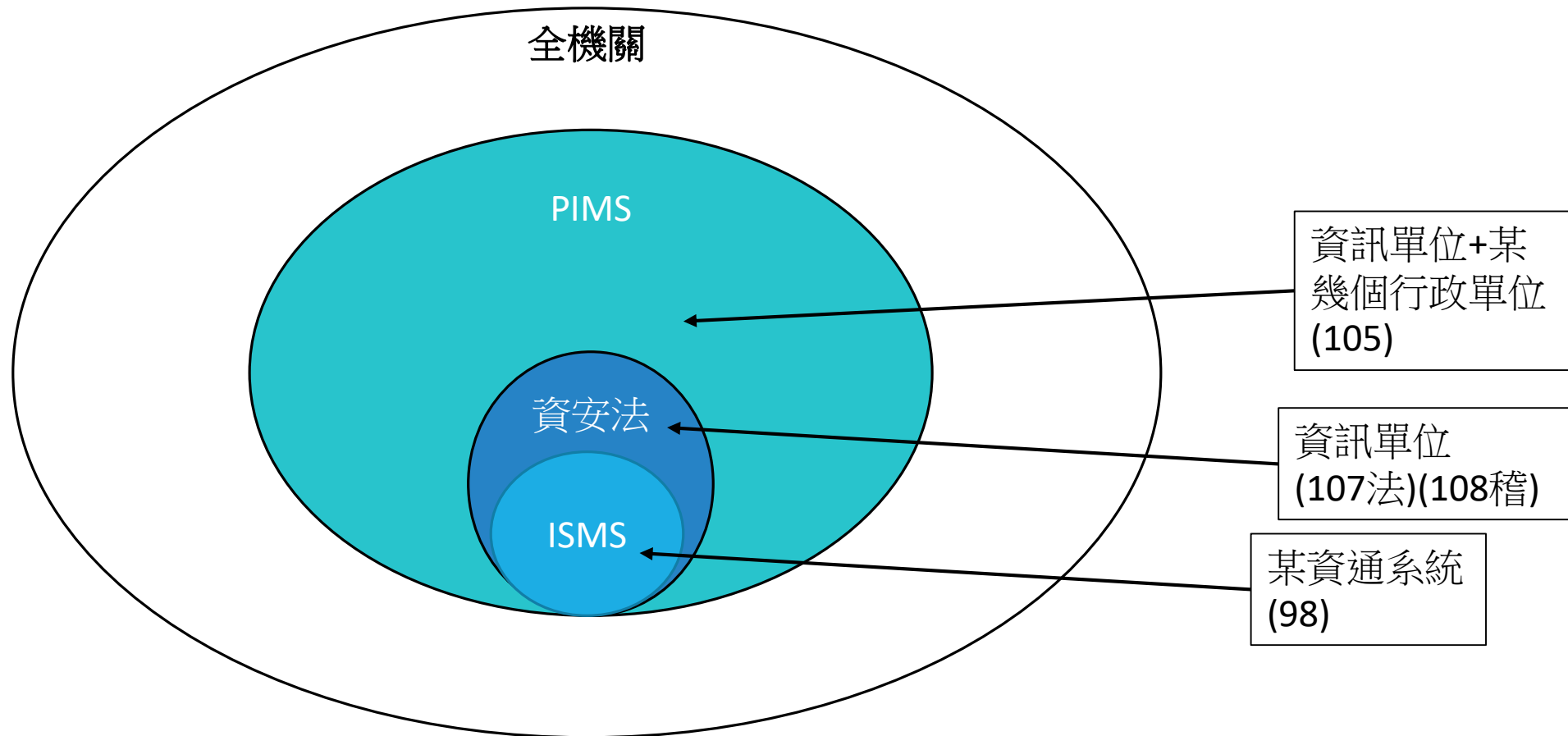
詳答文字

問題2.

詳答文字



適用範圍-初期



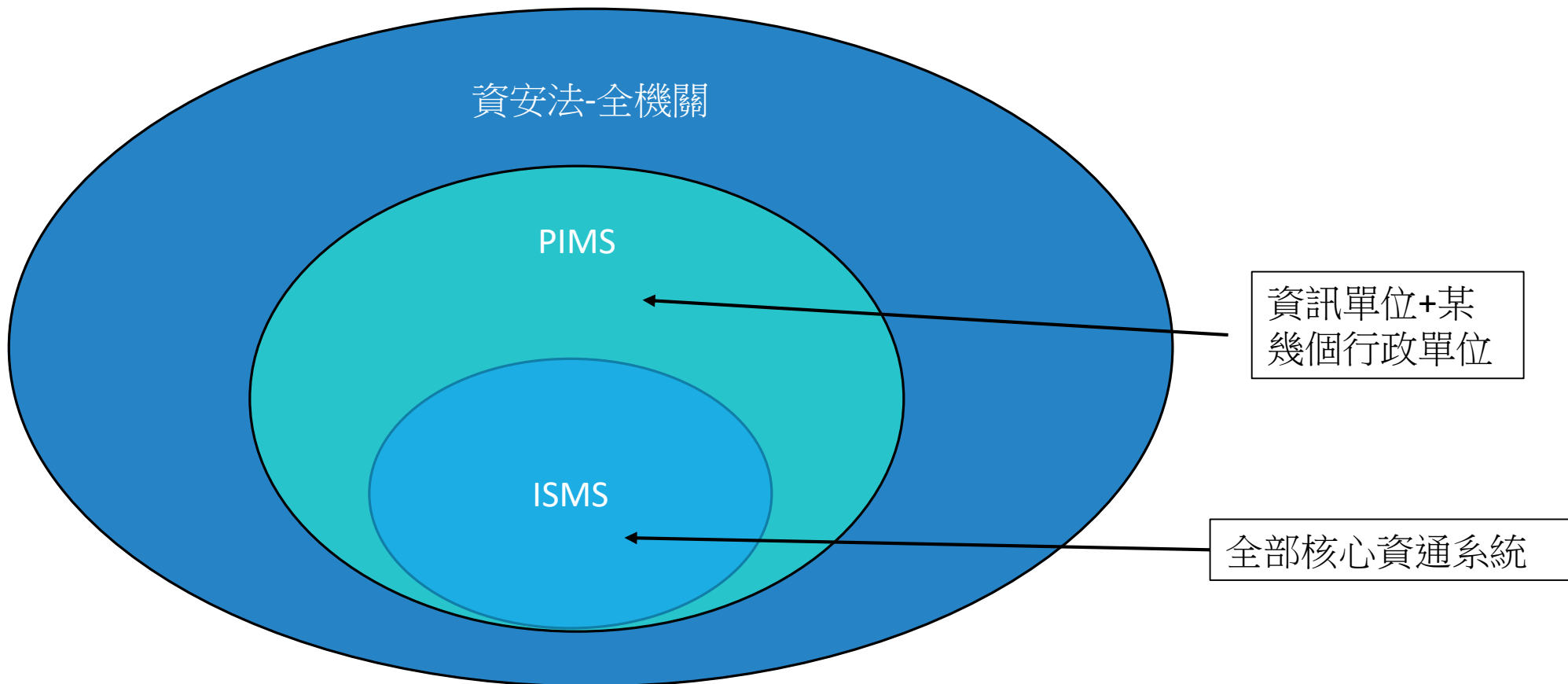
國立大專校院資通安全維護作業指引

護教職員生之權益，特訂定國立大專校院資通安全維護作業指引。

二、各校依資通安全管理法第 10 條訂定、修正及實施資通安全維護計畫，適用範圍應涵蓋全校各系、院、所教學單位及各行政單位（以下簡稱全校各單位），並應注意下列事項：

- （一）**資通安全長之配置**：各校置資通安全長，宜指派主任秘書以上人員兼任，以落實推動及監督校內資通安全相關事務。
- （二）**資通安全推動組織**：各校資通安全推動組織宜由資通安全長召集全校各單位主管或副主管組成，每年至少召開會議一次。

適用範圍-110



適用範圍-現象1

資通安全維護計畫

貳、適用範圍

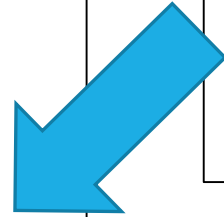
本計畫適用範圍涵蓋全機關。

捌、資通安全防護及控制措施
依ABC管理作業辦法之要求辦理。

ISMS管理文件 ABC管理作業辦法

X.適用範圍

資訊單位資訊作業。



資通安全責任等級分級辦法之應辦事項(A、B、C)
資訊安全管理系統之導入-全部核心資通系統導入??

