中華人民共和國香港特別行政區政府
保安局
關鍵基礎設施(電腦系統安全)專員辦公室

概述保護關鍵基礎設施(電腦系統)條例(香港法例第653章)

陳永安
關鍵基礎設施(電腦系統安全) 專員

2026.2.5

目錄

I.《條例》背景及規管範圍

立法目的

- 透過立法設定重要的基本要求，保障維持社會正常運作的關鍵基礎設施的電腦系統安全

- 減低必要服務因網絡攻擊被擾亂或破壞的可能，從而提升香港整體的電腦系統安全

立法原則

- 只涉及指定大型機構，不影響個人或中小企業
- 僅涵蓋香港辦事處的營運者，無域外效力
- 不針對個人資料 / 商業機密
- 以機構為單位，無個人刑責或監禁

其他司法管轄區的相關法例

內地	■ 網絡安全法 (2017) ■ 關鍵資訊基礎設施安全保護條例 (2021)
澳門	■ 網絡安全法 (2019)
英國	■ Network and Information Systems Regulations (2018)
澳洲	■ Security of Critical Infrastructure Act (2018)
加拿大	■ Critical Cyber Systems Protection Act (2025)
新加坡	■ Cybersecurity (Amendment) Act (2024)

兩類受規管的關鍵基礎設施

- 第一類 在香港提供必要服務的基礎設施

能源	銀行及金融服務	資訊科技
陸路運輸	八個界別	航空運輸
海上運輸	醫護服務	電訊及廣播服務

兩類受規管的關鍵基礎設施

- 第二類 維持重要的社會和經濟活動的基礎設施

例子

- 大型體育場地
- 大型表演場地
- 科研園區

規管涵蓋範圍

只監管被指明的**關鍵基礎設施營運者**和**關鍵電腦系統**

關鍵基礎設施營運者

- 採取「機構為本」的原則
- 會考慮該基礎設施有多依賴資訊科技運作、機構對基礎設施的控制程度
- 不涵蓋政府
- 不公開關鍵基礎設施營運者的名單

如何決定是否關鍵基礎設施?

- 若設施遭到破壞、喪失功能或數據泄漏時，對香港的必要服務或重要的社會和經濟活動影響
- 基礎設施提供的服務種類

如何決定是否關鍵基礎設施營運者?

