2024 年 10 月 8 日
資料文件

立法會保安事務委員會
加強保護關鍵基礎設施電腦系統安全 — 建議立法框架
諮詢報告

目的

保安局於 2024 年 7 月 2 日就「加強保護關鍵基礎設施電腦系統安全—建議立法框架」展開為期一個月的諮詢工作，諮詢期至 2024 年 8 月 1 日止。本文件旨在向委員簡介諮詢的結果及闡述政府就推展相關立法工作的未來路向。

立法背景

2. 隨著資訊和通訊技術的快速發展，關鍵基礎設施的運作越發依賴電腦系統的安全及暢順運作，同時亦面對日益增加的網絡攻擊風險。一旦關鍵基礎設施的電腦系統受到擾亂或破壞，不能正常運作，會影響設施所提供的必要服務，甚或產生連鎖效應影響整個社會，嚴重危害社會經濟、民生、公共安全以至國家安全。

3. 近年，保障關鍵基礎設施電腦系統安全的法規在其他司法管轄區越見普遍，中國內地、澳門特別行政區、澳洲、歐盟、新加坡、英國和美國等地都已訂立類似法例，加拿大國會亦正在審議相關法案。

4. 行政長官在 2022 年 10 月發表的《施政報告》宣布，會立法提升關鍵基礎設施的網絡安全。考慮到香港的情況，參考了其他司法管轄區的做法（見第 3 段）和最新國際標準，保安局著手擬備一條全新的法例，以加強關鍵基礎設施的電腦系統的保安能力，從而提升香港整體的電腦系統安全。擬議條例暫名為《保障關鍵基礎設施（電

腦系統）條例草案》（下稱「擬議條例」）。

5 由於擬議條例主要影響有機會被指明為關鍵基礎設施營運者的機構、網絡保安服務供應商和審計公司及行業監管機構，我們在展開正式諮詢前已與這些持份者展開前期討論，以期吸納他們的意見擬備建議立法框架。

與持份者的前期討論

6. 自 2023 年起，保安局舉辦了超過 15 場前期討論會議，聆聽持份者就初步建議立法框架的意見。超過 115 位應邀的持份者一致原則上支持立法，認同維護電腦系統安全是社會各界的共同責任。

諮詢工作

7. 保安局於 2024 年 7 月 2 日就「加強保護關鍵基礎設施電腦系統安全—建議立法框架」的討論文件（**附件一**），諮詢立法會保安事務委員會，獲得委員一致原則上支持，並於同日展開為期一個月的諮詢。立法建議概述如下：

(a) 考慮到保護關鍵基礎設施電腦系統安全的必要性、立法目的和原則，建議只有被明確指明為「關鍵基礎設施營運者」及「關鍵電腦系統」才會被納入監管範圍，需要承擔法定責任；

(b) 擬議條例所規管的範疇，包括在香港提供必要服務的基礎設施，或其他維持重要的社會和經濟活動的基礎設施；

(c) 就「關鍵基礎設施營運者」在架構、預防和事故通報及應對責任方面訂立要求；

(d) 建議成立專責辦公室，由行政長官委任的一名專

員帶領，負責執行法例；

(e) 引入行業監管機構成為「指定監管機構」，負責監管其界別內的「關鍵基礎設施營運者」，履行架構和預防責任；

(f) 以「機構為本」為原則，訂立相關罪行和處以罰款的罰則；

(g) 成立上訴委員會處理「關鍵基礎設施營運者」就不同意專責辦公室的指明或書面指示時所提出的上訴事宜；

(h) 建議賦權保安局局長可透過訂立附屬法例，訂明或修訂可被指明為關鍵基礎設施的服務界別、指定監管機構名單、需要向專責辦公室報告的重大變化和事故的類型等；以及

(i) 參考國際認可方法和標準制定《實務守則》，列出各項法定責任的建議標準及涵蓋範圍，包括獨立電腦系統保安審計、風險評估報告等。

8. 保安局亦設立了**專屬網頁**，以常見問題和一圖盡覽的形式介紹建議立法框架，並上載其他司法區相關法例，方便公眾了解擬議條例的內容。

（一）諮詢會

9. 在諮詢期間，保安局為業界舉辦了**五場諮詢會**，解說擬議條例的重點內容。**諮詢會**共有近 200 名持份者出席，包括有機會被指明為「關鍵基礎設施營運者」的機構、網絡保安服務供應商及審計服務公司，其中兩場也邀請了條例建議的「指定監管機構」，即香港金融管理局和通訊事務管理局的代表出席。與會期間，持份者踴躍提出建設性問題及意見，保安局和指定監管機構的代表亦積極回應。五場諮詢會收集到的意見歸納如下，建議擬議條

例應：

(a) 清晰解說「關鍵基礎設施營運者」及「關鍵電腦系統」的定義和列明「關鍵電腦系統」出現重大變更時必須向專責辦公室匯報的資料；

(b) 列明「關鍵基礎設施營運者」設立的電腦系統安全管理部門的職能；

(c) 詳細解說何謂「嚴重電腦系統保安事故」、「其他電腦系統保安事故」及「嚴重資料洩露」；

(d) 細化在得悉電腦系統保安事故後須在指定時限通報的法定責任中，有關「得悉」的定義；

(e) 釐清「關鍵基礎設施營運者」在聘用第三方服務時，在合規方面所需要承擔的法定責任；

(f) 簡化受指定監管機構規管的「關鍵基礎設施營運者」在履行擬議條例下法定責任的程序，避免不必要增加成本及重複工作；及

(g) 列明「關鍵基礎設施營運者」須向專責辦公室提交資料的類型、模式及保密配套。

（二）書面意見

10. 在諮詢期內（即截至8月1日），保安局透過電郵和郵寄方式共收到53份意見書。當中，有52份意見（佔總數98.1%）支持立法及草案框架內容或提出正面建議，而來自業界的47份意見則百分百支持立法或提出正面建議，唯一反對意見是來自一個英國註冊的人權組織，該建議書就保障言論自由、專責辦公室權限、指明界別等提出反對，保安局已對此即時作出反駁，釐清謬誤。其他所收到的意見涵蓋立法建議的不同範疇，為制定擬議條例提供寶貴的參考。

（三）書面意見數據分析

11. 書面意見來自以下類別：

提交意見人士類別			數目
(a)	**有機會被指明為「關鍵基礎設施營運者」的機構**		
	第一類	能源	3
		銀行和金融服務	5
		陸上交通	1
		航空交通	3
		醫療保健	2
		通訊和廣播	7
	第二類	科研園區	3
		展覽場地	2
		體育場地	1
	(a)類別小計(佔整體比例)		**27 (50.9%)**
(b)	**政黨及立法會議員**		**2 (3.8%)**
(c)	**行業專業團體、專業學會、公會、商會**		
	資訊科技界		8
	通訊界		1
	工程界		1
	銀行界		1
	商界		2
	(c)類別小計(佔整體比例)		**13 (24.5%)**
(d)	網絡保安服務供應商		4
	資訊科技審計公司		1
	法定機構		2
	(d)類別小計(佔整體比例)		**7 (13.2%)**
(e)	未能歸類的公眾人士		3 (5.7%)
(f)	外國人權組織及其他		1 (1.9%)
總計(佔整體比例)			**53 (100%)**

（四）書面意見內容總覽

12. 我們統整了上述所收到的意見和建議，把有關主要意見及建議的摘要及相關備註，詳載於**附件二**，並重點歸納在以下第 13 至 25 段。

A. 立法目的和原則：

13. 我們共收到 57 項意見就立法及相關原則提出意見。重點意見如下：

> 整體支持政府就保護香港的關鍵基礎設施立法或為完善擬議條例內容或提出正面建議，認同「關鍵基礎設施營運者」須承擔及履行法定責任。
>
> 〔**註**：我們感謝界別持份者提出寶貴意見和專業建議，所有建議均會被慎重考慮。政府會繼續與各界別的持份者保持溝通，持續完善法律框架和《實務守則》內容。〕

B. 規管範疇

14. 我們共收到 31 項意見、建議或詢問。主要意見認為應該對資訊科技界別有清晰的定義、建議延伸至其他界別及移除域外司法權。重點意見如下：

(a) 擬議條例所規管的範疇包括在香港提供必要服務的基礎設施（即能源、資訊科技、銀行和金融服務、陸上交通、航空交通、海運、醫療保健及通訊和廣播八個界別），或其他維持重要的社會和經濟活動的基礎設施（例如大型體育及表演場地、科研園區等）。有意見認為不同界別的關鍵基礎設施的運作均會涉及資訊科技，故此期望對個別營運者是否屬於「資訊科技」界別，有更清晰的準則。

〔**註**：保安局參考了其他司法管轄區（包括美國、澳洲、新加坡、內地）的相關條例，認為把「資訊科技」列作其中一個關鍵基礎設施的界別，做法合適。至於個別機構及其營運者是否需要納入「資訊科技」界別，保安局將會以定義為基礎，與界別有機會被指明的營運者保持緊密溝通，方會作出決定。〕

(b) 擬議條例賦權專責辦公室在調查事故或與「關鍵基礎設施營運者」法定責任相關的罪行時可要求「關鍵基礎設施營運者」提交其可取得的相關資料，即使該等資料位於香港境外。有意見擔心擬議條例或涉及對境外的電腦系統進行執法。

〔**註**：擬議條例不具域外效力。專責辦公室會確認所要求的資料，均為在香港設有辦公室的營運者可以取得的資料，並給予合理時間準備。〕

C. 規管對象

15. 我們共收到74項意見、建議或詢問。主要意見認為「關鍵基礎設施」、「關鍵基礎設施營運者」和「關鍵電腦系統」應有清晰的定義、條件和範圍，以評估是否需要開展準備工作。重點意見如下：

(a) 擬議條例下，只有直接與提供必要服務有關或關乎關鍵基礎設施核心功能的電腦系統，以及如受到干擾或破壞會嚴重影響設施正常運作的系統才會被指明為「關鍵基礎設施營運者」和「關鍵電腦系統」。有建議認為應加入其他會被考慮的因素，例如可量化的指標，以確保客觀標準。

〔**註**：專責辦公室在指明「關鍵基礎設施營運者」和「關鍵電腦系統」時，將會以定義為基礎，並透過與營運者相互溝通及了解，考慮其他相關因素，以確定是否適合。〕

(b) 有意見認為在考慮指明「關鍵電腦系統」時，若基於關聯（interconnected）系統可能因為喪失功能而影響營運者提供必要服務而一併被指明，範圍將會太廣。

〔**註**：擬議條例有關「關鍵電腦系統」的定義是考慮到香港的情況及參考了其他司法管轄區的相關法律後制定的。因此，我們認為現時的定義是合適的。專責辦公室將按定義及與營運者充分溝通，經通盤考慮後方會指明營運者賴以提供必要服務的電腦系統為「關鍵電腦系統」。然而，由於「關連」（interconnected）此詞彙可能未必精準反映「關鍵電腦系統」的考慮因素，保安局會積極考慮予以刪除。〕

D.「關鍵基礎設施營運者」的責任

I. 架構責任

16. 我們共收到 36 項意見、建議或詢問。主要意見表達及時匯報變更「擁有權」可能有實際困難、建議釐清經營權的定義，以及如何善用資源設立電腦系統安全管理部門。重點意見如下：

(a) 擬議條例下，我們原本建議「關鍵基礎設施營運者」須報告有關關鍵基礎設施「擁有權」的變更。有意見反映機構（尤其是上市公司）難以就「擁有權」變更經常向專責辦公室作出報告。