適用範圍-現象2

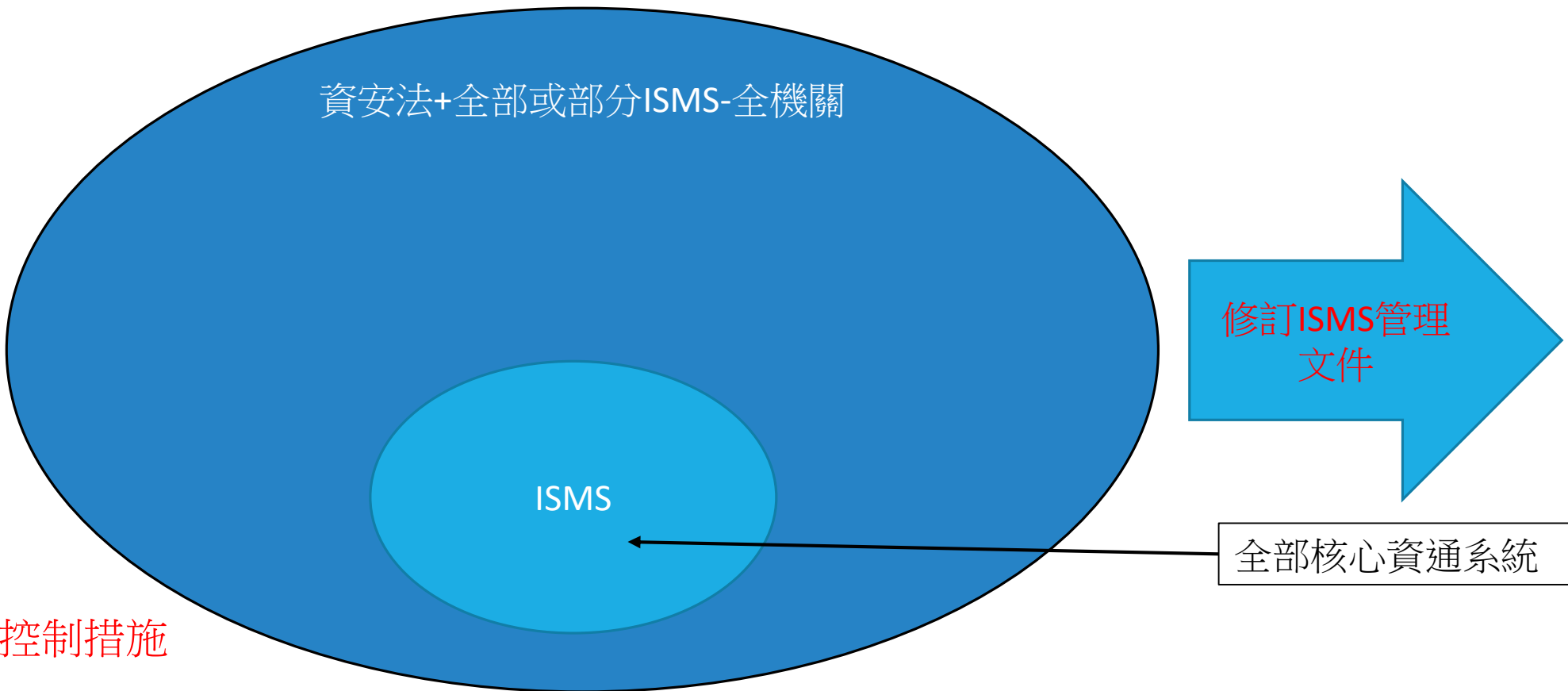
資安法+全部或部分ISMS-全機關

ISMS

修訂ISMS管理
文件

全部核心資通系統

推動組織
盤點
風險評鑑
資通安全防護及控制措施
內稽



WHAT & HOW

WHAT

法規、規定、要求、標準

HOW

符合、達成

WHAT

- 資通安全管理法 相關法規

<https://www-api.moda.gov.tw/File/Get/o39rMcG3VRjfhWz>

- 國立大專校院資通安全維護作業指引
- 臺灣學術網路各級學校資通安全通報應變作業程序
- 請持續加強辦理對外服務系統及網站導入安全傳輸協定(HTTPS)，依說明檢視網站內容(臺教資(五)字第1100059102號)
- 遠端維護資通系統，應採「原則禁止、例外允許」方式辦理(院臺護字第1100165761號)
- 行政院本（111）年8月資安警戒專案

等

機關內、外部利害關係人清單(2.7)

HOW-網路資源

- 行政院國家資通安全會報技術服務中心

<https://www.nccst.nat.gov.tw/>

- 校園資安輔導團-教育部國民及學前教育署

<https://www.k12ea.gov.tw/Tw/Rescue/Index?filter=c09bb778-3f97-4df0-9681-ffb1bbfc221d>

- 教育機構資安驗證中心ISCB

<https://iscb.nchu.edu.tw/>

行政院國家資通安全會報技術服務中心

<https://www.nccst.nat.gov.tw/>

Windows 7終止支援服務專區

<https://www.nccst.nat.gov.tw/Win7EndOfSupportIntro?lang=zh>

Windows 10 21H1版本 2022年底停止支援

校園資安輔導團-教育部國民及學前教育署

<https://www.k12ea.gov.tw/Tw/Rescue/Index?filter=c09bb778-3f97-4df0-9681-ffb1bbfc221d>

教育機構資安驗證中心

<https://iscb.nchu.edu.tw/>

教育部**111**年全國大專校院資安長會議

大專校院以全機關為範圍導入**ISMS**應優先落實的執行策略

<https://iscb.nchu.edu.tw/2021/12/isms.html>

<https://sites.google.com/email.nchu.edu.tw/ismsstrategy/>

<https://sites.google.com/email.nchu.edu.tw/nchu-isms/>首頁

教育部111至112年度對所屬公務機關及所管特定非公務機關資通安全稽核計畫

<https://iscb.nchu.edu.tw/2022/04/111112.html>

新版檢核表

HOME » »UNLABELLED » 「教育部111至112年度對所屬公務機關及所管特定非公務機關資通安全稽核計畫」公布新版檢核表



Tweet

「教育部111至112年度對所屬公務機關及所管特定非公務機關資通安全稽核計畫」公布新版檢核表

BY: ISCB POSTED DATE: 上午11:33:00 COMMENTS: 0

「教育部111至112年度對所屬公務機關及所管特定非公務機關資通安全稽核計畫」公文公布新版檢核表，教育機構驗證中心附上新版檢核表與舊版對照表予各單位參考

~~「教育部111至112年度對所屬公務機關及所管特定非公務機關資通安全稽核計畫」新版檢核表~~

「教育部111至112年度對所屬公務機關及所管特定非公務機關資通安全稽核計畫」新版檢核表與舊表檢核表對照
(111.06.07更新)

實地稽核_自評

<https://sites.google.com/email.nchu.edu.tw/nchu-isms/教育訓練/開放使用資安教材>



The screenshot shows a Google Docs form titled "實地稽核[資通系統防護基準]自評". The form contains the following fields: "電子郵件地址*", "填表人*", and "同時知會GMS窗口?". Each field has a small red asterisk icon to its left. The form is displayed on a mobile device screen.

實地稽核[資通系統防護基準]
自評



The screenshot shows a Google Docs form titled "實地稽核[資通安全稽核項目]自評". The form contains the following fields: "電子郵件地址*", "填表人*", and "同時知會GMS窗口?". Each field has a small red asterisk icon to its left. The form is displayed on a mobile device screen.