- 設施核心功能，對電腦系統依賴程度
- 設施所控制的數碼資料的敏感性
- 機構對設施的運作及管理的控制程度

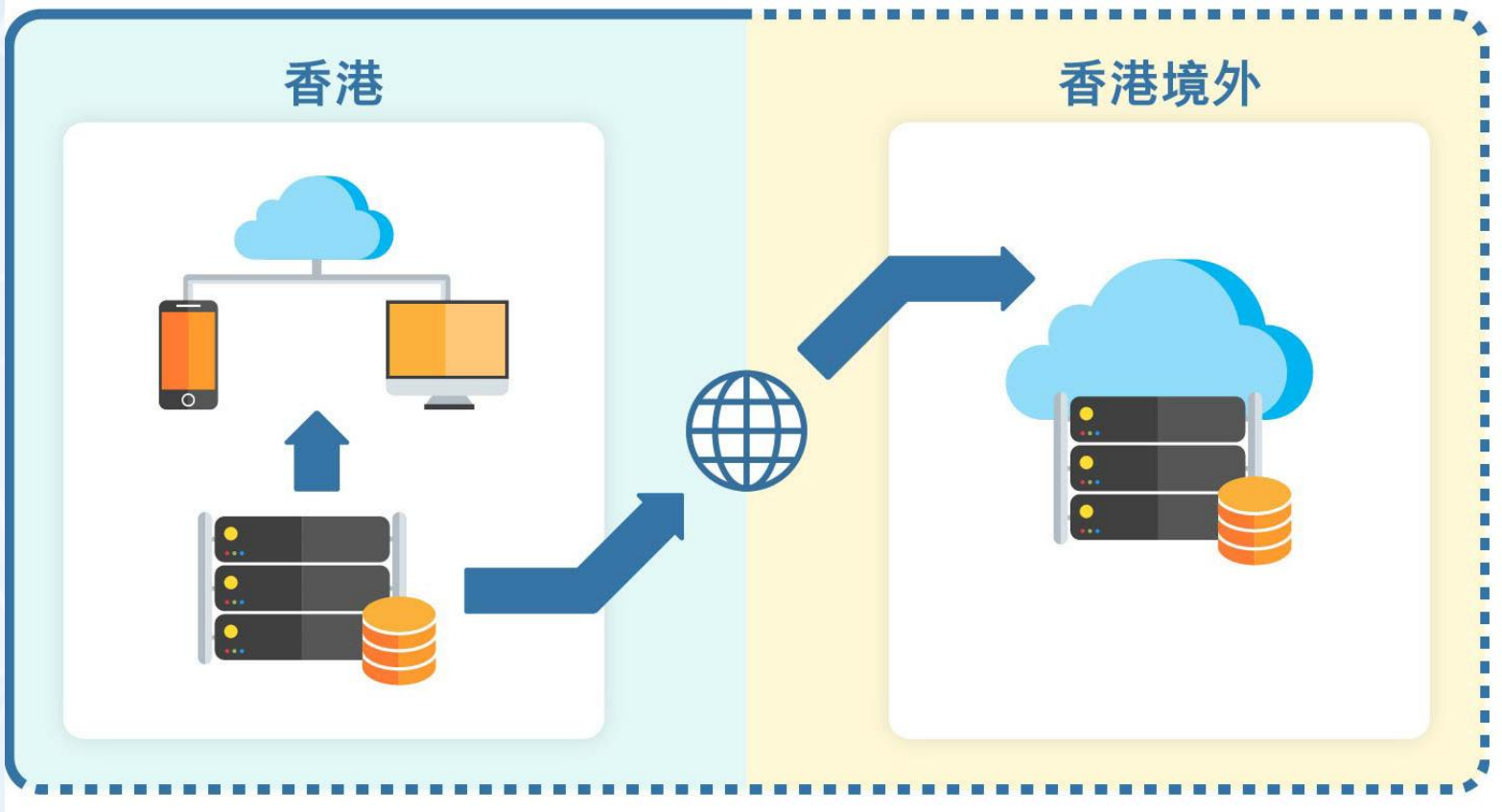
由於保安考慮，政府不公開關鍵基礎設施營運者的名單，但《條例》沒有禁止個別營運者自行公開其指定

如何決定是否關鍵電腦系統?

- 系統在核心功能方面擔任甚麼角色
- 如系統受到干擾或破壞時，核心功能會如何受影響
- 與營運者的其他電腦系統的相關程度
- 與其他營運者的電腦系統的相關程度

如何決定是否關鍵電腦系統?

- 營運者可否在香港或從香港接達



規管涵蓋範圍

例子

能源界別

關鍵基礎設施

關鍵基礎設施營運者

關鍵電腦系統

三類法定責任

架構責任

預防責任

事故通報及
應對責任

三類法定責任

I. 架構責任	目的
1. 在香港持續設有辦事處及提供通訊地址（指定後1個月內） 2. 通知變更通訊地址（變更後1個月內）	確保健全管理架構以執行必要的保護措施
3. 通知變更營運者（變更後1個月內）	
4. 設立和持續設有安全管理單位（指定後1個月內） 5. 委任具足夠知識的僱員監管該單位（指定後1個月內）	