〔**註**：保安局理解營運者在通報「擁有權」變更時可能遇到的實際困難，會積極考慮移除有關要求。〕

(b) 擬議條例要求「關鍵基礎設施營運者」須設有專責部門負責電腦系統保安及跟進專責辦公室的指

示。有意見指出現時在市場聘用合資格的電腦保安人員困難，建議放寬對人才專業資歷的要求。

〔**註**：擬議條例並無針對營運者的電腦系統保安人員的法定資格要求，保安局會在制定《實務守則》時詳列合乎標準的專業資歷名單，便利營運者聘請合適人員。〕

II. 預防責任

17. 我們共收到 105 項意見、建議或詢問。主要意見認為應就匯報「關鍵電腦系統」變化的要求有更清晰準則和要求、查詢如何保障披露有關系統資料的保密性、能否按國際或業界標準訂立電腦系統安全管理計劃、進行風險評估或審計，以減省重複工作。重點意見如下：

(a) 擬議條例要求「關鍵基礎設施營運者」須定期進行電腦系統保安風險評估和審計等，有意見期望能清晰界定評估和審計的涵蓋範圍（尤其是涉及運營科技的工業控制系統(Industrial Control System)及處於境外的關連電腦系統、可參照的標準、事故報告的格式等。

〔**註**：保安局將會參照最新科技及國際標準，制定《實務守則》的相關內容，提供符合法定要求的建議標準。〕

(b) 擬議條例要求「關鍵基礎設施營運者」須報告有關「關鍵電腦系統」在設計、配置、安全或運行方面的重大變化。有意見指報告的資料不宜涉及敏感或機密資料。

〔**註**：擬議條例並非針對「關鍵基礎設施營運者」系統內的個人資料和商業機密。專責辦公室要求營運者提供的資料，旨在確保營運者妥善履行保護其「關鍵電腦系統」的責任，並確保其「關鍵

電腦系統」遇到事故時，專責辦公室能有效評估事故對社會的嚴重性和對其他營運者的威脅。因此，專責辦公室在執行擬議條例下的職能時，會按法例要求「關鍵基礎設施營運者」提供必須的資料。〕

(c) 擬議條例要求「關鍵基礎設施營運者」須定期進行保安審計及提交報告。有意見認為應就審計的獨立性和審計人員的資歷列出更清晰準則。

〔**註**：我們認為獨立性是審計其中一個基本的原則，而審計人士應該獨立於被審計方，以避免任何利益衝突，確保審計公正客觀。專責辦公室會參考國際認可的標準和相關專業資格，在《實務守則》詳細列明對審計人員資歷的要求。〕

III. 事故通報和應對責任

18. 我們共收到 88 項意見、建議或詢問。主要意見認為應就事故通報設清晰準則和要求、放寬通報時限、減少重覆通報，以及為安全演習提供彈性。重點意見如下：

(a) 有意見認為機構難以按擬議條例的要求，在得悉嚴重電腦系統保安事故發生的兩小時內（或其他事故發生的 24 小時內），及時查證事故性質和成因，向專責辦公室通報。

〔**註**：保安局理解營運者在通報時可能遇到的實際困難，並參考了英國、歐盟及美國的相關要求，會積極考慮把通報嚴重電腦系統保安事故的時限，由得悉後兩小時放寬至 12 小時，而其他事故則由得悉後 24 小時放寬至 48 小時。同時，為確保有效及早應對事件，我們參考了新加坡和澳洲的做法，建議賦權專責辦公室在營運者賴以提供必要服務的「關鍵電腦系統」已經或可能受干擾或服務中斷時，可主動向營運者調查其原因以確

定是否由攻擊引致。〕

(b) 就擬議條例要求「關鍵基礎設施營運者」在得悉其他電腦系統保安事故發生的 24 小時內向專責辦公室通報，建議細化有關須匯報事故的定義。

〔**註**：擬議條例中，電腦系統保安事故是指未經合法授權在電腦或電腦系統上或透過電腦或電腦系統進行，而對其網路安全或另一台電腦或電腦系統的網絡安全構成危害或不良影響的行為或活動。《實務守則》將會詳細說明「須匯報事故」的涵蓋範圍及列舉例子。〕

(c) 擬議條例要求「關鍵基礎設施營運者」須定期參與由專責辦公室舉行的電腦系統安全演習。有意見認為應訂立演習的最低要求或規模以盡量減少因參與演習而影響服務。

〔**註**：擬議條例建議要求營運者至少每兩年一次參與由專責辦公室舉行的電腦系統安全演習，該要求參考了不同司法管轄區包括新加坡的做法和國際標準而釐定，我們認為有關電腦系統安全演習的要求和安排是合適的。〕

E. 專責辦公室

19. 我們共收到 35 項意見、建議或詢問。主要意見是查詢專責辦公室在甚麼情況下會發出書面指示、如何保護資料、與警方或個人資料私隱專員公署(「公署」)之間的分工，及建議專責辦公室應主動收集網絡風險情報。重點意見如下：

(a) 部分意見關注資料的保密性，及專責辦公室有何措施確保資料收集、保存、銷毀的安全性。

〔**註**：擬議條例並非針對「關鍵基礎設施營運者」

系統內的個人資料和商業機密。專責辦公室會按照相關法例和內部指引處理有關資料，亦會設立內部保密系統以確保資料傳送及貯存的安全性。〕

(b) 有意見指出如電腦系統事故涉及洩露個人資料，營運者或需同時向公署及專責辦公室報告事件，建議制定一套流程避免營運者重複工作。

〔**註**：專責辦公室及公署要求事故通報的目的及內容有所不同，前者負責找出發生洩露的原因並盡快堵塞漏洞，後者則著重保障個人資料的私隱；故此，若發生的事故涉及網絡攻擊電腦系統引致洩露個人資料，營運者確然需要同時向專責辦公室及公署報告，但並不存在「重複」工作，因兩類報告要求的目的及跟進工作並不相同。〕

F. 指定監管機構

20. 我們共收到 20 項意見、建議或詢問。主要意見認為應協調個別行業需求，避免重複合規工作。重點意見如下：

考慮到個別法定行業監管機構熟悉其行業及營運者的運作和需要，以及其擁有完善的督導營運者保障關鍵基礎設施電腦系統安全的架構及能力，擬議條例建議指定香港金融管理局負責監管銀行及金融服務界別內的部份機構，及通訊事務管理局負責監管通訊及廣播界別內的部份機構。有建議認為應沿用現存界別的監管機制或擴大其兼容性，以減低業界的合規成本。

〔**註**：指定界別的「關鍵基礎設施營運者」將透過遵循由該界別指定監管機構所發出的指引，履行擬議條例的「架構」及「預防」法定責任。此外，《實務守則》除引入各界別通用的基線要求外，亦會透過與不同界別保持緊密溝通及風險評估，

制定並詳細列出相關營運者適用的標準及方法，協助其滿足法定要求。〕

G.罪行及刑罰

21. 我們共收到96項意見、建議或詢問。主要意見關注若第三方服務供應商不合規可能引致法律的責任、建議設寬限期作充足準備、建議提供合理辯解的情況。重點意見如下：

(a) 有意見認為擬議條例罰則過重，建議清楚列明計算罰則的方法及可被視作「合理辯解」的情況，以及按營運者規模和財政能力處以罰款。

〔**註**：是次立法的原意並非懲罰營運者，訂立罪行及罰則旨在確保條例能有效實施及執行。擬議條例的罪行及罰則是考慮到香港的情況及參考了其他司法管轄區的相關法律後制定的。因此，我們認為現時的罰則是合適的。專責辦公室會積極協助營運者提升架構及預防保安事故的水平，避免觸犯法例。〕

(b) 擬議條例也要求「關鍵基礎設施營運者」須採取措施確保即使聘用了第三方服務提供者，營運者本身的「關鍵電腦系統」仍然符合相關法定要求。有意見擔心難以確保第三方服務提供者（尤其身處海外的服務供應商）遵守協議和符合法規，希望釐清當第三方服務提供者未能達到合規要求時，營運者所需要承擔的法律責任。

〔**註**：擬議條例容許「關鍵基礎設施營運者」聘用第三方服務提供者，但營運者仍需要負起履行條例下的相關法定責任。保安局會積極參考其他司法管轄區的經驗，在《實務守則》提供更多如何完善履行「盡責查證」(Due Diligence)及「合理努力」(Reasonable Endeavour)的指引，為「關鍵

基礎設施營運者」在聘用第三方服務提供者時訂定及履行合約提供參考。〕

(c) 有意見期望為條例生效設立寬限期，給予業界充分時間評估系統風險、制定事故應變計劃、聘請人才、與第三方服務供應商磋商合約條款等。

〔**註**：政府的目標是在擬議條例通過的一年內成立專責辦公室，以期讓法例可於其後半年內正式生效。期間，保安局和專責辦公室會與有機會被指明的營運者保持緊密溝通，按風險和機構準備程度分階段指明「關鍵基礎設施營運者」及其「關鍵電腦系統」，並制定《實務守則》的相關內容。條例中附設期限的法定要求，例如進行風險評估或獨立審計，以及提交相關報告等，將會由指明後才開始計算。因此，有機會被指明的營運者應有充足時間準備。〕

H.專責辦公室的調查權力

22. 我們共收到25項意見、建議或詢問。主要查詢向「關鍵基礎設施營運者」索取資料和進行調查和現場搜證的範圍。重點意見如下：

有意見擔心擬議條例賦權專責辦公室在「關鍵電腦系統」連接設備或安裝程式，會影響系統的正常運作。

〔**註**：擬議條例訂明，只有當發生嚴重事故時，營運者不願意或未能自行應對事故，專責辦公室才會考慮向裁判官申請手令，因應必要性、適當性、相稱性及公眾利益，在「關鍵電腦系統」連接設備或安裝程式，以應對事故。其他司法管轄區（如澳洲和新加坡）的相關監管機構也擁有類似的權力。〕

I. 上訴機制

23. 我們共收到14項建議或詢問。主要意見圍繞上訴委員會的組成方法和程序細節。重點意見如下：

> 擬議條例建議成立上訴委員會，處理有關營運者及電腦系統的指明，以及專責辦公室發出的書面指示的上訴。有意見詢問上訴委員會的組成方法，例如成員是否有界別專業知識、如何同時合乎保密性和維持獨立性等。
>
> 〔**註**：保安局參考了現時不同法定上訴委員會的安排，建議擬議條例下的上訴委員會由大約十五位來自業界、網絡安全及法律專業的專家組成團隊（包括一位委員會主席），並由特首委任。委員會成員須與專責辦公室保持獨立。每次進行上訴聆訊時，會由三位委員進行聆訊。三位成員必須申報沒有利益衝突（例如行業競爭者），並對聆訊內容簽署保密協議。〕

J. 附屬法例

24. 我們共收到3項意見或建議。主要意見圍繞立法程序和機制。重點意見如下：

> 擬議條例賦權保安局局長藉附屬法例，在有需要時在日後補充、更新或修改關於專責辦公室權限或營運者法定責任和細節。有意見擔憂訂立附屬法例會繞過立法程序。
>
> 〔**註**：附屬法例的制定或修訂有既定和相當嚴謹的程序，確保公平、公開、公正和透明，並且由立法會監察。〕

K.《實務守則》

25. 我們共收到53項意見或建議。主要意見建議就電腦系統保安培訓方面提供清晰指引和要求、詢問或建議按照國際或業界準則及邀請業界專家儘早制定《實務守則》內容、並就基線要求以上提出建議。重點意見如下：

(a) 就制定《實務守則》內容方面，多個界別均建議邀請界別專家參與制定內容，並廣泛諮詢業界意見，按照國際標準制定內容。

〔**註**：專責辦公室在制定《實務守則》時，會充分考慮業界持份者意見，按照界別的獨特性，以現行國際標準或行業特性，制定切實可行的要求。專責辦公室亦會持續檢視和完善《實務守則》的內容。〕