實地稽核[資通安全稽核項目]
自評

版面

資通安全專業證照(3.9)

<https://moda.gov.tw/ACS/laws/certificates/676>

111年修正資通安全專業證照認可審查作業流程及更新資通安全專業證照清單



為持續完善資通安全專業證照認可審查作業流程及資通安全專業證照清單，爰由本院資通安全處邀集相關學者專家共同檢討作業流程並更新證照清單。

請各機關依旨揭證照清單辦理資通安全責任等級分級辦法附表規定之機關人員取得資通安全專業證照事宜；本證照清單定期更新，各機關如有新增資通安全專業證照建議，請依資通安全專業證照認可審查作業流程辦理。

相關檔案

- ▶ 資通安全專業證照清單 (1110315修正) PDF
- ▶ 資通安全專業證照認可審查作業流程 (1110315修正) PDF
- ▶ 資通安全專業證照認可審查申請表 (1110315) ODT

檢核表

構面	稽核項目
策略面	1.核心業務及其重要性
	2.資通安全政策及推動組織
	3.專責人力及經費配置
管理面	4.資訊及資通系統盤點及風險評估
	5.資通系統或服務委外辦理之管理措施
	6.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
技術面	7.資通安全防護及控制措施
	8.資通系統發展及維護安全
	9.資通安全事件通報應變及情資評估因應

策略面

策略面-教育部111年全國大專校院資安長會議

<https://iscb.nchu.edu.tw/2022/09/111.html>

HOME > 公告事項 > 活動記錄 > 教育部111年全國大專校院資安長會議

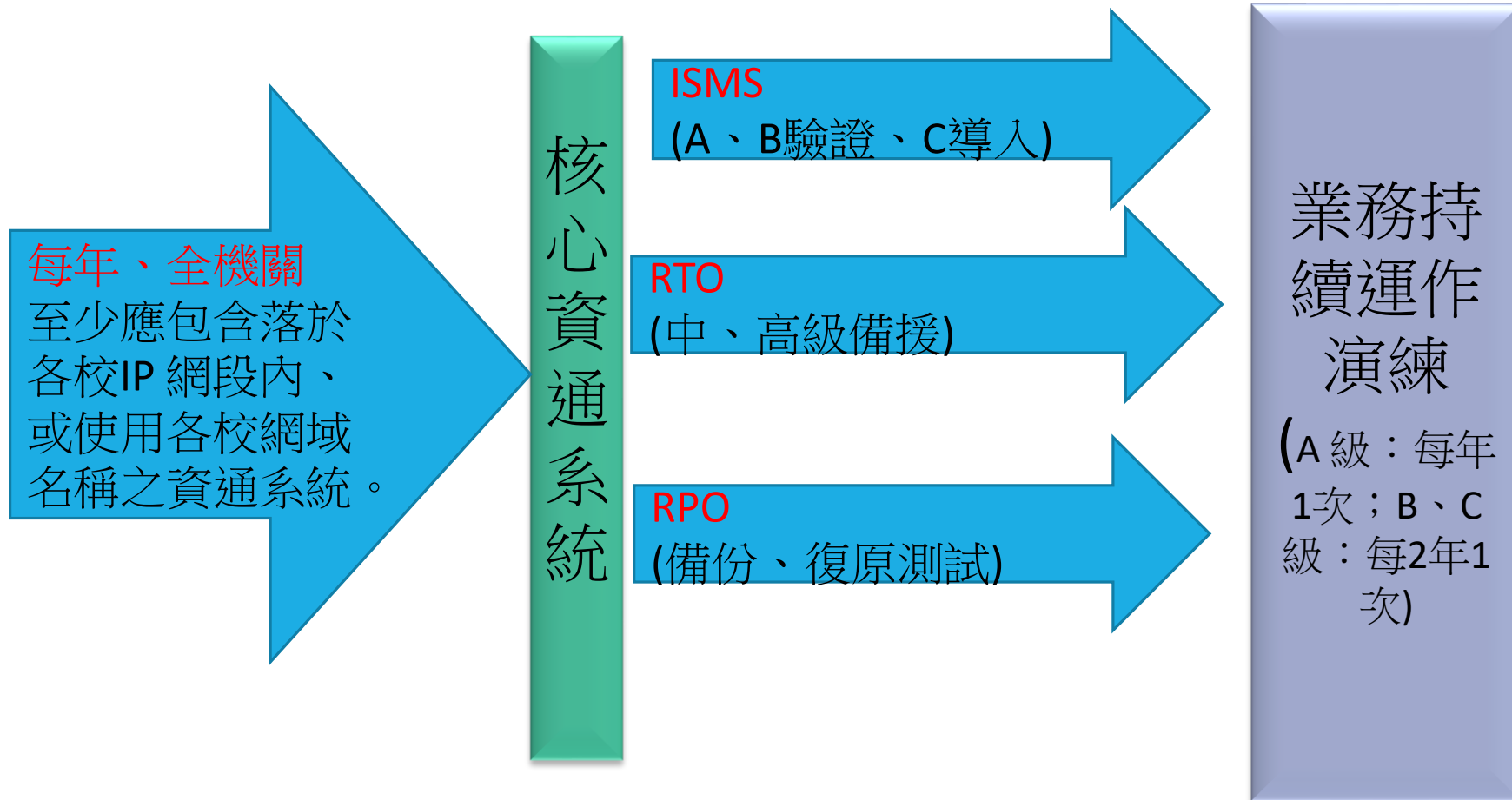
 教育部111年全國大專校院資安長會議

BY: ISCB POSTED DATE: 下午5:27:00 COMMENTS: 0

驗證中心將會議中報告事項剪輯成影片(驗證中心報告的部分)供各校參考·影片連結如下

興大 111年全國大專校院資...
111年全國大專校院資安長會議

資通系統之盤點及分級(1.1-1.7、4.1.1)



RTO(復原時間目標)

因為是VM所以很快?

機房淹水設備泡水?

問題

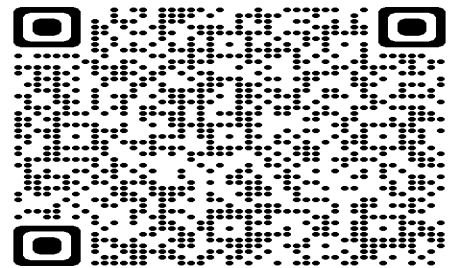
機關首頁主機硬碟嚴重毀損，更換硬碟後系統重建:

問題1.重建完成後，測試機關內外都無法讀取機關首頁，系統營運是不是完成復原?

答:是、不是

問題2.重建完成後，測試機關內可以讀取到機關首頁，機關外都無法讀取機關首頁，系統營運是不是完成復原?

答:是、不是



問題

機關因雷擊造成核心交換器與首頁主機嚴重損壞無法運作:

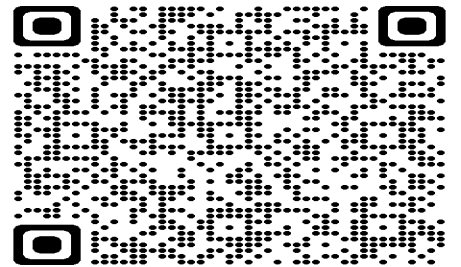
1.主機廠商於4小時支援備用機到場，並於2小時後恢復首頁服務

2.網路設備廠商於10小時支援備用機到場，並於1小時後恢復全機關及對外網路服務

問題1.機關首頁RTO 8小時，在本次事件中有沒有達到目標?

答案:

有、沒有



問題

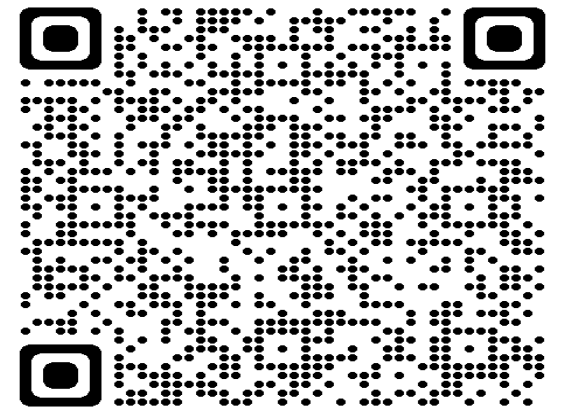
機關備份政策每日0時執行:

10/1 完整備份、10/2 差異備份、10/3 差異備份、10/4 差異備份、
10/5 差異備份、10/6 差異備份

問題1. 機關10/4下午13時整機毀損，請問資料復原下列何者正確?