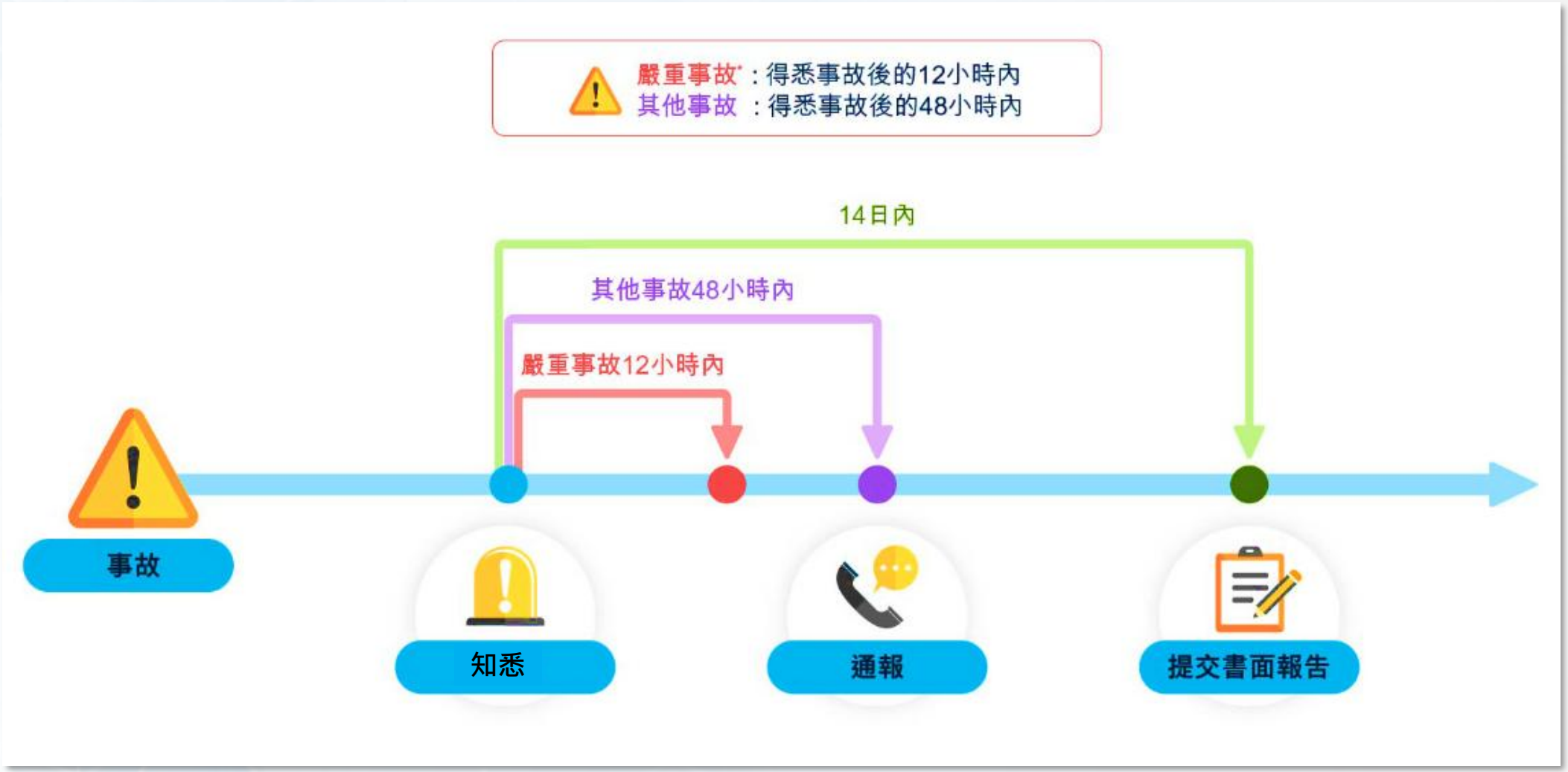
三類法定責任

II. 預防責任	目的
1. 通知有關關鍵電腦系統的重大變化（變更後1個月內）	確保採取必要措施防止遭受網路攻擊
2. 提交及實施安全管理計劃（指定後3個月內，修改後1個月內）	
3. 定期進行安全風險評估（每12個月至少1次，評估限期屆滿後3個月內提交報告）	
4. 定期進行獨立安全審核（每24個月至少1次，審核限期屆滿後3個月內提交報告）	

三類法定責任

III.事故通報及應對責任	目的
1. 定期參與安全演習（按專員辦公室書面通知）	確保營運者迅速應對事故和還原系統
2. 提交和實行應急計劃 （指定後3個月內，修改後1個月內）	
3. 指明限期內通知電腦系統安全事故，即事件涉及： ■ 無合法權限下接達該系統；或 ■ 任何其他在無合法權限下對或透過該系統（或另一系統）作出的作為；及 ■ 該事件對該系統的電腦安全，構成實際的不良影響	儘早採取行動防止進一步攻擊、堵塞系統漏洞及阻止攻擊擴散