(b) 就《實務守則》概覽內有關電腦系統保安管理計劃下的電腦系統保安培訓方面，提出「關鍵基礎設施營運者」要為供應商、承辦商和服務供應商等提供培訓。有意見要求清楚列明訓練範圍、深度、方法及受訓人員類別。

〔**註**：專責辦公室在制定《實務守則》時，會詳細列明電腦系統保安培訓的要求和範圍，以及提供培訓的相關資料作參考。〕

<u>未來路向</u>

26. 保安局會參考在諮詢期間所收到的意見，爭取儘快將《保障關鍵基礎設施（電腦系統）條例草案》定稿，在本年內提交立法會進行審議。我們的目標是在條例通過後一年內成立專責辦公室，期間會繼續與各界別的持份者保持聯繫，共同制定界別適用的《實務守則》，並與有機會被指明的營運者緊密溝通，以敲定其是否符合被

指明為營運者的考慮因素，確定其賴以提供必要服務的相關「關鍵電腦系統」，並因應它們的系統對社會的影響和準備程度等，分階段作出指明，從而提升香港整體的電腦系統安全。

結語

27. 請委員備悉以上諮詢結果及未來路向。

保安局
2024 年 10 月

2024 年 7 月 2 日
討論文件

立法會保安事務委員會
加強保護關鍵基礎設施電腦系統安全—
建議立法框架

目的

本文件旨在向委員會簡介政府就加強保護關鍵基礎設施電腦系統安全的建議立法框架。

立法背景

2. 關鍵基礎設施是指一些維持香港社會正常運作和維持市民正常生活所必需的設施，例如銀行、金融機構、通訊網絡、供電設施、鐵路系統等。一旦關鍵基礎設施的資訊系統、資訊網絡或電腦系統受到擾亂或破壞，可能會影響主要設施的正常運作，甚或產生連鎖效應影響整個社會，嚴重危害社會經濟、民生、公共安全以至國家安全。例如，當電力和燃料供應、通訊、大型交通運輸、金融等必要服務因受到網絡攻擊而停頓，均會嚴重影響社會正常運作，甚至令整個社會陷於停擺。

3. 目前，我們沒有就針對保護關鍵基礎設施電腦系統作出任何法定要求。但隨著資訊和通訊技術的快速發展，關鍵基礎設施的運作越來越依賴互聯網、電腦系統、通訊基礎設施及智慧設備等，因此其電腦系統亦更容易受到網絡攻擊。

4. 事實上，全球的關鍵基礎設施均有受到惡意網絡攻擊的風險，而實際上亦曾發生過關鍵基礎設施被攻擊而對社會造成重大影響的事故。例如，2021 年，美國有燃油運輸管道營運商遭受勒索軟件攻擊，事件影響美國

東岸近半燃油供應。2024 年，美國一家醫療保險公司也受勒索軟件攻擊，部分醫療服務停頓，大量個人資料及醫療資訊有洩漏風險。2024 年，一間位於瑞典的數據中心遭黑客攻擊，令政府及商戶的運作受到干擾。香港也曾發生類似的事件。2024 年，本港一間私營醫院的電腦系統被黑客用勒索軟件攻擊，導致電腦系統未能如常運作，影響部分醫療服務。

5. 近年，保障關鍵基礎設施電腦系統安全的法規在其他司法管轄區越見普遍，中國內地、澳門特別行政區、澳洲、歐盟、新加坡、英國和美國等地都已訂立類似法例，加拿大國會亦正在審議相關法案，詳細見下列(a)至(h)：

(a) **中國內地**：《中華人民共和國網絡安全法》(2016 年) 及《關鍵信息基礎設施安全保護條例》(2021 年)；

(b) **澳門特別行政區**：《網絡安全法》(2019 年)；

(c) **澳洲**：《2018 年關鍵基礎設施安全法》（譯名）(Security of Critical Infrastructure Act 2018)；

(d) **英國**：《2018 年網絡與資訊系統規則》（譯名）(Network and Information Systems Regulations 2018)；

(e) **新加坡**：《2018 年網絡安全法》（譯名）(Cybersecurity Act 2018)；

(f) **歐盟**：《2022 年於歐盟實施高度共通程度之網絡安全措施指令》（譯名）(Directive on the measures for a high common level of cybersecurity across the Union 2022)；

(g) **美國**：有不同的聯邦法律、州法律以及適用於特定行業的規則，其中包括—

- 《2018 年網絡安全與基礎設施安全局法》(譯名)(Cybersecurity and Infrastructure Security Agency Act of 2018, CISA)

- 《2022 年關鍵基礎設施網絡事件報告法》(譯名) (Cyber Incident Reporting for Critical Infrastructure Act of 2022, CIRCIA)；以及

(h) **加拿大**：加拿大國會正在審議政府在 2022 年 6 月提交的相關法案，通過後，將成為《保障關鍵網絡系統法》(譯名) (Critical Cyber Systems Protection Act)。

6. 儘管不同司法管轄區的立法方式和管轄範圍不盡相同，相關法例均明確要求關鍵基礎設施的營運者遵守一系列責任，落實保護其電腦系統的措施，加強其應對網絡攻擊的能力，以及在發生電腦系統保安事故時向規管當局匯報，並盡快採取應對措施。

7. 行政長官在 2022 年 10 月發表的《施政報告》中宣布，會立法提升關鍵基礎設施的網絡安全，以推動關鍵基礎設施營運者建立良好的防範管理體系，確保其電腦系統的安全運作，讓重要服務運作順暢，鞏固香港良好營商環境及國際金融中心地位。

擬議的立法制度

8. 考慮到香港的情況，參考了上文第 5 段提述的司法管轄區的做法，並吸納了自去年初與不同持份者(包括有機會被指明為「關鍵基礎設施營運者」的機構、網絡保安服務供應商及審計公司、行業監管機構等)進行諮詢所

得的意見，我們**建議**訂立一條全新的法例。由於「網絡安全」一詞涵蓋的範圍甚廣，而為了更精準地反映我們的政策目標，即加強關鍵基礎設施的電腦系統的保安能力，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，擬議條例暫名為**《保障關鍵基礎設施（電腦系統）條例草案》**（下稱「擬議條例」）。

9. 上述所有參考了的司法管轄區均設有專責機構監督相關法例的執行情況，因此我們亦**建議**成立一個新的**專責辦公室**負責執行擬議條例（詳見下文 E 部第 25 段）。

A. 立法目的和原則

10. 我們的立法目的是要求關鍵基礎設施的營運者承擔一些法定責任，在多方面採取適當措施，加強其電腦系統的保安能力，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。

11. 我們必須強調以下立法原則：

(a) 擬議條例參考其他司法管轄區（包括中國內地、澳門特別行政區、澳洲、歐盟、新加坡、英國和美國）的立法方向，制定一套適合香港的監管模式；

(b) 擬議條例的規管對象是維持(i)香港社會必要服務攸關或(ii)重要的社會和經濟活動的「關鍵基礎設施營運者」，換言之絕大部分受規管的會是有規模的大機構，中小企及一般市民均不受影響；

(c) 擬議條例只會要求「關鍵基礎設施營運者」承擔起保護其「關鍵電腦系統」的責任，絕不涉及系統內的個人資料和業務內容；以及

(d) 法定責任旨在設立基線要求，讓「關鍵基礎設施營運者」可在此基礎上，根據各自的需要和特點，建立和加強保障其電腦系統安全的能力。雖然立法的原意並非旨在懲罰營運者，但是為了確保條例能有效實施及執行，條例必須要訂定相關的罪行及適當的罰則。平衡了規管對機構的影響，以及確保擬議條例有足夠的阻嚇力這兩方面的考慮後，刑罰方面會以機構作為單位，並只會以罰款方式處理。但是若相關的違規行為涉及觸犯現有的一些刑事法例，例如虛假陳述、行使虛假文書或其他詐騙相關罪行，則一如現時的情況，涉事人員亦有機會要負上個人刑事責任。

B. 規管範疇

12. 參考了英國和澳洲的做法，我們**建議**擬議條例清晰界定，只有被明確指明的「**關鍵基礎設施營運者**」及其「**關鍵電腦系統**」才受規管。下文第 13 至 23 段詳述有關主要概念的定義。

關鍵基礎設施

13. 關鍵基礎設施是社會及經濟命脈，與維持社會正常運作攸關。我們**建議**擬議條例下的「**關鍵基礎設施**」涵蓋以下兩大類：

第一類：在香港提供必要服務的基礎設施

14. 必要服務是指社會日常生活必需的至為重要的服務，如遭干擾、破壞、或長時間無法使用，會嚴重影響社會日常生活和運作。參考了上文第 5 段所述的司法管轄區的相關法例及考慮到香港的情況，我們**建議**擬議條例涵蓋以下八個提供必要服務的界別的基礎設施：

(a) 能源；
(b) 資訊科技；
(c) 銀行和金融服務；
(d) 陸上交通；
(e) 航空交通；
(f) 海運；
(g) 醫療保健；以及
(h) 通訊和廣播。

第二類：其他維持重要的社會和經濟活動的基礎設施

15. 除了必要服務外，亦有其他基礎設施，例如大型體育及表演場地、科研園區等，一旦遭到破壞、喪失功能或數據洩漏，可能嚴重危害重要的社會和經濟活動。參考了英國、澳洲、美國及歐盟的做法，我們**建議**有必要將此類設施納入規管範圍，保障其電腦系統的安全運作。

C. 規管對象

關鍵基礎設施營運者

16. 由於絕大部分關鍵基礎設施均由大機構營運，經參考英國、澳洲及歐盟的做法，我們**建議**擬議條例採取「機構為本」，即以負責營運每個「關鍵基礎設施」的機構為一個單位，履行保障其電腦系統安全的責任，確保每個機構整體電腦系統保安部署穩妥，避免漏洞。

17. 如上文第 12 段提述，只有被明確指明的「關鍵基礎設施營運者」方需要履行法定責任。參考了英國的做法，我們**建議**專責辦公室在決定某基礎設施是否「關鍵基礎設施」而需要被納入擬議條例規管時，考慮下列因素：

(a) 由於「關鍵基礎設施」是在香港提供必要服務或其他維持重要的社會和經濟活動的基礎設施，會考慮如果該基礎設施遭到破壞、喪失功能或數據洩漏時對香港的必要服務及重要的社會和經濟活動的影響；

(b) 由於基礎設施會用不同方法及工具（包括資訊科技）去提供其服務及維持運作，會考慮該基礎設施有多倚賴資訊科技運作。如資訊科技對其運作並無重大影響，則無必要要求指定履行法定責任；以及

(c) 由於第二類「關鍵基礎設施」涵蓋一旦遭到破壞、喪失功能或數據洩露，可能嚴重危害重要的社會和經濟活動的基礎設施，會考慮有關基礎設施所控制的數據的重要性。

18. 鑒於擬議條例採取「機構為本」的原則要求承擔法定責任，如專責辦公室根據上述理由認為某基礎設施是擬議條例規管的「關鍵基礎設施」，會考慮某機構對該「關鍵基礎設施」的控制程度等，以決定是否指明該機構為擬議條例下的「關鍵基礎設施營運者」，承擔法定責任。

19. 為免「關鍵基礎設施」成為網絡攻擊的目標，我們**建議**擬議條例只列出必要服務的界別名稱（如上文第14段提及的八個界別），而不公開「關鍵基礎設施營運者」的名單。有關做法和其他司法管轄區（例如英國及澳洲等）的做法一致。

20. 就政府提供的必要服務（例如供水、渠務、緊急救援等），政府內部已經有一套詳盡的《政府資訊科技保安政策及指引》（《政策及指引》），並且參照最新國際標準及業界良好作業模式定期檢討和更新，以確保政府資訊系統安全。最新一輪的檢討和更新工作已完成，並於2024年4月發出更新的《政策及指引》，過程中政府已參考最