答案:

1. 復原10/1
2. 復原10/1、10/2、10/3
3. 復原10/1、10/2、10/3、10/4



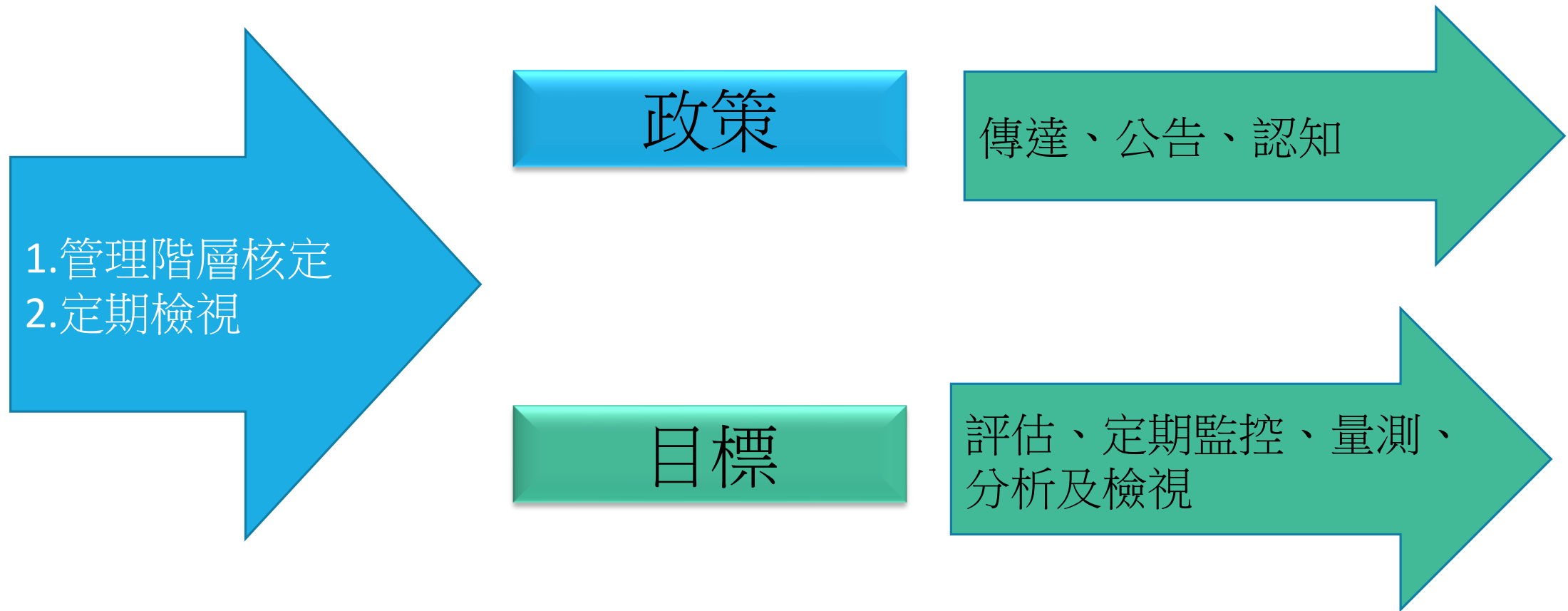
演練

- 情境全面規劃
- 環境因素演練(火、淹水、地震、停電等)
- 發現網頁遭竄改後**10分鐘內**切換為維護公告頁面

(111年全國大專校院資安長會議-簡報第13頁) <https://iscb.nchu.edu.tw/2022/09/111.html>

- 針對網頁**遭竄改**事件：
 - **備妥應變機制**。請各行政單位、系所**盤點所管網站**，**事先建立維護公告頁面及切換機制**，以利及時應變。(發現網站內容遭竄改後10分鐘內切換為維護公告頁面)
 - **「行政單位、系所網頁遭竄改」**應納入學校**業務持續運作演練(BCP)**演練情境，並請相關單位**實際演練緊急應變**作業程序。

資通安全政策(2.1、2.2)



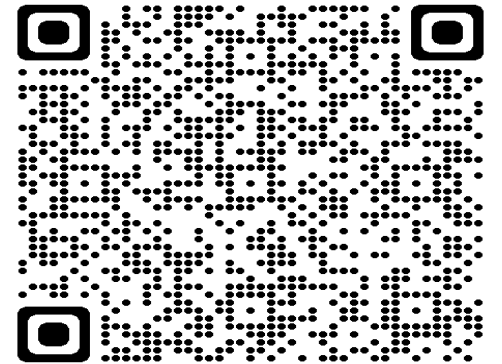
問題

問題1.各位知不知道機關資通安全政策在哪裡取得或查閱?

答案:知道、不知道

問題2.機關資通安全政策有沒有放置在對外公開網頁?

答案:有、沒有



政策與目標

- 全機關知道如何取得或查閱
- 對外公告(廠商知悉)
- 認知宣導

抽問機關人員

推動組織

- 資通安全長，宜指派主任秘書以上人員兼任。
- 成員全機關。
- 每年至少召開會議一次。
- 考核機制及獎懲基準。

<https://sites.google.com/email.nchu.edu.tw/isms-strategy/資安推動組織>

資通安全責任等級分級之應辦事項-資安專職人力及證照 (3.2-3.7)

<https://moda.gov.tw/ACS/laws/faq/03/636>

資通安全責任等級分級之應辦事項-資安專職人力及證照



資通安全管理法FAQ PDF

3.1. 何謂資通安全專職人員



3.2. 資安專職人員之職務內容為何？



3.3. 機關規模不大且沒有資訊單位，如何在短時間配置資通安全專職人員？



3.4. 資通安全專職人員是否要求要在資訊單位，或是否要求資訊職系？



3.5. 資通安全專職人力，如果分散在好幾人的身上，可以用 $0.5+0.5=1$ 的方式配置嗎？



3.6. 有關資通安全專業證照，所指由主管機關認可之資通安全證照，其清單在哪可取得？



一般人員教育訓練-通識教育訓練(3.8)

<https://sites.google.com/email.nchu.edu.tw/nchu-isms/教育訓練>



資安通識教育訓練

3.16. 資通安全專職人員以外之資訊人員、一般使用者及主管，每人每年需3小時之資通安全通識教育訓練，時數應如何取得？

1. 資通安全通識教育訓練時數，可透過以下方式取得：
- (1) 由機關自行辦理資通安全教育訓練。
 - (2) 至數位學習資源整合平臺「e等公務園+學習平臺」(<https://elearn.hrd.gov.tw>)線上修習包含資安管理制度、社交工程攻擊防護、個人資

資通安全管理法常見問題

依據行政院國家資通安全會報網站於109年11月24日公告之資通安全管理法常見問題，3.16說明資安通識教育訓練可由機關自行辦理，實體課程或數位課程均可。而所謂的一般使用者及主管，不僅機關編制內人員，亦須包含外聘

一般人員教育訓練-案例宣導(3.8)

<https://www.nccst.nat.gov.tw/Law?lang=zh>



https://www.nccst.nat.gov.tw/Law?lang=zh

法律彙編

考量資訊科技的蓬勃發展，資通安全威脅與相關議題日趨複雜、多元，本中心除針對我國資安法制及相關規範進行研議外，亦持續深入研究各項新興科技與應用之資安法制與政策議題。同時，為協助公務機關及各界瞭解資安法制議題之最新趨勢與管理作法，十餘年來，本中心持續蒐整國內外資安與資訊相關案例，並從法制與管理的角度，對案例進行分析，並提出因應建議與可行作法，供機關與各界參考。

請以左右鍵切換精選案例(最左邊)、自我評量(左邊)、評量解析(右邊)、下載專區(最右邊)之頁籤

精選案例 自我評量 評量解析 下載專區

類別：資訊保護【案號：S11011】國內某基金會個資外洩，影響2,000名考生

【焦點話題】

國內某政府捐助成立之基金會(下簡稱該基金會)針對111年度之新式學測辦理試辦考試，該試辦考試系統自110年4月1日上線，並自4月12日開始正式報名。該基金會於4月15日自行查知，其試辦考試報名系統之資料庫，遭駭客入侵，約有2,000筆學生報名資料(占報名總數2.67%)遭不明人士瀏覽，其發現後即通報權責機關，實施緊急應變措施，並進行系統調整與修補(系統邏輯之改善)，強化資通安全防護措施，亦已依個人資料保護法之規定通知相關當事人。全案並送司法機關調查中。該基金會另說明此試辦考試系統與110年度指定科目考試系統不同，並完全區隔，因此110年度指考報名系統並未受此次事件影響。