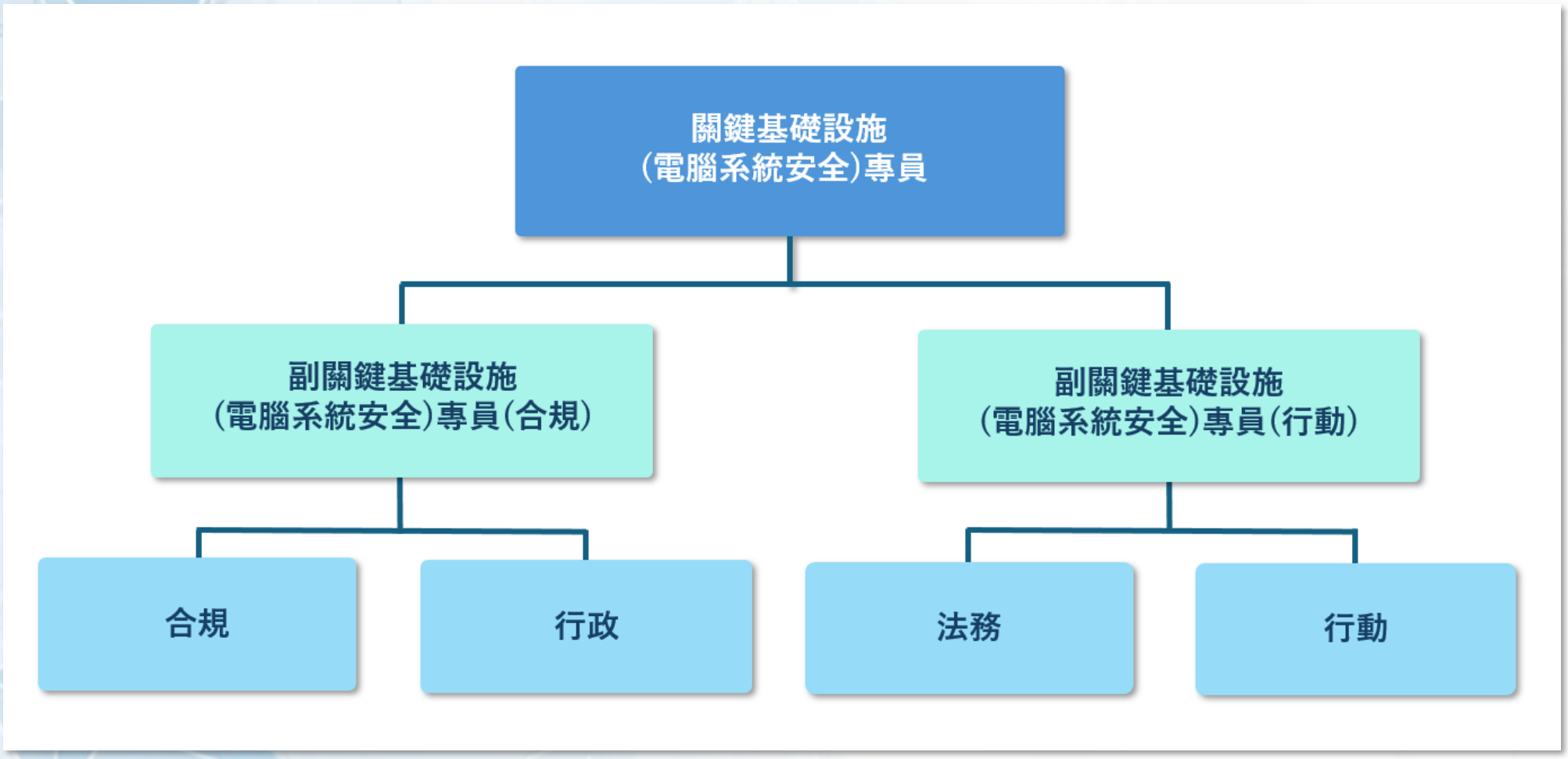
指定時間內報告電腦系統安全事故



II. 專員辦公室及指定當局

專員辦公室

- 由一名隸屬保安局的專員帶領來自數字政策辦公室和警務處的專家



專員辦公室

主要職能

- 指明**關鍵基礎設施營運者**及**關鍵電腦系統**
- 制定《**實務守則**》
- **監察**針對關鍵電腦系統的**保安威脅**

專員辦公室

主要職能

- **協助**營運者**應對**保安事故，包括可**主動調查**
- **協調政府部門**制定政策 / 指引和處理事故
- 向營運者**發出書面指示**，以堵塞潛在保安漏洞
- **調查**保安**事故**、**違規**及**罪行**
- 為履行職能，**要求提供資訊**並**採取必要措施**，必要時可**申請手令**

專員辦公室

應對電腦系統安全威脅及事故的職能

早期介入

- 如合理地懷疑有**某事件**發生，可**主動作出查訊** (提問問題/提交文件)
- 如營運者**不願意**或**未能採取合理步驟回應**及合乎**公眾利益**，向裁判官**申請手令**進入處所進行查訊

調查電腦系統安全威脅及事故

- 如合理地懷疑有**威脅或事故**發生，可**主動**對營運者作出**調查**及作出**應對**
- 如營運者**不願意**或**未能採取合理步驟回應**及合乎**公眾利益**，可：
  - 要求營運者採取補救措施 / 向人員提供協助等
  - 向裁判官**申請手令**，進入處所搜尋相關資料 / 檢查系統採取適當措施進行補救等，及要求**不屬被調查營運者的機構**協助調查或應對
- 如符合上述條件，但**取得手令並非合理地切實可行**，可授權人員在無手令下**緊急**進入處所調查

指定當局

- 個別行業已有法定行業監管機構，範疇亦涵蓋電腦安全，例如：

行業	指定當局
銀行和金融服務業	金融管理專員
電訊和廣播業	通訊事務管理局