新的國際資訊保安管理標準加強政府資訊科技保安要求，以應對日益增加的網絡保安風險。政府各部門必須嚴格遵循《政策及指引》，政府資訊科技總監辦公室亦會定期為各部門進行遵循審計。由於《政策及指引》要求的水平與擬議條例對「關鍵基礎設施營運者」的法定要求相若，再加上涉事政府人員若涉嫌有違規情況，相關政策局/部門會根據《公務員守則》等相關規管的既定程序在紀律方面作適當處理，我們**建議**繼續沿用現有的行政方法規管政府部門，無需納入擬議條例。

關鍵電腦系統

21. 由於我們的主要目的是規管與「關鍵基礎設施」正常運作相關的電腦系統，而非其他系統，而「關鍵基礎設施」可同時設有大量系統負責執行不同功能，為令營運者可按擬議條例的要求集中資源處理最重要的系統，並參考了上文第 5 段所述司法管轄區的相關法例，我們**建議**只有直接與提供必要服務有關或關乎設施核心功能的電腦系統，以及如受到干擾或破壞會嚴重影響設施正常運作的系統才會被指明為「關鍵電腦系統」。擬議條例的要求適用於所有符合定義的「關鍵電腦系統」，不論系統是否實際設置於香港。

22. 在具體運作上，專責辦公室會諮詢「關鍵基礎設施營運者」有哪些對其營運必不可少的系統，協助其考慮是否作出指明。

23. 考慮到「關鍵基礎設施」是在香港提供必要服務或其他維持重要社會和經濟活動的基礎設施，擬議條例旨在令營運者集中資源處理最重要的系統，故此營運者未被指明的其他電腦系統並不會受擬議條例規管。舉例而言，如個別機構的人事管理系統喪失功能並不會影響機構提供必要服務，而且和其提供必要服務的系統並無關聯，則不會被指明。相關做法和澳洲、英國和歐盟的方向一致。

D. 「關鍵基礎設施營運者」的責任

24. 參考了澳洲、英國和歐盟的相關法例，我們**建議**擬議條例對「關鍵基礎設施營運者」施加的責任主要分為三大類：I.架構；II.預防及 III.事故通報及應對。目的是讓營運者有良好、針對保護電腦系統安全的管理架構，實施必要措施，防止對「關鍵電腦系統」的網絡攻擊，當發生電腦系統保安事故時也能迅速應對並還原受事故影響的系統。其他司法管轄區的法例也是循這方向制訂各項營運者責任。這些責任包括－

I. 架構

(a) 由於營運者在香港營運重要的基礎設施而必須履行下述有關預防和事故通報及應對的責任，並為確保專責辦公室可向「關鍵基礎設施營運者」保持通訊，營運者必須在香港設有地址和辦事處（及報告任何隨後變更）；

(b) 為使專責辦公室了解「關鍵基礎設施」的擁有權及運作情況，並在有需要時更改或更新指明「關鍵基礎設施營運者」的名冊，營運者必須報告有關「關鍵基礎設施」的擁有權和營運權的變更；

(c) 為確保營運者有專責部門負責電腦系統保安及跟進專責辦公室的指示，營運者必須設有具專業知識的電腦系統安全管理部門（可自設或外判），並由營運者公司的專責主管負責監管；

II. 預防

(d) 為使專責辦公室可掌握營運者有何「關鍵電腦系統」，有需要時更改或更新指明「關鍵電腦系統」的名單，營運者必須向專責辦公室報告有關「關鍵電腦系統」的重大變化，包括對其設計、配置、

安全或運行的重大變化等；

(e) 為確保營運者未雨綢繆，詳盡計劃如何保護其電腦系統，營運者必須制定及實施電腦系統安全管理計劃，並向專責辦公室提交計劃；

(f) 為確保營運者有效監控其電腦系統保安風險，營運者必須至少每年進行一次電腦系統保安風險評估，並向專責辦公室提交報告；

(g) 為檢查營運者的合規情況，營運者必須至少每兩年一次進行獨立電腦系統保安審計，並向專責辦公室提交報告；

(h) 為確保機構整體保安，不會因第三方服務提供者的系統出現保安漏洞而影響其服務，營運者必須採取措施確保即使聘用了第三方服務提供者，營運者本身的「關鍵電腦系統」仍然符合相關法定要求；以及

III. 事故通報及應對

(i) 為測試營運者應對電腦系統攻擊的能力，營運者必須至少每兩年一次參與由專責辦公室舉行的電腦系統安全演習；

(j) 為確保營運者能夠有效地應對並妥善處理突發事件，營運者必須制訂應急計劃，並向專責辦公室提交計劃；

(k) 營運者必須在指定時間內向專責辦公室報告有關「關鍵電腦系統」的保安事故，讓專責辦公室有需要時可盡快指示相關的應對工作:

- 嚴重電腦系統保安事故（指已經或即將對必

要服務的連續性及關鍵基礎設施的正常功能造成重大影響，或導致個人資料等數據大量外洩的事故）：在得悉事件發生後2小時內；

- 其他電腦系統保安事故：在得悉事件發生後24小時內。

應專責辦公室在調查事故或與上述第(I)至(III)類責任相關的罪行時所發出的要求，營運者必須提交其可取得的相關資料，即使該等資料位於香港境外。

E. 專責辦公室

25. 參考上文第5段不同司法管轄區的做法，為妥善監察「關鍵電腦系統」的安全狀況，並確保擬議條例對不同界別的關鍵基礎設施一致落實，我們**建議**成立一個隸屬保安局的專責辦公室，由行政長官委任的一名專員帶領，執行擬議條例下的工作。專責辦公室的主要職能包括：

(a) 指明「關鍵基礎設施營運者」及「關鍵電腦系統」；

(b) 制定《實務守則》，就「關鍵基礎設施營運者」應採取的措施提供建議；

(c) 監察針對關鍵基礎設施的電腦系統保安威脅；

(d) 協助「關鍵基礎設施營運者」應對電腦系統保安事故；

(e) 調查及跟進「關鍵基礎設施營運者」違規情況；

(f) 協調不同政府部門及專家，例如政府資訊科技總監辦公室、警方網絡安全及科技罪案調查科（網罪科）及香港電腦保安事故協調中心等，在制定政策及指引和處理事故方面的工作；以及

(g) 向「關鍵基礎設施營運者」發出書面指示，以堵塞可能出現的保安漏洞。

F. 個別行業的指定監管機構

26. 擬議條例擬規管的部分必要服務行業現已受其他法定行業監管機構的全面規管（例如透過發牌制度），個別更有發出與電腦系統保安有關的指引，鑒於這些法定行業監管機構最熟悉其相關行業的運作和需要，我們**建議**這些個別行業監管機構為「指定監管機構」，負責監管這些必要服務行業的「關鍵基礎設施營運者」履行架構及預防的責任（見上文第 24 段所列出的第(I)及(II)類責任）；而事故通報及應對的責任（見上文第 24 段所列出的第 (III)類責任），除部分可能由專責辦公室指明豁免外，則由專責辦公室全權負責監管所有八個界別的「關鍵基礎設施營運者」。

27. 上述做法一方面讓行業「指定監管機構」可在它們現有的規管制度下，就架構及預防責任訂立一套最切合這些行業的標準和要求，監管其行業的「關鍵基礎設施營運者」履行這兩類責任，而這些界別的營運者不用再額外滿足專責辦公室在這兩類責任所訂的要求。另一方面，亦確保專責辦公室可以掌握所有「關鍵基礎設施營運者」的事故及應對安排，以作出協調、調查及提供協助，並防範事故擴散至其他關鍵基礎設施。英國、澳洲及美國的相關法例也有類似將個別行業規管責任交予行業監管機構的做法。

28. 現階段，我們**建議**指定(1)金融管理局監管部分與銀行和金融服務相關的服務提供者，以及(2)通訊事務管理局監管部分與通訊和廣播相關的服務提供者。這兩個「指定監管機構」負責的界別已有非常成熟且完善的監管制度，也設有與電腦系統保安有關的指引，例如金融管理局發出的《網絡防衛評估框架》及通訊事務管理局發出的《關於操作和管理物聯網裝置的業務守則》和《下一代網絡保安指引》等。

29. 具體而言，「指定監管機構」會負責在其組別／類別下，指明「關鍵基礎設施營運者」及「關鍵電腦系統」，並按其現在的監管方式（例如發牌制度）監察及處理其行業的「關鍵基礎設施營運者」履行架構及預防責任、合規情況、處理營運者提交的各項報告等。相關「關鍵基礎設施營運者」也只需要在履行架構及預防的責任方面，向其對應的指定監管機構作相關的匯報，而不需再向專責辦公室提交報告。「指定監管機構」也會因應其規管行業的特殊情況發出指引，以達致擬議條例下架構及預防兩類責任方面相若的要求，及在違規時作出適當的懲處。

30. 儘管如此，為確保專責辦公室可以掌握所有「關鍵基礎設施營運者」的事故通報及應對情況，如這些行業的「關鍵基礎設施營運者」遇上電腦保安事故，除了按「指定監管機構」現有規管架構的要求向「指定監管機構」作出報告外，還必須按擬議條例的要求向專責辦公室報告，以便專責辦公室協調應對工作，並防範事故擴散至其他關鍵基礎設施。在收到事故通報後，專責辦公室會與警方的網罪科作出調查及應變，並提供協助盡快修復相關電腦系統。

31. 為了確保專責辦公室可全面監管香港整體「關鍵基礎設施」電腦系統的安全，專責辦公室保留可向所有「關鍵基礎設施營運者」根據擬議條例發出書面指示的權力，不論該「關鍵基礎設施營運者」是否由「指定監管機構」監管。

G. 罪行及刑罰

32. 如文件第 11 段提及，雖然立法的目的旨在促使「關鍵基礎設施營運者」承擔企業責任，加強其「關鍵電腦系統」的安全保護，而立法原意並非懲罰營運者，但是為了確保條例能有效實施及執行，必須要訂定相關的罪行及適當的罰則。若未有合理辯解下干犯了條例下的罪行，即屬違法，專責辦公室可以提出檢控。參考了英國、澳洲及歐盟的做法，我們**建議**擬議條例所訂的罪行包括：

(a) 「關鍵基礎設施營運者」不履行法定責任；

(b) 「關鍵基礎設施營運者」不遵從專責辦公室發出的書面指示；

(c) 不遵從專責辦公室按法定調查權力提出的要求；以及

(d) 不遵從專責辦公室就提供與關鍵基礎設施有關的資料的要求。

33. 如上文第 11(d)段所述，雖然我們**建議**擬議條例下的罪行及罰則只會針對機構，並不會在個人層面懲罰機構的主管或員工，但是若相關的違規行為涉及觸犯現有的刑事法例，例如向專責辦公室提交虛假資料有機會會觸犯虛假陳述、行使虛假文書或其他詐騙相關罪行，則一如現時的情況，涉事人員亦有機會要負上個人刑事責任。

34. 就罪行的建議刑罰而言，考慮到立法原意，和英國及歐盟的相關法例做法一致，我們**建議**擬議條例的罰則只有罰款。違者可處最高罰款港幣五十萬元至五百萬元不等，經法庭審訊而定；個別罪行也會就持續違法行為處以額外的每日罰款。

35. 一般而言，如果違法行為可以透過營運者跟進修正，因而不會嚴重影響其電腦系統安全或者專責辦公室規管的能力，建議最高罰款會較低，以反映其違規情況的相對較低的嚴重程度。例如營運者未有準時提交電腦安全管理計劃，營運者可以及後提交報告補救，最高罰款為港幣五十萬元。反之，未有在指定時間內向專責辦公室報告電腦系統保安事故可以導致延誤處理，對「關鍵基礎設施」的電腦系統安全，甚至香港整體的公共安全可以有嚴重影響，最高罰款則為港幣五百萬元。就違反上文第 24 段所述針對營運者的責任要求、及違反其他專責辦公室的指示的罪行及其建議罰則見**附件一**。