【參考資料來源：聯合報，110/6/2】

資通安全專業證照(3.9)

<https://moda.gov.tw/ACS/laws/certificates/676>

111年修正資通安全專業證照認可審查作業流程及更新資通安全專業證照清單



為持續完善資通安全專業證照認可審查作業流程及資通安全專業證照清單，爰由本院資通安全處邀集相關學者專家共同檢討作業流程並更新證照清單。

請各機關依旨揭證照清單辦理資通安全責任等級分級辦法附表規定之機關人員取得資通安全專業證照事宜；本證照清單定期更新，各機關如有新增資通安全專業證照建議，請依資通安全專業證照認可審查作業流程辦理。

相關檔案

- ▶ 資通安全專業證照清單 (1110315修正) PDF
- ▶ 資通安全專業證照認可審查作業流程 (1110315修正) PDF
- ▶ 資通安全專業證照認可審查申請表 (1110315) ODT

補充

3、4、5

管理面

資產盤點與風險評鑑(4)

- 每年、全機關
- 設備分級標示(7.25)
- 弱點掃描結果與風險評鑑關係

資訊資產管理

<https://sites.google.com/email.nchu.edu.tw/nchu-isms/資安文件/資安文件資訊資產管理>



資安管理

首頁 資安文件 教育訓練 系統檢測

資安文件(資訊資產管理)

資訊資產管理使用

資訊資產分類

1. **人員(People)**: 包含全體同仁, 以及委外廠商。
2. **文件(Document)**: 以紙本形式存在之文書資料、報表等相關資訊, 包含公文、列印之報表、表單、計畫等紙本文件。

資訊及系統使用

1. 使用資訊及資通系統前應經其**管理人授權**。
2. 使用資訊及資通系統時, 應留意其資通安全要求事項, 並負對應之責任。

資通系統風險評鑑參考指引

<https://www.nccst.nat.gov.tw/CommonSpecification?lang=zh>

資通系統防護基準驗證實務(V1.1)_1110928.rar

參考指引：

政府資訊作業委外資安參考指引v6.3_1110830.rar

資安治理成熟度評估參考指引v1.2_1110829.rar

政府機關雲端服務應用資安參考指引v1.2_1110817.rar

安全控制措施參考指引v4.0_1110131.rar

資通系統風險評鑑參考指引(修訂)v4.1_1101231.rar

網路架構規劃參考指引(修訂)v3.1_1101231.rar

Web應用程式安全參考指引(修訂)v2.1_1101231.rar

VPN安全參考指引(修訂)v2.2_1101231.rar

電子郵件安全參考指引(修訂)v3.1_1101231.rar

電子資料保護參考指引(修訂)v2.1_1101231.rar

防火牆建置資安參考指引(修訂)v3.0_1091015.rar

教育機構資安驗證中心-詳細風險評鑑

<https://sites.google.com/email.nchu.edu.tw/ssdlc/ra2>



Assessment 首頁 高階風險評鑑

資訊資產詳細風險評鑑

「教育機構資安驗證中心」基於協助教育體系加速將資安管理制度落實至全機關範圍，重新探究現有風險評鑑的普遍問題，著手設計下列「[資訊資產清冊](#)」、「[資訊資產威脅及弱點評估表](#)」、「[詳細風險評鑑彙整表](#)」及「[詳細風險評鑑相關程序參考條文](#)」，提供各界可依循的詳細風險評鑑執行方案。

 **查核資產清冊欄位到什麼程度呢？**
系統名稱、資產管理者、資產擁有者、存放位置...



委外辦理資通系統相關(5、8.8)

<https://moda.gov.tw/ACS/laws/guide/rules-guidelines/1355>

資通系統籌獲各階段資安強化措施



依據資通安全管理法(以下簡稱本法)第九條規定，公務機關或特定非公務機關於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。為協助公務機關及特定非公務機關於本法適用範圍內委外辦理相關作業，補充說明委託機關依本法施行細則第四條規定選任或監督受託者之相關行政流程及應注意事項，特訂定本措施。

相關檔案

- ▶ 資通系統籌獲各階段資安強化措施 (PDF)
- ▶ 附件1_廠商估價單_資安作業範例_ (ODT)
- ▶ 附件2_評選委員評選表_範例_ (ODT)
- ▶ 附件3_廠商資安管理作業自我評估表_範例_ (ODT)
- ▶ 附件4_資訊服務採購案之資安檢核事項 (PDF)
- ▶ 附件5_資料所在地及跨境傳輸切結書_範例_ (ODT)

NEW

5.5 是否依資通系統分級，於徵求建議書文件 (RFP) 相關採購文件中明確規範防護基準需求？

<https://moda.gov.tw/ACS/laws/guide/rules-guidelines/1331>

資訊服務採購案之資安檢核事項



為強化各機關資通訊相關採購案之資安防護，已依本院公共工程委員會公布之「投標須知範本(1090323修正)」及「資訊服務採購契約範本(1100409)」等採購文件制定「資通訊採購案之資安檢核事項」，請各機關於辦理資通訊採購案時參考上述檢核事項，並轉知採購單位配合辦理相關事項。

<https://www.nccst.nat.gov.tw/SecurityRFP?lang=zh>

政府機關資訊安全系統(TOPI)公正第三方驗證(TPI)報告

資通系統委外開發RFP範本(v3.0)

資通安全維護計畫(6.1)

資通安全管理法施行細則 第六條

- 一、核心業務及其重要性。
- 二、資通安全政策及目標。
- 三、資通安全推動組織。
- 四、專責人力及經費之配置。
- 五、公務機關資通安全長之配置。
- 六、資通系統及資訊之盤點，並標示核心資通系統及相關資產。
- 七、資通安全風險評估。
- 八、資通安全防護及控制措施。
- 九、資通安全事件通報、應變及演練相關機制。
- 十、資通安全情資之評估及因應機制。
- 十一、資通系統或服務委外辦理之管理措施。
- 十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制。
- 十三、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。

資通安全維護計畫(6.1)

- 定期檢視。
- 每年向上級或監督/主管機關提出資通安全維護計畫實施情形。

計畫內容沒有要變更，所以不用檢視？

計畫內容沒有要變更，不過有檢視但沒有檢視紀錄？

內部資通安全稽核計畫(6.3)

(A 級機關：每年2次；B 級機關：每年1次；C 級機關：每2年1次)

- 國立大專校院資通安全維護作業指引-稽核範圍應包含全校各單位。
- 分年分階段規劃辦理，並明訂於各校資通安全維護計畫。

<https://sites.google.com/email.nchu.edu.tw/isms-strategy/>內部稽核

歡迎使用教育機構資安驗證中心設計的檢核自評工具

問題

機關某教學單位，自建資通系統並對外服務:

機關於今年內部資通安全稽核時，稽核人員只針對該單位的行政人員個人電腦進行資安稽核，故未發現任何不符合事項?

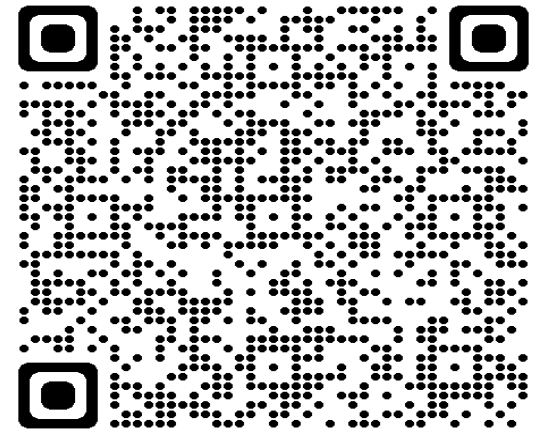
問題1.本次內部資通安全稽核事項，有沒有足夠或完整?

答案: 有，沒有

問題2.如果沒有完整的話，還缺什麼?