- 指定當局規管行業營運者履行**架構**及**預防**責任

與指定當局的分工

	指定當局	專員辦公室
指明營運者/系統	其監管的營運者	其他營運者
I. 架構	其監管的營運者	其他營運者
II. 預防	其監管的營運者	其他營運者
III. 事故通報及應變		所有營運者

專員辦公室
指定當局

規管當局

規管當局 = **專員辦公室** + **指定當局**

- **一般權力（規管當局）**
  - **第1或2類責任**
    - 如營運者未有遵從／遵從上有欠妥之處，可發出書面指示
  - **第3類責任（專員辦公室）**
    - 如營運者未有遵從／遵從上有欠妥之處，可發出書面指示
- **發出《實務守則》**，就其負責類別的責任作出建議標準
  - 《實務守則》並非附屬法例
  - 無遵守《實務守則》本身不構成民事或刑事責任

III. 主要罪行、上訴機制及附屬法例

針對營運者的主要罪行

- 不履行法定責任
- 不遵從書面指示
- 不遵從按法定權力提出的要求
- 不遵從要求提供資料

視乎有否**盡一切努力**或作出**合理辯解**，經法庭審訊而定罪

針對營運者的主要罪行及罰則（詳列）

條	罪行	最高罰則
	未有在指明限期內：	
19	■ 在香港持續設有辦事處或就變更辦事處地址通知當局*	$ 50萬 (罪行持續期間每日另處罰款$5萬)
21	■ 設立或持續設有電腦系統安全管理單位；或 ■ 委任一名擁有足夠專業知識僱員，監管電腦系統安全管理單位	
22	■ 就某些電腦系統的重大變化通知當局*	
23	■ 提交電腦系統安全管理計劃（「計劃」）／經修改的計劃	
24	■ 進行電腦系統安全風險評估／提交該項評估報告	
25	■ 進行電腦系統安全審核／提交該項審核報告	
27	■ 提交應急計劃／提交經修改的應急計劃	
	無合理辯解而：	
42	■ 不遵從專員就應對電腦系統安全威脅及電腦系統安全事故，所施加的指明要求	$ 50萬
45	■ 不遵從規管當局就調查罪行所給予的指示或施加的要求	