36. 我們理解到有些「關鍵電腦系統」或會由第三方服務提供者擁有或控制，為確保這些「關鍵電腦系統」不會成為電腦系統保安的缺口，「關鍵基礎設施營運者」有責任確保第三方服務提供者有就其控制的「關鍵電腦系統」落實相關安全措施（見上文第 24 段 II(h)項）。如因第三方服務提供者的不足而導致違反法定責任，依然要為違規行為負責。

H. 專責辦公室的調查權力

37. 上文第 5 段列出的所有司法管轄區均有賦予有關盤問、索取資料、進入處所、查閱電腦系統等權力。我們**建議**擬議條例賦權專責辦公室行使各種調查權力，調查擬議條例下所訂定的罪行，讓專責辦公室有能力調查電腦系統保安事故，以協助「關鍵基礎設施營運者」應對及復原；以及跟進違規行為。

38. 每一項權力均有特定的條件、行使權力或作出授權的機關（包括要否先取得裁判官手令）等規範，確保這些調查權力為最低限度而必要的。

I. 應對保安事故的權力

39. 儘管一般而言，「關鍵基礎設施營運者」有責任處理電腦系統保安事故，參考了澳洲、英國及歐盟的相關法例，我們**建議**專責辦公室獲賦權調查，以評估事故的影響，減低損害和防止事故蔓延。就此，專責辦公室將可以在事故發生後，要求營運者回答問題及提交有關事故的資料。如發現營運者不願意或未能自行應對事故，則可進一步要求營運者採取補救措施、協助調查，及在營運者同意下進入處所調查。在較嚴重的情況下，專責辦公室可基於公眾利益，向裁判官取得手令以行使進一步的權力，如要求營運者以外控制「關鍵電腦系統」的人協助調查。至於受「指定監管機構」規管的「關鍵基礎設施營運者」，如上文第 30 段所述，除了向「指定監管機構」按其現行規管架構報告事故外，亦須按擬議條例向專責辦公室報告，以便協調警方網罪科一如以往在事故發生後作出調查並提供適當的協助。

II. 調查條例下罪行的權力

40. 專責辦公室有權調查擬議條例下的罪行（例如營運者違反法定責任），有關權力包括盤問、索取資料、在裁判官手令下進入處所調查等。擬議條例會清楚列明可行使權力的條件及程序（例如通知期）等。

41. 有關權力的要點（包括條件、作出授權的機關及可行使能力的人員等）見**附件二**。

I. 上訴機制

42. 在具體運作上，專責辦公室一般會和有機會被指明的機構保持緊密合作和溝通，以期大家對專責辦公室指明有關營運者或「關鍵電腦系統」有共識。儘管如此，不能排除營運者或會反對被專責辦公室指明為「關鍵基

礎設施營運者」或指明其某些電腦系統為「關鍵電腦系統」。此外，專責辦公室根據擬議條例下的權力，可向被指明的「關鍵基礎設施營運者」發出書面指示，要求營運者採取進一步措施以達致法定要求。參考了英國的做法，我們**建議**擬議法例設有上訴機制，成立上訴委員會，當營運者不同意專責辦公室有關「關鍵基礎設施營運者」或「關鍵電腦系統」的指明、或其發出的書面指示時，可透過獨立的渠道提出上訴。

43. 上訴委員會委員應包括電腦資訊保安專業人士及法律界人士等，確保有平衡、獨立的第三方意見考慮上訴。委員會可以決定維持、推翻或更改相關決定。擬議條例會詳列相關程序。至於專責辦公室下的其他決定，例如檢控營運者違反法例規定，如營運者不服，則可在司法程序中處理。

J. 附屬法例

44. 除了主體法例外，由於有一些關於專責辦公室權限或營運者法定責任和細節或需要在日後補充、更新或修改，我們**建議**擬議條例賦權保安局局長藉附屬法例訂明或修訂這些部分，例如：

(a) 可被指明為關鍵基礎設施的必要服務界別；

(b) 指定監管機構名單；

(c) 專責辦公室可以向關鍵基礎設施的營運者索取的資料；

(d) 需要向專責辦公室報告有關「關鍵電腦系統」的重大變化的類型；

(e) 電腦系統安全管理計劃及電腦系統保安審計的涵蓋範圍及模式；

(f) 電腦系統保安風險評估及應急計劃的涵蓋範圍；

(g) 需要向專責辦公室報告的電腦系統保安事故的類型；以及

(h) 提交報告的時限等。

K. 《實務守則》

45. 鑒於科技日新月異，一些詳細的操作模式或需不時更新。我們**建議**擬議條例賦權專責辦公室發出《實務守則》，列出在法例要求的基礎上的建議標準，讓專責辦公室能更靈活地適時參照最新科技及國際標準更新指引，協助營運者滿足法例要求。專責辦公室也會跟不同界別的營運者溝通，有需要時在《實務守則》加入針對特定界別的指引。

46. 舉例而言，擬議法例要求營運者定期進行獨立電腦系統保安審計，《實務守則》會列出獨立電腦系統保安審計師應具備的相關專業資格、審計涵蓋範圍、可參考的國際認可方法和標準、及報告及修正計劃的細節等。其他司法管轄區（例如歐盟）也有類似將建議合規標準列入條例以外的指引的做法。《實務守則》的涵蓋範圍見**附件三**。同樣地，「指定監管機構」亦可就其規管的機構發出相關指引。

47. 《實務守則》並非附屬法例，「關鍵基礎設施營運者」不遵守《實務守則》的條文，本身並不構成罪行。不過，在發現懷疑違規情況時，「關鍵基礎設施營運者」若已跟從《實務守則》的建議標準，可作為有力的證據，證明並無違反法定責任。儘管如此，只要達到法定責任的目

的，營運者仍可透過《實務守則》以外的方法去履行法定責任。

L. 綜合建議

48. 上述 B 至 K 項所提出的各項建議，綜合列出在**附件四**以方便參考。

持份者的意見

49. 我們自 2023 年起，舉辦超過 15 場針對超過 110 個不同持份者（包括有機會被指明為關鍵基礎設施營運者的機構、網絡保安服務供應商及審計公司、行業監管機構等），就立法的初步建議框架諮詢持份者。相關持份者一致認同維護電腦系統安全是社會各界的共同責任，原則上支持立法。大部份基礎設施營運者的代表也表示他們所屬的機構已施行一定的電腦系統的保安措施。持份者的主要關注以及我們的回應如下：

(a) 合規成本 — 有意見指有一些行業已經有類似的電腦安全要求，重複滿足不同監管機構的要求會進一步增加合規成本。就此，我們**建議**加入「指定監管機構」負責監管相關營運者在架構及預防兩類責任方面的合規情況(見上文第 26 段)；

(b) 聘請合資格的電腦保安人才擔任主管的困難 — 有意見指由於相關人才短缺，聘請合資格的電腦系統安全管理部門主管或有一定困難，就此，我們已適當地修訂相關要求，營運者只需設立具專業知識的電腦系統安全管理部門（見上文第 24 I (c)項），也可按需要選擇從第三方相關服務提供者外聘有關服務，唯必須由營運者公

司的專責主管負責監管。此外，我們**建議**只將有關電腦系統安全管理部門主管的要求納入《實務守則》作為建議標準，讓營運者有更大彈性聘請適合的人選；

(c) 報告事故的時限 — 有意見指營運者在發生事故後需時確認事故，吸納了他們的意見，我們**建議**更清晰界定有關報告電腦系統保安事故的時間要求，在擬議條例中訂明報告的時限[1]只會在營運者得悉[2]與「關鍵電腦系統」相關的保安事故後起計（見上文第 24 III (k)項），確保營運者有時間先初步調查事件是否電腦系統保安事故；以及

(d) 刑事責任 — 有營運者關注違反法定要求會負上個人刑事責任。雖然立法原意並非旨在懲罰營運者，擬議條例下的罪行及罰則只會針對機構，並不會在個人層面懲罰機構的主管或員工，所訂罪行也只會以罰款處理；但是若相關的違規行為涉及觸犯現有的一些刑事法例，例如虛假陳述、行使虛假文書或其他詐騙相關罪行等，則一如現時的情況，涉事人員亦有機會要負上個人刑事責任。

未來路向

50. 我們會在 7 月 2 日諮詢立法會保安事務委員會後，發送專函再次諮詢相關業界，就本文所列的立法建議提供意見，諮詢期為期一個月。同時，保安局聯同律政司、政府資訊科技總監辦公室及香港警務處已開展擬議條例草案的草擬工作。我們會考慮和吸納是次諮詢所收到的

---

1 嚴重事故：在得悉事件發生後 2 小時內；其他事故：在得悉事件發生後 24 小時內。

2 「得悉」指合理確定網絡保安事件已對「關鍵電腦系統」的機密性、完整性或可用性造成損害，或已損害其運作。為了確立網絡保安事故是否已發生而進行的短期調查可能不被視為「得悉」。

意見，計劃於2024年年底前將擬議條例草案提交立法會審議。

51. 擬議條例通過後，政府的目標是在一年內成立專責辦公室，以期讓擬議條例可於其後半年內正式生效，屆時，專責辦公室會因應不同關鍵基礎設施的界別內可能被指明為「關鍵基礎設施營運者」的情況，包括其準備程度及其服務對社會的影響等，逐步分階段指明「關鍵基礎設施營運者」及其「關鍵電腦系統」。

基礎設施實體安全的保障

52. 是次立法建議重點為保障關鍵基礎設施的電腦系統安全。就基礎設施的實體安全，香港警務處的重要基礎設施保安協調中心（協調中心）會繼續透過公私營機構合作、風險管理、現場保安檢查等，致力強化重要基礎設施整體的保護及韌性。

53. 此外，針對基礎設施的攻擊，視乎攻擊者的意圖及犯罪情況，可能會干犯現行法例下的罪行（例如「刑事毀壞」(《刑事罪行條例》第60條)、「縱火」(《刑事罪行條例》第60(3)條）等）。

徵詢意見

54. 請委員就政府提出加強保護關鍵基礎設施的電腦系統的建議立法框架提供意見。

保安局
政府資訊科技總監辦公室
香港警務處
2024年6月

附件一

「關鍵基礎設施營運者」的責任、擬議罪行及罰則一覽表

A.「關鍵基礎設施營運者」責任及相關違規行為

營運者責任		違法行為	罰則
I.	**架構**		
(a)	向專責辦公室**提供和維持在香港的地址和辦事處** - 於指明為「關鍵基礎設施營運者」後的 30 天內提供 - 任何變更須於 30 天內報告	無合理辯解下，未有於指定時間內向專責辦公室提供該地址／報告變更	最高罰款 50 萬元 持續罪行：每日罰款 5 萬元
(b)	向專責辦公室報告有關「關鍵基礎設施」的**擁有權和營運權的變更** - 擁有權：任何變更須於 30 天內報告 - 營運權：於變更日期前至少 3 個月報告	無合理辯解下，未有於指定時間內向專責辦公室報告變更	最高罰款 500 萬元 持續罪行：每日罰款 10 萬元
(c)	設有具專業知識的**電腦系統管理部門**（可自設或外判）並由營運者公司的**專責主管**負責監管，確保有專責部門處理電腦系統保安及跟進專責辦公室的指示 （註:《實務守則》會列出有關部門組成，及主管的經驗及資歷等建議）	如未有達致相關的標準，專責辦公室有權向營運者發出書面指示，無合理辯解下違反書面指示，即屬違法	最高罰款 500 萬元 持續罪行：每日罰款 10 萬元