答案:

GOOGLE搜尋:個人資料保護 有效性量測表，確認算不算資安內稽?



採「原則禁止、例外允許」方式辦理(6.8)

- 開放機關內部同仁及委外廠商進行遠端維護資通系統。

確認相關申請與審核作業!

很久以前就開放了，如何處理?

核心系統主機，裝反向連結遠端管理!!!!

Google 搜尋原則禁止、例外允許

補充

6

技術面

網站安全弱點檢測(7.1)

(A 級機關：每年2次；B 級機關：每年1次；C 級機關：每2年1次)

https://download.nccst.nat.gov.tw/attachfilespmo/弱點掃描服務RFP範本v4.0_1100915.pdf

弱點掃描服務RFP範本 第2頁

Web 網頁弱點掃描
主機系統弱點掃描

修補紀錄



平台公告

日期	事項
2022-05-27	EVS平臺因掃描授權轉換，於2022/05/30 9點起暫停服務 預計5/31恢復服務，不便之處，敬請見諒!
2022-04-14	1. 檢測排程申請功能已恢復。 2. 每日新授權限額調整為6個。

資通安全健診(7.3)

(A 級機關：每年1次；B、C 級機關：每2年1次)

資通安全健診	網路架構檢視
	網路惡意活動 檢視
	使用者端電腦 惡意活動檢視
	伺服器主機惡 意活動檢視
	目錄伺服器設 定及防火牆連 線設定檢視

缺項?
沒有
目錄伺服器

資通安全健診

<https://moda.gov.tw/ACS/laws/faq/04/638>

4.6. 應辦事項列表的「資安健診」中「使用者端電腦惡意活動檢視」，請問有規定檢視的比例嗎？機關沒有那麼多經費可以檢視100%的電腦怎麼辦？



資通安全健診對於使用者端電腦惡意活動檢視並無明確比例之規定，原則上檢測範圍為全機關，機關如囿於經費，可將部分非從事核心業務之使用者電腦，分年完成使用者電腦檢測，惟檢測週期不宜逾2年。


另建議機關單位正副主管以上及機要人員、資訊單位同仁、委外廠商駐點人員、維護機關核心資通系統之承辦同仁等電腦，應加強檢測頻率，以利及早掌握資安威脅狀態。

日誌log(7.7)

<https://moda.gov.tw/ACS/laws/faq/04/638>

4.12. 分級辦法附表十所要求資通系統應保存日誌 log之項目為何？



包含但不限於資通系統伺服器日誌、資料庫日誌檔案及伺服器作業系統日誌等，以符合程式除錯、行為歸責、稽核取證及法律規範等用途。詳參技術服務中心網站發布之「資通系統防護基準驗證實務」2.2.1.記錄事件章節之內容 (<https://www.nccst.nat.gov.tw/CommonSpecification?lang=zh> )。

只保存登入成功的日誌符合規定嗎？

日誌log(7.8)

<https://www.nccst.nat.gov.tw/CommonSpecification?lang=zh>

資通系統防護基準驗證實務 第30頁

資通安全 責任等級	保存範圍	保存項目
A	機關應保存全部資通系統與各項資通及防護設備最近六個月之日誌紀錄。	1. 作業系統日誌(OS event log) 2. 網站日誌(web log) 3. 應用程式日誌(AP log) 4. 登入日誌(logon log)
B	機關應保存全部核心資通系統與相連之資通及防護設備最近六個月之日誌紀錄。	
C	機關應保存全部核心資通系統最近六個月之日誌紀錄。	

應定期審查機關所保留資通系統產生之日誌(中、高)

資通系統防護基準驗證實務 第35頁

佐證資料	<ul style="list-style-type: none">▪ 機關訂定之日誌相關管理辦法▪ 日誌審查紀錄
------	--

資通系統防護基準-稽核與可歸責性

Google Workspace

This Suspicious login alert is to inform you that Google has detected a suspicious login in your domain. Google considers login activity suspicious if we notice a sign in attempt that doesn't match a user's normal behavior, such as a sign in from an unusual location, or because we think an unauthorized person attempted to access a user's account.

The alert details include:

- User: [\[redacted\]@\[redacted\]](#)
- Attempted Login IP: 36.232.246.152

帳號

IP

成功登入

資通安全防護措施(7.11)

下列為本行目前實施之資通安全防護措施：

安全防護項目	A 級	B 級	C 級	D 級
防毒軟體	√	√	√	√
網路防火牆	√	√	√	√
電子郵件過濾機制	√	√	√	√
入侵偵測及防禦機制	√	√		
應用程式防火牆(具有對外服務之核心資通系統者)	√	√		
進階持續性威脅攻擊防禦	√			

資通安全防護措施(7.11)

相關指引

<https://www.nccst.nat.gov.tw/CommonSpecification?lang=zh>

A screenshot of a list of security reference guides. The text is blue and appears to be from a document or a list. The items are:

- 網路架構規劃參考指引(修訂)v3.1_1101231.rar
- Web應用程式安全參考指引(修訂)v2.1_1101231.rar
- VPN安全參考指引(修訂)v2.2_1101231.rar
- 電子郵件安全參考指引(修訂)v3.1_1101231.rar
- 電子資料保護參考指引(修訂)v2.1_1101231.rar
- 防火牆建置資安參考指引(修訂)v3.0_1091015.rar
- 入侵偵測與防禦系統建置資安參考指引(修訂)v2.0_1091015.rar
- 個人資料保護參考指引(修訂)v2.0_1051107.rar

帳號清查(7.13)

<http://nchu-iscb-casestudy.blogspot.com/2018/06/ISMS106TOP10LA1003.html>

- AD管控後本機帳號是否要清查?

網路安全(7.14-7.16)

<https://www.nccst.nat.gov.tw/CommonSpecification?lang=zh>

網路架構規劃參考指引

無線網路安全參考指引



資通系統風險評鑑參考指引(修訂)v4.1_1101231.rar
網路架構規劃參考指引(修訂)v3.1_1101231.rar
Web應用程式安全參考指引(修訂)v2.1_1101231.rar
VPN安全參考指引(修訂)v2.2_1101231.rar
電子郵件安全參考指引(修訂)v3.1_1101231.rar
電子資料保護參考指引(修訂)v2.1_1101231.rar
防火牆建置資安參考指引(修訂)v3.0_1091015.rar
入侵偵測與防禦系統建置資安參考指引(修訂)v2.0_1091015.rar
個人資料保護參考指引v2.0_1051107.rar
無線網路安全參考指引(修訂)v3.0_1050309.rar
政府行動化安全防護規劃報告v1.0_1031231.rar

電腦機房及重要區域之安全(7.20-7.22、7.25)