*須以指明的格式及方式作通知，表格可在本辦公室網頁下載

針對營運者的主要罪行及罰則（詳列）

條	罪行	最高罰則
	未有：	
7	■ 遵從規管當局給予就遵從第1至3類責任上的指示	罰款 $ 500萬 (罪行持續期間每日另處罰款 $10萬)
18	■ 就確定關鍵基礎設施 / 指定營運者 / 指定關鍵電腦系統 / 了解潛在威脅或潛在事故向規管當局提交資料*	
20	■ 在指明限期內，就營運者變更通知當局*	
26	■ 遵從專員的書面通知參與電腦系統安全演習	
28	■ 在指明限期內，就電腦系統安全事故通知專員或提交書面報告*	
70	■ 遵從保安局局長就條例而訂立的規例	

*須以指明的格式及方式作通知，表格可在本辦公室網頁下載

上訴機制

由包括**法律專業、業界、電腦資訊保安**等專業人士組成委員會，處理就指明和書面指示的上訴

- 規管當局給予的書面指示（第7條）
- 被指定為關鍵基礎設施營運者（第 12 條）
- 被指定為關鍵電腦系統（第 13 條）等

附屬法例

賦權保安局局長在日後**補充、更新或修改**-

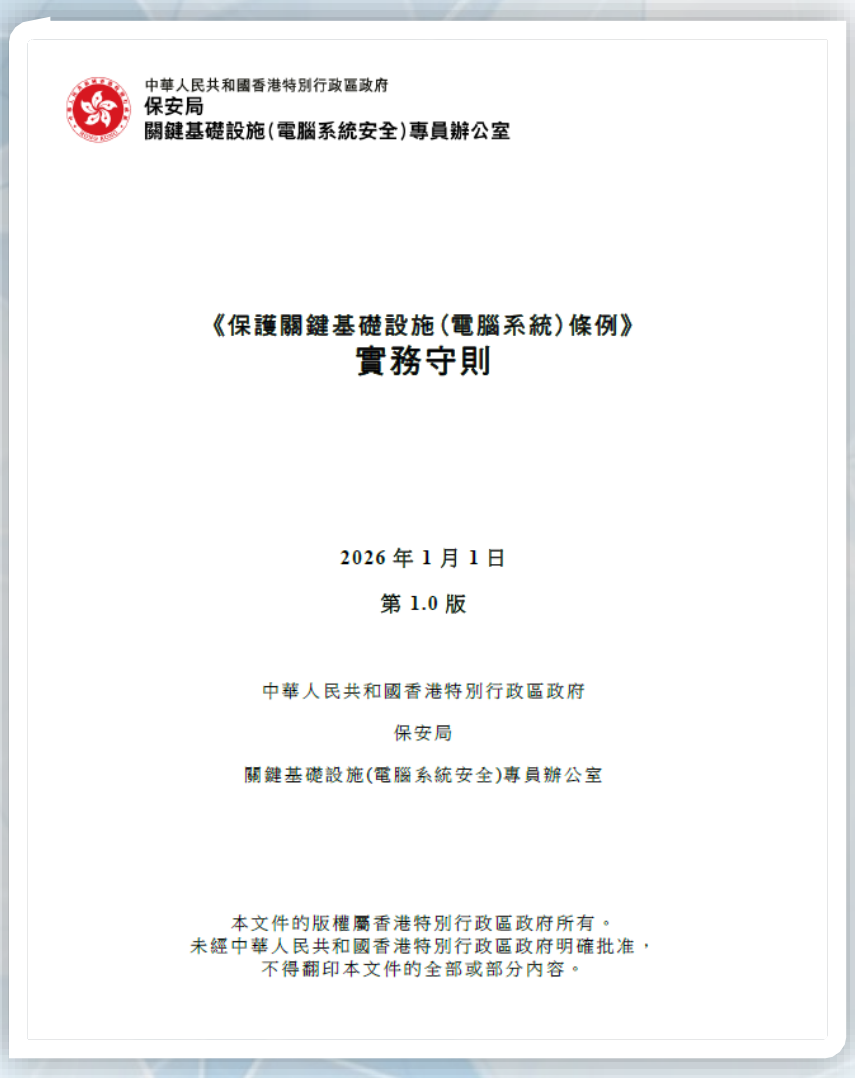
- 就專員辦公室權限
- 營運者法定責任
- 必要服務界別
- 指定當局名單等

營運者被指定後的工作

日期 / 期限	進程
通知	機構會收到規管當局的正式通知，說明指定的生效日期以及將被指定的關鍵電腦系統
生效日(“T”)	開始遵守本條例的生效日期
T +1 個月	通知規管當局在**香港的辦事處地址**及設立**電腦系統安全管理單位主管**
T+3 個月	提交**電腦系統安全管理計劃**及**應急計劃**
T+12 個月	進行**安全風險評估**
T+15 個月	提交**安全風險評估報告**
T+24 個月	進行**安全審核**