營運者責任		違法行為	罰則
II.	**預防**		
(d)	向專責辦公室**報告有關「關鍵電腦系統」的重大變化**，例如包括： - 對其設計、配置、安全或運行的重大變化等 （註:《實務守則》會列出重大變化的例子供參考）	無合理辯解下，未有於變更後30天內向專責辦公室報告	最高罰款50萬元 持續罪行：每日罰款5萬元
(e)	**制定並實施電腦系統安全管理計劃** - 於指明為「關鍵基礎設施營運者」的三個月／變化的一個月內提交內向專責辦公室提交 （註:《實務守則》會列出有關電腦系統安全管理計劃應涵蓋的範圍（詳情另見<u>**附件三**</u>））	無合理辯解下，未有於指定時間內提交計劃	最高罰款50萬元 持續罪行：每日罰款5萬元
		如未有達致相關的標準，專責辦公室有權向營運者發出書面指示，無合理辯解下違反書面指示，即屬違法	最高罰款500萬元 持續罪行：每日罰款10萬元
(f)	進行**電腦系統保安風險評估** - 至少每年進行一次 - 評估報告須在評估完成後30天內向專	無合理辯解下，未有於指定時間內提交報告	最高罰款50萬元 持續罪行：每日罰款5萬元

營運者責任		違法行為	罰則
	責辦公室提交 - 包括安全漏洞評估及滲透測試 （註:《實務守則》會列出可參考的國際認可方法和標準）	如未有達致相關的標準，專責辦公室有權向營運者發出書面指示，無合理辯解下違反書面指示，即屬違法	最高罰款500萬元 持續罪行：每日罰款10萬元
(g)	進行**獨立電腦系統保安審計** - 至少每兩年進行一次 - 保安審計完成後30天內向專責辦公室提交審計報告 - 當審計報告不完備或不合規時，按專責辦公室指示作額外審計 （註:《實務守則》會列出審計師建議具備的專業資格、保安審計涵蓋的範圍、可參考的國際認可方法和標準、提交報告及修正計劃的細節）	無合理辯解下，未有於指定時間內提交報告	最高罰款50萬元 持續罪行：每日罰款5萬元
		如未有達致相關的標準，專責辦公室有權向營運者發出書面指示，無合理辯解下違反書面指示，即屬違法	最高罰款500萬元 持續罪行：每日罰款10萬元
(h)	採取措施確保即使聘用了第三方服務提供者，**營運者本身的「關鍵電腦系統」仍然符合**相關法定**要求** - 包括合同條款或採取其他措施	如未有達致相關的標準，專責辦公室有權向營運者發出書面指示，無合理辯解下違反書面指示，即屬違法	最高罰款500萬元 持續罪行：每日罰款10萬元

營運者責任		違法行為	罰則
III. 事故通報及應對			
(i)	參與**電腦系統安全演習** - 至少每兩年一次 - 由專責辦公室舉行 （註:《實務守則》會列出演習的模式、規模等例子作參考）	無合理辯解下，未有至少每兩年一次參與電腦系統安全演習	最高罰款 500 萬元
(j)	就應對並妥善處理突發事件制訂**應急計劃** - 於指明為「關鍵基礎設施營運者」的三個月內向專責辦公室提交	無合理辯解下，未有於指定時間內提交計劃	最高罰款 50 萬元 持續罪行：每日罰款 5 萬元
	- 於變化的一個月內向專責辦公室提交 （註:《實務守則》會列出應急計劃應涵蓋的範圍(詳情另見 **附件三**)）	如未有達致相關的標準，專責辦公室有權向營運者發出書面指示，無合理辯解下違反書面指示，即屬違法	最高罰款 500 萬元 持續罪行：每日罰款 10 萬元

營運者責任		違法行為	罰則
(k)	在指定時間內向專責辦公室報告有關「關鍵電腦系統」的**保安事故** - 嚴重電腦系統保安事故[1]：得悉事故後2小時內作出初步報告 - 其他電腦系統保安事故則在得悉事故後24小時內作出初步報告 - 如果初步報告是透過電話或短訊方式報告，須在報告後48小時內提交書面記錄 - 14天內提交書面報告，詳述原因、影響、補救措施等資料。 - 需要報告的事故類型會於條例內訂明[2] （註:《實務守則》會列出報告格式及範本（詳情另見 **附件三** ））	無合理辯解下，未有在指定時間內報告有關「關鍵電腦系統」的安全事故	最高罰款500萬元

1 嚴重事故指已經或即將對必要服務的連續性及「關鍵基礎設施」的正常功能造成重大影響，或導致個人資料等數據大量外洩的事故。

2 包括未經授權而取得「關鍵電腦系統」的控制的黑客攻擊；在「關鍵電腦系統」上安裝或運行未經授權的惡意程式；針對系統之間關連的攻擊；分散式阻斷服務的攻擊；以及其他影響「關鍵電腦系統」的使用或操作的事故。

B. 專責辦公室構索取資料和調查的權力及違法行為

專責辦公室的權力		違法行為	罰則
(a)	為**考慮是否指明機構為「關鍵基礎設施營運者」**，專責辦公室可書面要求任何控制有可能被指名為「關鍵基礎設施」的機構提交有關資料 - 包括該機構提供的必要服務、依賴科技的程度、其資訊系統受阻或被破壞的後果及影響範圍等	無合理辯解下，違反專責辦公室有關提交資料的指令	就已被指明的「關鍵基礎設施」而言： 最高罰款 500 萬元 持續罪行： 每日罰款 10 萬元 就未被指明的設施而言： 最高罰款 50 萬元 持續罪行： 每日罰款 5 萬元
(b)	為**考慮是否指明某電腦系統為「關鍵電腦系統」時**，專責辦公室可書面要求「關鍵基礎設施營運者」提交有關資料 - 包括系統數目、組成、設計、服務對象、關聯性等	無合理辯解下，違反專責辦公室有關提交資料的指令	最高罰款 500 萬元 持續罪行： 每日罰款 10 萬元

專責辦公室的權力		違法行為	罰則
(c)	專責辦公室可**調查針對「關鍵電腦系統」的保安事故**，以評估事故的影響，減低損害和防止事故蔓延。 - 權力包括盤問、索取資料、要求營運商採取補救措施、在裁判官手令下進入處所調查等 （註:有關權力的要點（包括條件及作出授權的機關）另見**附件四**）	無合理辯解下，違反專責辦公室任何為調查有關「關鍵電腦系統」的保安事故而行使的法定權力的指令	最高罰款50 萬元
(d)	專責辦公室**可調查本條例下所訂罪行** - 權力包括盤問、索取資料、在裁判官手令下進入處所調查等 （註:有關權力的要點（包括條件及作出授權的機關）另見**附件四**）	無合理辯解下，違反專責辦公室任何為調查條例下罪行而行使的法定權力的指令	最高罰款50 萬元

附件二

專責辦公室的調查權力

I. 調查「關鍵電腦系統」保安事故的權力

行使權力的情況和門檻	作出授權的機關	權力	不遵從權力所干犯的罪行
• 發生有關「關鍵電腦系統」的保安事故	專責辦公室	針對「關鍵基礎設施營運者」（下稱營運者） • 盤問營運者 • 要求營運者提交資料	無合理辯解下，違反專責辦公室任何為調查有關「關鍵電腦系統」的保安事故而行使的法定權力的指令，最高罰款 50 萬元 (見 附件一 第 B(c)項)
• 營運者不願意或未能自行應對事故 • 有必要行使有關權力時 • 有關權力是適當及與有關事故相稱的		針對營運者 • 指示營運者採取補救行動 • 指示營運者採取行動協助調查 • 在營運者同意下，檢查營運者擁有／控制的「關鍵電腦系統」	
• 營運者不願意或未能自行應對事故 • 有必要行使有關權力時 • 有關權力是適當及與有關事故相稱的 • 行使的權力有助調查事故 • 符合公共利益	裁判官手令	針對營運者 • 未得營運者同意下，檢查營運者擁有／控制的「關鍵電腦系統」 針對不屬營運者控制的「關鍵電腦系統」(例如第三方服務提供者控制的「關鍵電腦系統」) • 進入不屬營運者控制的「關鍵電腦系統」所在的處所並檢查有關系統 • 要求控制「關鍵電腦系統」的人回答問題及提交文件	

行使權力的情況和門檻	作出授權的機關	權力	不遵從權力所干犯的罪行
		• 指示控制「關鍵電腦系統」的人採取補救行動 • 指示控制「關鍵電腦系統」的人採取行動協助調查 • 在「關鍵電腦系統」上連接設備或安裝程式	

II. 調查條例下罪行的權力

行使權力的情況和門檻	作出授權的機關	權力	不遵從權力所干犯的罪行
• 專責辦公室懷疑有條例下的罪行發生時	專責辦公室	• 要求調查人員認為可能持有有關資料的人提交資料及回答問題	無合理辯解下，違反專責辦公室任何為調查條例下罪行而行使的法定權力的指令，最高罰款 50 萬元 (見 **附件一** 第 B(d)項)
• 有合理理由懷疑處所內有一些和調查有關、但未在調查人員要求下提交的文件；或 • 如調查人員要求提交有關文件，文件會被隱藏、移走、篡改或銷毀	裁判官手令	• 進入處所並取得任何相關文件	

附件三

《實務守則》主要內容概覽

（一） 報告關鍵電腦系統的重大變更

1. 可歸納為「重大變更」的例子包括但不限於平台遷移、伺服器虛擬化、應用程式重新設計、與外部系統或其他電腦系統的整合或相互依存關係變更等

（二） 獨立電腦系統保安審計

1. 獨立電腦系統保安審計師應具備的相關專業資格
2. 保安審計涵蓋的範圍
3. 可參考的國際認可方法和標準
4. 提交獨立電腦系統保安審計報告及修正計劃的細節

（三） 電腦系統保安風險評估

1. 風險評估涵蓋的範圍，包括安全漏洞評估（Vulnerability assessment）及滲透測試（Penetration test）
2. 可參考的國際認可方法和標準

（四） 電腦系統保安管理計劃

應涵蓋的主要內容包括：

1. **電腦系統安全管理部門**的架構、權限、職務和職責；
2. 電腦系統安全管理部門**主管**應具備合適的專業資格；

3. 就營運者在制定**政策**、**標準**、**指引**時應考慮的因素，例如本身的保安要求、《實務守則》及法定組織為個別行業所制訂的相關要求；

4. 制訂**電腦系統保安風險管理架構**時，如何識別、評估、減低和監控與營運者及其關鍵電腦系統(下稱系統)相關的風險；

5. 建立**監察和偵測**機制：

    - 界定系統運行的正常行為基準，並根據該基準監察異常情況；

    - 制定程序和流程，以持續和及時應對監察系統所接收到的任何電腦系統保安事故；

    - 建立機制和程序，以持續收集和分析與資訊保安威脅有關的資訊或情報，包括攻擊者手法、所涉及工具和技術，以及可採用的適當緩解措施；

    - 應定期對監察機制進行覆檢(至少每 2 年一次)，以確保該機制的性質和技術發展維持有效；

6. 有關電腦系統保安培訓：因應參與關鍵基礎設施操作的所有人員，包括供應商、承辦商和服務供應商的角色，以制定各種電腦系統保安方式的培訓計劃

7. 設計層面的保安 (Security by Design) ，以確保保安在系統的整個生命週期中都是重要的一環；

8. 實施資產管理 (Asset Management)，以確保能妥善持有、保管及維護系統的最新清單和其他相關資產，並符合「有需要知道」原則限制接達；

9. 實施接達控制 (Access Control) 及帳戶管理 (Account Management)，只允許獲授權用戶和電腦資源接達系統及貫徹最小權限原則，並作定期覆檢，註銷不再需要的用戶及數據接達權限，備存所有接達和嘗試接達系統的日誌；