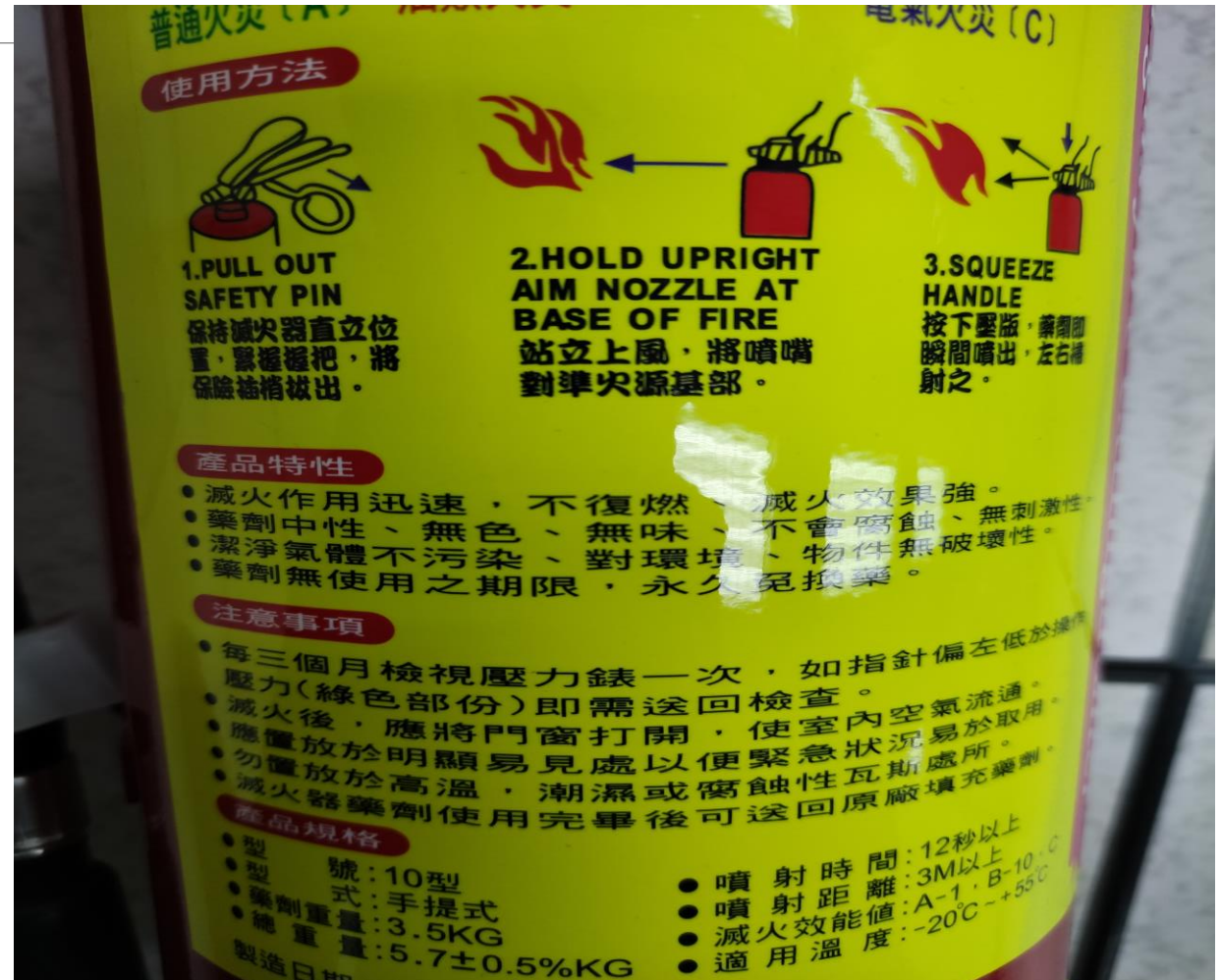
CNS27002或相關規範

- 進出管控、實體區隔、設備環境巡檢、溫溼度控制
- 危害因素(如火、煙、水、震動、化學效應、電力供應、電磁輻射或人為入侵破壞等)
- 設備分級標示
- 報廢程序

是否看過?

手提滅火器的注意事項:

緊急照明



問題

機關機房使用手提式滅火器，滅火器上貼有一張注意事項

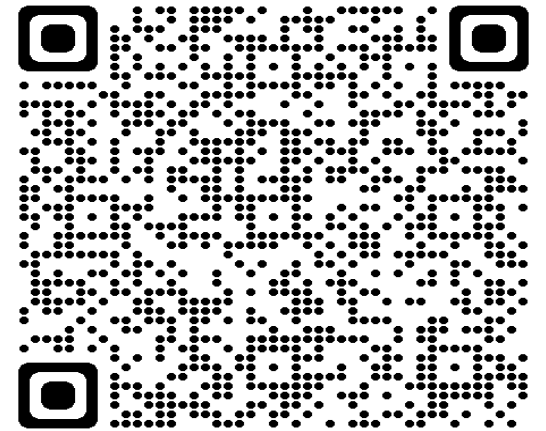
問題1.不依照注意事項檢查或維護有沒有風險?

答案:有、沒有

問題2.風險為何?

答案:

發現1支滅火器壓力為0



軟體安裝管控(7.27)

- 校園保護智慧財產權行動方案
- 授權軟體表列

國立陽明交通大學
校園授權軟體服務網
請尊重智慧財產權

[首頁](#) [最新消息](#) [下載](#) [安裝說明](#) [KMS認證](#) [常見問題](#) [授權軟體清單](#) [相關資源](#) [授權政策](#)

Windows	MacOS	Linux		
作業系統				
軟體名稱	32 bit	64 bit	中文版	英文版
Windows 11		◆	◆	◆
Windows 10	◆	◆	◆	◆
Windows 8.1	◆	◆	◆	◆
Windows 8	◆	◆	◆	◆
文書應用				
軟體名稱	32 bit	64 bit	中文版	英文版
Office Professional Plus 2019	◆	◆	◆	◆
Office Professional Plus 2016	◆	◆	◆	◆

問題

區分行動裝置及可攜式媒體:

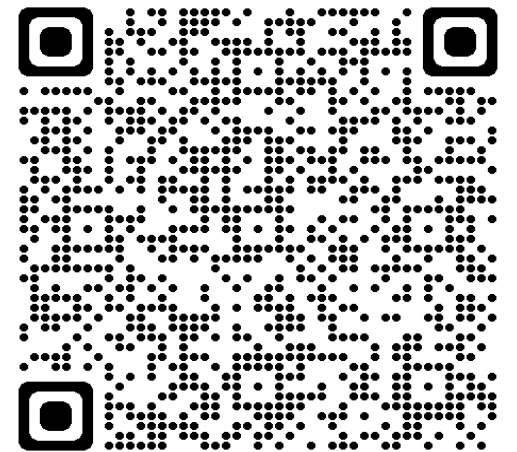
問題1.USB隨身碟、DVD光碟，是屬於下列哪一個?

答案: 1.行動裝置、2.可攜式媒體

問題2.手機、平板電腦，是屬於下列哪一個?

答案: 1.行動裝置、2.可攜式媒體

<https://reurl.cc/dWNWZ2>



行動裝置及可攜式媒體管理程序(7.28)

- 訂定管理程序
- 定期審查、監控及稽核

訂定網路即時通訊使用原則(7.29)

<https://sites.google.com/email.nchu.edu.tw/nchu-isms/教育訓練/即時通訊資安考量>

NEW 刪

https://sites.google.com/email.nchu.edu.tw/nchu-isms/教育訓練/即時通訊資安考量 90% ☆

首頁 資安文件

不應使用即時通訊軟體傳遞之資訊類型

- 依政府採購相關法規有保密必要者

- 決策形成前有保密必要者

機密性 No!

- 具名或具體內容之檢舉、陳情案件

- 調(檢)查或處理中有保密必要者

- 各項法規所列機密(保密)事項

- 為執行電腦系統安全管理相關作業事項

安全/隱私/敏感 No!

- 涉及隱私或個資

- 因承辦公務知悉或持有他人秘密

- 機關人事資料

- 其他非機密，若不當公開或外洩可能造成決策困擾、個人或機關信譽非必要損害等負面效應事項

資通系統防護基準(8.1)

- 資通安全責任等級分級辦法 附表十
- 資通系統防護基準驗證實務

<https://www.nccst.nat.gov.tw/CommonSpecification?lang=zh>

8

- 安全軟體測試參考指引
- 安全軟體設計參考指引
- 安全軟體發展流程指引
- 資通系統防護基準驗證實務(84頁)

<https://www.nccst.nat.gov.tw/CommonSpecification?lang=zh>

- 資通系統籌獲各階段資安強化措施

<https://moda.gov.tw/ACS/laws/guide/rules-guidelines/1355>

教育機構資安驗證中心-SSDLC

<https://sites.google.com/email.nchu.edu.tw/ssdlc/首頁>

SSDLC & Risk Assessment

首頁 高階風險評鑑 詳細風險評鑑

安全系統發展生命週期

系統防護需求 分級		高	中	普
		高	中	普
系統與 服務獲得	系統發展生命週期需求階段	針對系統安全需求（含機密性、可用性、完整性），以檢核表方式進行確認。		
	系統發展生命週期設計階段	一、根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。 二、將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。	無要求。	一、執行「源碼掃描」安
		一、應針對安全需求實作必要控制措施。		

SSDLC原則

在「[資通安全責任等級分級辦法](#)」附表十「[資通系統防護基準](#)」，要求落實「安全系統發展生命週期 (Secure Software Development Life Cycle, **SSDLC**)」，系統發展過程的需求、設計、開發、測試、部署維運等每個階段都應該納入必要的安全項目考量。

但是，這部分所提的**只是SSDLC原則**，像是需求階段應以檢核表確認安全需求、開發階段應針對安全需求實作必要控制措施、部署階段應針對資安威脅進行更新修補。但是，SSDLC如何更具體執行呢？

教育機構資安驗證中心-SSDLC教育訓練資料

<https://iscb.nchu.edu.tw/2022/04/ssdlc.html>



The screenshot shows a web browser window with the address bar displaying <https://iscb.nchu.edu.tw/2022/04/ssdlc.html>. The website header features the ISCB logo and the text "ISCB Information Security Certification Body". A navigation menu is visible on the left side. The main content area includes a breadcrumb trail: "HOME » 教育訓練 » SSDLC課程". Below this is the title "SSDLC課程" accompanied by the ISCB logo. The post information shows "BY: ISCB POSTED DATE: 下午5:05:00 COMMENTS: 0". The main text of the announcement states that the course has been moved online and provides contact information for inquiries. A list of details follows, including the course dates (April 20-21, 2022) and the purpose of the training.