T+27 個月	提交**安全審核報告**

IX.《實務守則》

在法律程序中使用《實務守則》



中華人民共和國香港特別行政區政府
保安局
關鍵基礎設施(電腦系統安全)專員辦公室

《保護關鍵基礎設施(電腦系統)條例》
實務守則

2026 年 1 月 1 日

第 1.0 版

中華人民共和國香港特別行政區政府

保安局

關鍵基礎設施(電腦系統安全)專員辦公室

- 沒有遵守《守則》的任何條文，**本身並不構成任何罪行**
- 然而，如在法律程序中，法院／上訴委員會信納，《守則》關乎受爭議的事宜的裁斷，則 —
  - 《守則》可獲接納為證據；及
  - 關於該營運者違反／沒有違反該《守則》的有關條文的證明，可由任何一方援引

《實務守則》的標準

- 首套**「香港製造」**業界通用電腦系統安全標準
- 包含超過**200個要求**，涵蓋**治理**、**風險管理**、**保護**、**監測**、**應對及復原**
- 絕大部分都可以對標**國家標準**（國標）、**國際標準**，包括ISO 27000系列、IEC 62443、NIST網絡安全框架及**業界標準**（如銀行界別 C-RAF 2.0）
- 目前為個別業界制定界別適用《實務守則》
- 未來將不時檢視及更新《實務守則》

《實務守則》重點覆蓋範圍

治理

- 安全管理單位
- 政策、標準及指引
- 電腦系統安全培訓

風險管理

- 風險管理方法
- 設計層面保安 (Security-by-Design)
- 資產管理

《實務守則》重點覆蓋範圍

保護

- 接達控制及帳戶管理
- 特權接達管理
- 加密方法 / 密碼管理
- 配置管理及系統強化
- 變更管理
- 修補程式管理
- 儲存媒體 / 備份及復原
- 遠程連接
- 實體 / 網絡保安
- 應用系統保安
- 雲端運算保安
- 供應鏈管理