10. 實施特別接達管理 (Privileged Access Management)，確保人員只能接達所需的管理功能，並定期由獨立方審計特權帳戶的使用情況；

11. 實施密碼匙管理 (Cryptographic Key Management)，確保適當和有效地使用加密方法，以保護資料的機密性、真確性和完整性；

12. 實施密碼管理 (Password Management)，制訂嚴謹密碼政策；

13. 實施實體保安 (Physical Security)，確保數據中心及電腦室等設於完善的環境；

14. 實施系統強化 (System Hardening) ，採取最小功能和最小權限兩項原則，建立、維持及定期覆檢電腦系統的基本配置；

15. 實施變更管理 (Change Management)，如對生產系統的變更進行適當的規劃、監察和跟進、充分備份系統檔案和配置等；

16. 實施修補程式管理 (Patch Management)，採用風險為本的方法來盡早制訂系統的適當修補程式管理策略；

17. 制訂適當的遠程連接 (Remote Connection) 政策及程序；

18. 制訂便攜式電腦裝置及抽取式儲存媒體 (Portable Computing Devices and Removable Storage Media) 管理政策；

19. 實施備份與復原 (Backup and Recovery) 政策，確保系統的復原能力；

20. 實施網絡保安 (Network Security) 控制，以僅容許獲授權的通訊進入網絡；

21. 實施應用程式保安 (Application Security) ，例如版本控制機制和隔離發展、以維持應用系統的完整性；

22. 實施記錄管理 (Log Management)，提供足夠的資料，以作為對保安措施的成效及遵行情況進行全面審計的憑證

23. 實施雲端運算保安 (Cloud Computing Security)，明確定義並落實雲端服務供應商和組織之間的資訊保安共同責任，確保提供適當保護；及

24. 實施供應鏈管理 (Supply Chain Management)，界定和制定流程和程序以妥善管理、覆檢保密及不可向外披露資料的有關協議。

（五） 事故應變責任

1. 電腦系統保安演習

- 營運者須參加由專責辦公室指定的電腦系統保安演習
- 演習的主題和範圍將由專責辦公室制訂

2. 委任 24／7 聯絡人

- 應委任至少兩名負責管理和運作關鍵基礎設施的關鍵人員擔任聯絡人，與專責辦公室就電腦系統保安事宜進行溝通
- 將任何變更盡快及按照法律指明的期限內通知專責辦公室

3. 應急計劃涵蓋的範圍，包括但不僅限於：

- 專責事故應變小組的架構及對應職務和職責；
- 啟動事故應變程序的指標；
- 確保遵行事故報告責任的報告程序；
- 減低事故影響和保存證據的程序；
- 調查事故原因和影響，並向專責辦公室提供協助調查的有關資料；

- 關鍵基礎設施回復正常操作狀態的復原計劃；
- 營運者與持份者及公眾的溝通計劃，包括制定溝通和協調的結構及模式
- 事故後覆檢程序，包括減低風險和防止再度發生事故的建議措施。
- 確保所有相關人員熟習緊急應變計劃
- 至少每 2 年一次，或當營運者的運作環境發生重大變化時，覆檢其緊急應變計劃

4. 電腦系統保安事故報告的要求

- 得悉[1]與系統相關的電腦系統保安事故後，須及時向專責辦公室報告

  初步報告

  - 可透過電子郵件、電話或短訊報告，內容應至少涵蓋事故的性質、受影響的系統及影響
  - 時限：嚴重電腦系統保安事故[2]須在得悉事故後 2 小時內；其他電腦系統保安事故則須在得悉事故後 24 小時內
  - 如果初步報告是透過電話或短訊方式報告，營運者須在報告後 48 小時內提交書面記錄報告

  書面報告

  - 營運者須在得悉事故後 14 天內，按照專責辦公室指定的事故報告表，透過指定渠道（如官方網絡）進一步向專責辦公室提交書面報告，以提供事故

---

1 「得悉」指合理確定事件已對關鍵電腦系統的機密性、完整性或可用性造成損害，或已損害其運作。為了確立事故是否已發生而進行的短期調查可能不被視為「得悉」。

2 嚴重事故指已經或即將對必要服務的連續性及關鍵基礎設施的正常功能造成重大影響，或導致個人資料等數據大量外洩的事故。

的詳情，包括原因、影響、補救措施。

- 營運者應按專責辦公室要求或指定的時間內向其報告事故的最新情況
- 營運者亦應確定相關證據得以保存，並進行適當調查，以找出事故原因，評估影響或潛在影響，以及制訂保安措施以防止事故再次發生。

附註：除部份由「指定監管機構規管」的「關鍵基礎設施營運者」外，此《實務守則》主要內容概覽一般適用於所有其他「關鍵基礎設施營運者」。「指定監管機構規管」可就其規管的「關鍵基礎設施營運者」發出相關指引。

附件四

擬議條例的主要建議

建議	
B. 規管範疇	
1.	只有被明確指明為「關鍵基礎設施營運者」及其「關鍵電腦系統」才受規管。
2.	「關鍵基礎設施」涵蓋兩大類，包括: 第一類：在香港提供必要服務的基礎設施，涵蓋八個界別— (a) 能源； (b) 資訊科技； (c) 銀行和金融服務； (d) 陸上交通； (e) 航空交通； (f) 海運； (g) 醫療保健；以及 (h) 通訊和廣播。 第二類：其他維持重要的社會和經濟活動的基礎設施。
C. 規管對象	
3.	採取「機構為本」，即以負責營運每個「關鍵基礎設施」的機構為一個單位，履行保障其電腦系統安全的責任。
4.	專責辦公室在決定某基礎設施是否「關鍵基礎設施」而需要被納入擬議條例規管時，考慮下列因素— (a) 該基礎設施遭到破壞、喪失功能或數據洩漏時對香港的必要服務及重要社會和經濟活動的影響； (b) 該基礎設施倚賴資訊科技運作的程度；以及 (c) 該基礎設施所控制的數據的重要性。
5.	只列出八個必要服務的界別名稱，而不公開個別「關鍵基礎設施營運者」的名單。
6.	繼續沿用現有的行政方法對政府各部門提供的必要服務作出規管，無需納入擬議條例。
7.	「關鍵電腦系統」：直接與提供必要服務有關或關乎設施核心功能的電腦系統，以及如受到干擾或破壞會嚴重影響正常運作的系統。

建議	
D.	**「關鍵基礎設施營運者」的責任**
8.	向「關鍵基礎設施營運者」施加的法定責任，包括在(I)架構；(II)預防及(III)事故通報及應對三方面－ **(I) 架構** (a) 在香港設有地址和辦事處（及報告任何隨後變更）； (b) 向專責辦公室報告有關「關鍵基礎設施」的擁有權和營運權的變更； (c) 設立電腦系統管理部門並由營運者公司的專責主管負責監管； **(II) 預防** (d) 向專責辦公室報告有關「關鍵電腦系統」的重大變化，包括對其設計、配置、安全或運行的重大變化等； (e) 制定及實施電腦系統安全管理計劃並提交計劃； (f) 進行電腦系統保安風險評估（至少每年一次）並提交報告； (g) 進行獨立電腦系統保安審計（至少每兩年一次）並提交報告； (h) 採取措施確保即使聘用了第三方服務提供者，營運者本身的「關鍵電腦系統」仍然符合相關法定要求；以及 **(III) 事故通報及應對** (i) 參與由專責辦公室舉行的電腦系統安全演習（至少每兩年一次）； (j) 制訂應急計劃並提交計劃； (k) 在指定時間內向專責辦公室報告有關「關鍵電腦系統」的保安事故: – 嚴重電腦系統安全事故：在得悉事件發生後 2 小時內； – 其他電腦系統事故：在得悉事件發生後 24 小時內。 應專責辦公室在調查事故或與上述第(I)至(III)類責任相關的罪行時所發出的要求，營運者必須提交其可取得的相關資料，即使該等資料位於香港境外。

建議	
E. 專責辦公室	
9.	成立一個隸屬保安局的專責辦公室，擬議條例賦權行政長官委任一名專員，負責帶領辦公室執行擬議條例下的工作。主要職能包括－ (a) 指明「關鍵基礎設施營運者」及「關鍵電腦系統」； (b) 制定《實務守則》，就「關鍵基礎設施營運者」應採取的措施提供建議； (c) 監察針對「關鍵基礎設施」的電腦系統保安威脅； (d) 協助「關鍵基礎設施營運者」應對電腦系統保安事故； (e) 調查及跟進「關鍵基礎設施營運者」違規情況； (f) 協調不同政府部門及專家，例如政府資訊科技總監辦公室、警方網罪科及香港電腦保安事故協調中心等，在制定政策及指引和處理事故方面的工作；以及 (g) 向「關鍵基礎設施營運者」發出書面指示，以堵塞可能出現的保安漏洞。
F. 個別行業的指定監管機構	
10.	指定個別行業監管機構為「指定監管機構」，負責監管這些必要服務行業的「關鍵基礎設施營運者」履行架構及預防的責任；而事故通報及應對的責任，除部分可能由專責辦公室指明豁免外，則由專責辦公室全權負責監管所有八個界別的「關鍵基礎設施營運者」。
11.	現階段指定－ (a) 金融管理局監管部分與銀行和金融服務相關的服務提供者；以及 (b) 通訊事務管理局監管部分與通訊和廣播相關的服務提供者。
12.	專責辦公室保留可向所有「關鍵基礎設施營運者」根據擬議條例發出書面指示的權力，不論該「關鍵基礎設施營運者」是否由「指定監管機構」監管。
G. 罪行及刑罰	
13.	建議罪行包括－ (a) 「關鍵基礎設施營運者」不履行法定責任； (b) 「關鍵基礎設施營運者」不遵從專責辦公室發出的書面指示；

建議	
	(c) 不遵從專責辦公室按法定調查權力提出的要求；以及 (d) 不遵從專責辦公室就提供與「關鍵基礎設施」有關的資料的要求， 在未有合理辯解下有以上行為，即屬違法，可遭檢控。
14.	各項罪行只針對機構，並不會在個人層面懲罰機構的主管或員工。但是若相關的違規行為涉及觸犯現有的刑事法例，則一如現時的情況，涉事人員亦有機會要負上個人刑事責任。
15.	罰則只有罰款，罰款會經法庭審訊而定，違者可處最高罰款港幣 50 萬元至 500 萬元不等；個別罪行也會就持續違法行為處以額外的每日罰款。
H. 專責辦公室的調查權力	
16.	賦權專責辦公室行使各種的調查權力，包括: (1) 應對保安事故的權力；以及 (2) 調查條例下罪行的權力。
I. 上訴機制	
17.	成立上訴委員會，讓營運者可就有關「關鍵基礎設施營運者」或「關鍵電腦系統」的指明，以及專責辦公室發出的書面指示提出上訴。
J. 附屬法例	
18.	賦權保安局局長藉附屬法例訂明或修訂一些關於專責辦公室權限或營運商法定責任和細節，例如— (a) 可被指明為「關鍵基礎設施」的必要服務類別； (b) 指定監管機構名單； (c) 專責辦公室可以向「關鍵基礎設施」的營運者索取的資料； (d) 需要向專責辦公室報告有關「關鍵電腦系統」的重大變化的類型； (e) 電腦系統安全管理計劃及獨立電腦系統保安審計的涵蓋範圍及模式； (f) 電腦系統保安風險評估及應急計劃的涵蓋範圍； (g) 需要向專責辦公室報告的電腦系統保安事故的類型；以及 (h) 提交報告的時限等。

建議	
K. 《實務守則》	
19.	賦權專責辦公室發出性質並非附屬法例的《實務守則》，列出在法例要求的基礎上的建議標準，例如獨立電腦系統保安審計師應具備的專業資格、審計涵蓋範圍、可參考的國際認可方法和標準、及報告及修正計劃的細節等。「指定監管機構」亦可就其規管的機構發出相關指引。