HOME » 教育訓練 » SSDLC課程

 **SSDLC課程**

BY: ISCB POSTED DATE: 下午5:05:00 COMMENTS: 0

本課程已改為線上辦理，報名後會寄送網址，謝謝大家。
若沒收到視訊網址請來信詢問iscb@nchu.edu.tw

主旨：教育機構資安驗證中心於111年4月20日至21日辦理教育體系資安教育訓練課程，敬請派員參加，並准予公差假登記，請查照。

說明：

一、配合教育部協助教育體系各級學校有效推動資通安全與個人資料管理制度，驗證中心於111年4月20日至21日辦理資訊人員教育訓練課程，課綱如附件。

漏洞通報(7.14、8.5、8.12)

<https://www.nccst.nat.gov.tw/Vulnerability?lang=zh>

首頁 > 漏洞警訊公告

漏洞警訊公告

- 1 Sophos Firewall存在安全漏洞(CVE-2022-3236)，請儘速確認並進行更新
09/30/2022
- 2 Google Chrome、Microsoft Edge、Brave及Vivaldi瀏覽器存在高風險安全漏洞(CVE-2022-3075)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新
09/12/2022
- 3 VMware存在安全漏洞(CVE-2022-31656)，攻擊者可藉此取得管理員權限，請儘速確認並進行更新
08/08/2022
- 4 微軟支援診斷工具存在安全漏洞(CVE-2022-30190)，攻擊者可藉此遠端執行任意程式碼，請儘速確認並進行更新
06/20/2022
- 5 F5 Networks之BIG-IP產品存在高風險安全漏洞(CVE-2022-1388)，允許攻擊者繞過身分鑑別程序，進而遠端執行任意程式碼，請儘速確認並進行更新



最新消息

- 2022年9月27日 16:30 【漏洞預警】微軟緊急修補SCCM遭公開的漏洞
- 2022年9月26日 09:11 【攻擊預警】加密勒索軟體猖獗，請加強系統/應用程式更新與資料備份作業
- 2022年9月20日 13:54 【漏洞預警】Google、微軟分別修補已遭開採的瀏覽器零時差漏洞
- 2022年9月13日 11:57 【攻擊預警】QNAP 提醒用戶近期出現針對NAS 暴露外網並有安裝 Photo Station...
- 2022年9月13日 11:54 【漏洞預警】Google Chrome、Microsoft Edge、Brave及Vivald...

法規1

- 資通安全事件通報及應變辦法
- 資通安全情資分享辦法

資通安全事件通報窗口及聯繫方式

資通安全事件通報及應變辦法

公務機關:

第九條 公務機關應就資通安全事件之通報訂定作業規範，其內容應包括下列事項：

非公務機關:

第十五條 特定非公務機關應就資通安全事件之通報訂定作業規範，其內容應包括下列事項：

資通安全事件通報及應變管理程序範本

檔案下載-教育部國民及學前教育署 (k12ea.gov.tw)

<https://www.k12ea.gov.tw/Tw/Common/Download?filter=5D4EE052-4477-4756-A717-74F64C27ED66>

三、本校之資通安全事件通報窗口及聯繫專線為：↓

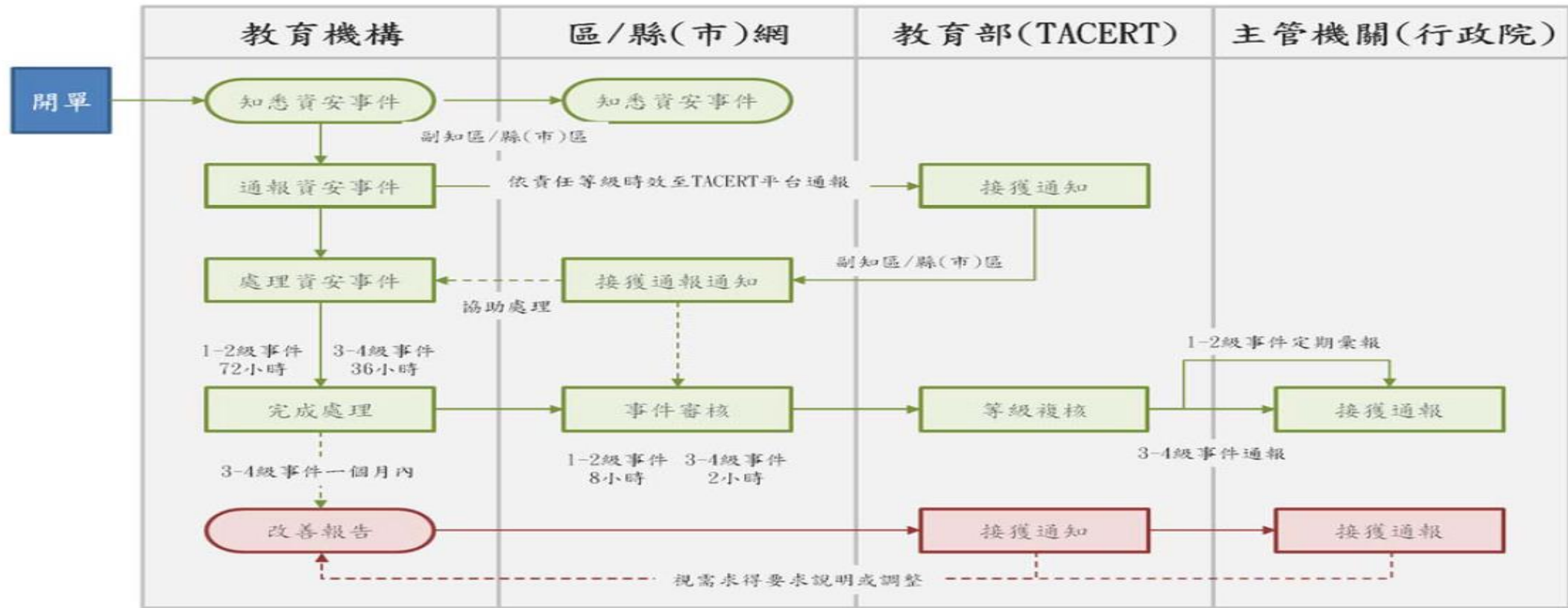
(一)聯絡電話：(99)999999#999↓

(二)聯絡單位：XXXXX↓

(三)聯絡人：XXXX↓

四、本校應以適當方式使相關人員明確知悉本機關之通報窗口及聯絡方式。↓

臺灣學術網路各級學校資通安全通報 應變作業程序



個資事件也要通報

圖二、各級學校通報及應變流程

臺灣學術網路各級學校資通安全通報 應變作業程序

第3章 通報作業

- 「2」、「1」級資安事件通報應變完成後，應至通報應變網站列印單件，**每月彙整送呈單位主管**；「4」、「3」級資安事件需於事件發生後**36**小時內，通報送陳單位資通安全長。
- 「4」、「3」級資安事件依本項規定完成損害控制或復原作業後，應持續進行資通安全事件之調查及處理，並於一個月內將調查、處理及改善報告函送本部，由本部彙送主管機關。

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？(9.9)

補充

7、8、9、10

感謝參與!!

Q&A