《實務守則》重點覆蓋範圍

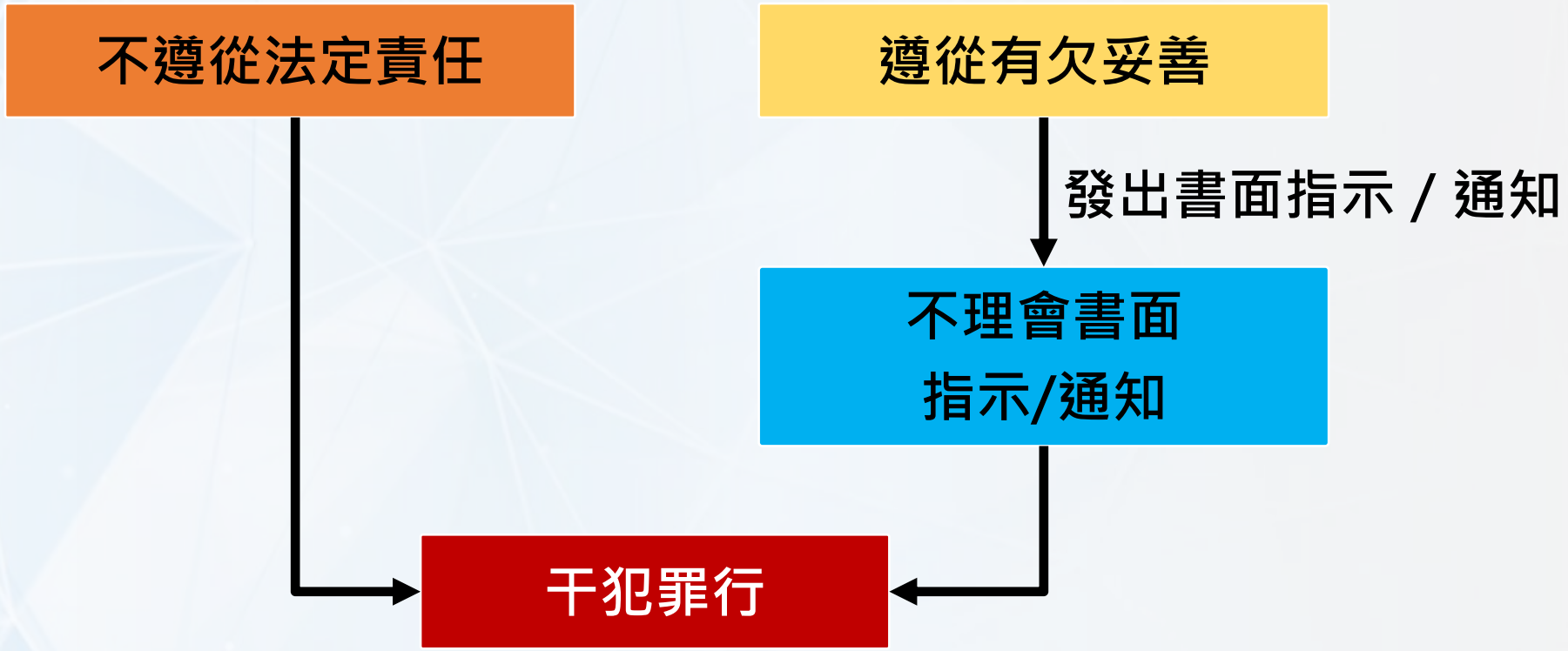
監測

- 記錄管理
- 監察及偵測

應對及復原

- 備份及復原
- 事故管理
- 業務持續運作管理
- 災後復原計劃

未能履行責任／不符合《實務守則》的要求，會犯法嗎？



V. 合規部門常見問題

第三方 / 境外服務供應商（外判商）

外判商是否需要間接承擔法定責任？

- 營運者可以外判工作，但不能外判責任
- 需要透過合約條款管理外判商，以確保遵從法定責任

如外判商拒絕提供資料，會否導致營運者會干犯法例？

- 營運者須按當局要求提交其在香港或從香港可以取得的資料
- 營運者就沒有遵從法定責任或規管當局的書面指示的罪行，可以提出「已盡應盡的努力」為免責辯護

事故通報

需要通報的例子

- 分布式阻斷服務攻擊
- 勒索軟件攻擊
- 感染惡意軟件或透過保安漏洞，導致系統與外部產生非預期的連接
- 僱員接達關鍵電腦系統，並惡意泄漏敏感資料
- 關鍵電腦系統被惡意負載或編碼修改
- 僱員濫用職權干擾關鍵電腦系統的運作

不需要通報的例子

- 純技術故障、天災、大規模停電、已被偵測和及時移除或隔離的電腦系統安全威脅或因人為錯誤而導致個人資料外泄

事故通報

嚴重事故的例子

- 核心功能停止運作時間，超過由營運者界定的最大可容忍停止運作時間
- 服務表現已低於由營運者界定的最低水平
- 已啓動業務持續運作或災後復原程序
- 已導致或相當可能導致大量客戶資料外泄
- 已泄漏或相當可能泄漏敏感數碼資料
- 遭威脅將於指定時間對關鍵電腦系統發動攻擊

事故通報

向警方或其他單位通報的責任

- 營運者仍需要根據其他法例或行業監管要求等向相關單位作出通報
- 如涉及刑事成份，營運者應報警求助

更多資訊

網址: www.occics.gov.hk

攜手合作

提升香港的整體電腦安全