附件二

加強保護關鍵基礎設施電腦系統安全—建議立法框架
書面意見內容總覽和備註

A. 立法目的和原則

序號	意見和備註
1	就**整體立場**方面，收到 52 份支持政府就保護香港的關鍵基礎設施立法或為完善擬議條例內容或提出正面建議。意見認同「關鍵基礎設施營運者」(下稱「營運者」)須履行法定責任，亦從資訊保安和營運者角度提出實務建議，讓營運者順利實踐提升關鍵基礎設施電腦安全的目標。
2	就立法原則方面，有意見指出《討論文件》第 11(c)段立法原則提到「只會要求『關鍵基礎設施營運者』承擔起保護其『關鍵電腦系統』的責任，絕不涉及系統內的個人資料和業務內容」，與第 24(k)段要求指營運者必須報告「導致個人資料等數據大量外洩的事故」或出現矛盾（5 份）。 〔**註**：我們感謝界別持份者提出寶貴意見和專業建議，所有建議均會被慎重考慮。政府會繼續與各界別的持份者保持溝通，持續完善法律框架和《實務守則》內容。〕

B. 規管範疇

序號	意見和備註
1	就**資訊科技界別**，有意見認為定義太廣闊（5 份），當中有建議取消該界別（3 份），也有建議明確列出不會被納入規管的範圍（2 份）。

序號	意見和備註
2	就**第二類關鍵基礎設施（即其他維持重要的社會和經濟活動的基礎設施）**，有意見認為有需要進一步澄清定義（5份）；當中包括認為場地只為活動舉辦者提供設施及配套，應不屬關鍵基礎設施（1份）；詢問園區有何電腦系統會符合「關鍵電腦系統」的定義（1份）；建議取消該界別（1份）。
3	建議擴闊條例範圍以涵蓋**其他界別**： (a) 有建議認為「關鍵基礎設施營運者」的範圍，應擴闊以涵蓋高等教育及研究學府（2份）、緊急服務（1份）、食水供應（1份）、排污及廢物處理（1份）、食物製造（如屠宰業）（1份）及公開密碼匙基礎建設（1份）。 (b) 建議包含政府機構（如水務署等）（3份），當中建議訂明是否包含有政府參與或代表的機構（1份）。
4	就**域外司法權**方面，有意見建議條例只限適用於香港的營運者（2份）。 〔**註：**保安局參考了其他司法管轄區（包括美國、澳洲、新加坡、內地）的相關條例，認為把「資訊科技」列作其中一個關鍵基礎設施的界別，做法合適。至於個別機構及其營運者是否需要納入「資訊科技」界別，保安局將會以定義為基礎，與界別有機會被指明的營運者保持緊密溝通，方會作出決定。 擬議條例不具域外效力。專責辦公室會確認所要求的資料，均為在香港設有辦公室的營運者可以取得的資料，並給予合理時間準備。〕

C. 規管對象

序號	意見和備註
1	就「**關鍵基礎設施營運者**」方面： (a) 建議更清晰解說「關鍵基礎設施」及「必要服務」的定義和「關鍵基礎設施營運者」的指明條件（11份）。 (b) 查詢「數據中心」、「雲端服務供應商」及不受香港金融管理局（下稱「金管局」）規管的金融服務是否符合「必要服務」的定義（5份）。 (c) 關注營運者身份的保密性或向外界透露自身作為營運者身份的後果（5份）。當中亦有意見認為應容許營運者互相披露身份，促進經驗交流（2份）。 (d) 建議營運者須在認可域名服務供應商註冊並使用.hk域名（1份）。 (e) 建議更改「關鍵基礎設施營運者」(Critical Infrastructure Operator)的英文縮寫「CIO」，避免與「總資訊科技主任」(Chief Information Officer)一詞混淆（1份）。
2	就「**關鍵電腦系統**」方面： (a) 建議更清晰解說「關鍵電腦系統」的定義和指明條件（18份）。 (b) 查詢「關鍵電腦系統」是否涵蓋「運營科技」（Operational Technology），包括「監視控制與資料採集系統」（Supervisory Control and Data Acquisition，下稱SCADA）、「可編程邏輯控制器」（Programmable Logic Controller，下稱PLC，如交通燈系統）、「物聯網」（Internet-of-Thing，下稱IoT）、

序號	意見和備註
	與互聯網隔絕的「孤島模式系統」(Island System)（7份）。 (c) 認為如果擁有故障安全（fail-safe）或「業務連續性規劃」(Business Continuity Planning)，即能夠確保系統故障時，業務仍可以正常運作，則該系統不應被指明為「關鍵電腦系統」（1份）。 (d) 查詢例如「微軟 365」、「亞馬遜雲」等服務及在域外連接到「關鍵電腦系統」的電腦設施是否會被指明（1份）。
3	**就「關聯」（interconnected）的定義：** 查詢「關聯」的範圍是否包含「安全信息和事件管理系統」（Security Information and Event Management，下稱SIEM）、「中間軟件系統」（Middleware，如網站伺服器、數據庫連接器）、裝載應用軟件（如微軟 Active Directory 及 Office 365），其服務中斷會影響關鍵電腦系統提供服務的關連系統（8份）。
4	就「**嚴重影響**」方面，有建議更清晰解說該詞定義（5份）。
5	就**指明條件**方面，收到9份問題或建議，內容包括： (a) 建議在考慮指明營運者時，應同時考慮其「關鍵電腦系統」是否符合相關定義和門檻，而不應先行指明營運者，再指明「關鍵電腦系統」（2份）。 (b) 建議邀請潛在營運者參與決定應否被指明（1份）；詢問是否需要營運者同意才被指明（1份）；詢問如營運者不同意時的處理機制（1份）。 (c) 建議以原則分階段指明、分級管理各層次的營運者

序號	意見和備註
	（1份）。 (d) 詢問如母公司被指明時，是否所有其子公司均需要負起法定責任（1份）；詢問如某機構被指明時，其母公司會否被自動指明及需要負起法定責任（1份）。 (e) 詢問除被指明的電腦系統外，關鍵基礎設施的實體保安是否會列入監管之列（1份）。 〔**註**：專責辦公室在指明「關鍵基礎設施營運者」和「關鍵電腦系統」時，將會以定義為基礎，並透過與營運者相互溝通及了解，考慮其他相關因素，以確定是否適合。 擬議條例有關「關鍵電腦系統」的定義是考慮到香港的情況及參考了其他司法管轄區的相關法律後制定的。因此，我們認為現時的定義是合適的。專責辦公室將按定義及與營運者充分溝通，經通盤考慮後方會指明營運者賴以提供必要服務的電腦系統為「關鍵電腦系統」。然而，由於「關連」（interconnected）此詞彙可能未必精準反映「關鍵電腦系統」的考慮因素，保安局會積極考慮予以刪除。〕

D. 「關鍵基礎設施營運者」的責任

I. *架構*

序號	意見和備註
1	就**擁有權**方面，有建議取消匯報更改的要求（2份），詢問如何定義變更擁有權（1份），詢問會否以國家安全角度考慮限制擁有者的國籍（1份）。

序號	意見和備註
2	就**營運權**方面，詢問更改營運權的定義（3份）；詢問如何處理少於三個月內發生的更改（2份）。
3	就**匯報**方面，有建議只有當營運權發生可能造成不利影響時才需要匯報（2份）；建議只限回報已知更改（1份）。
4	就**電腦系統安全管理部門**方面收到以下意見或詢問： (a) 建議清晰列明主管及人員合符資格的學歷和經驗的最低要求及認可專業資歷的名單（6份）。 (b) 資訊科技業界認為部門人員須有較高資歷和較深經驗（4份）；潛在營運者則考慮到人才短缺因素，建議只設最低要求或把人員資歷納入非必要標準（3份）。 (c) 建議及／或詢問部門人員可否由組織的資訊科技部門人員兼任（4份）。 (d) 詢問可否外判與第三方服務供應商、由母公司相關部門兼任或部門人員是否必須駐守香港（3份）。 (e) 詢問是否需要對部門人員進行背景審查（1份）。 (f) 詢問如主管人員有變更時是否需要匯報（1份）。 (g) 建議須由合資格的主題專家（subject matter expert）擔任主管（1份）。 (h) 詢問會否參考新加坡的做法，設立及維持合資格的專業資訊科技人員名單（1份）。 〔**註**：保安局理解營運者在通報「擁有權」變更時可能遇到的實際困難，會積極考慮移除有關要求。

序號	意見和備註
	擬議條例並無針對營運者的電腦系統保安人員的法定資格要求。保安局會在制定《實務守則》時詳列合乎標準的專業資歷名單，便利營運者聘請合適人員。〕

II. *預防*

序號	意見和備註
1	就**報告「關鍵電腦系統」變化**方面，收到以下意見或詢問： (a) 建議清晰列明需要通報的「重大變化」所包含有關系統、技術、配置或更新保安設定的涵蓋範圍（9份）。 (b) 認為需報告的條件及範圍不清晰（2份）；建議僅在「關鍵電腦系統」發生可能產生負面影響的重大變更時才須匯報（4份）。 (c) 建議列明匯報方法（1份）及頻率（1份）；首年、次年和後續年份的匯報要求（1份）；提供匯報樣本（1份）。 (d) 建議在《實務守則》列明「關鍵電腦系統」的分類和與專責辦公室的溝通機制（如新建系統會否符合「關鍵電腦系統」的定義）（1份）。 (e) 建議提供更有彈性的匯報和提交報告期限（2份）。 (f) 詢問進行「關鍵電腦系統」改變前是否需要取得同意，如不同意是否需要還原（1份）。 (g) 詢問如有不合規事項，營運者是否須在修正期間和完成後進行匯報，及需要進行後續審計（1份）。

序號	意見和備註
	(h) 建議應要求詳盡記錄有關「關鍵電腦系統」的變更，以確保透明度和問責性（1 份）。 (i) 擔心如匯報「關鍵電腦系統」的改變，可能會披露商業機密（1 份）。
2	就**資料披露**方面，收到 11 分建議或問題，包括： (a) 建議只披露一般資料，而不涉及營運機密（2 份）。 (b) 認為「關鍵電腦系統」的設計、配置、營運等資訊不宜披露（2 份）。 (c) 建議披露時隱藏敏感資訊（例如品牌、軟體版本、IP 位址），除非發生嚴重事故（1 份）。 (d) 建議只限按「需要知道」的原則披露最少資料（1 份）。 (e) 詢問會收集哪些關於「關鍵電腦系統」的敏感資料（1 份）。 (f) 建議明確豁免提供與國家安全、個人私隱及商業機密等資料（2 份）。 (g) 詢問專責辦公室在調查事件有否保護「關鍵電腦系統」及其敏感營運資訊相關的的規定（1 份）。 (h) 建議就資料的跨境流通進行嚴格規管和提供明確指引（1 份）。
3	就**電腦系統安全管理計劃**方面，收到以下意見或詢問： (a) 詢問會否或建議採用國際標準化組織，如（International Organization for Standardization，下

序號	意見和備註
	稱 ISO）、國際電工委員會（International Electro-technical Commission，下稱 IEC）等標準（如 ISO 27001、IEC 62443)（4 份）。 (b) 詢問是否需要定期覆核計劃或覆核頻率為何（2 份）、能否由母公司涵蓋覆核計劃（1 份）。 (c) 建議提供實用指引保護「關鍵基礎設施」（1 份）。 (d) 建議計劃涵蓋的範圍採用風險優先順序、分配充足的預算制定計劃、分階段升級系統安全、考慮廠商合作等因素（1 份）。 (e) 建議清楚列明管理計劃涵蓋範圍（1 份）、建議需要匯報的管理計劃改變項目及訂定匯報時限（1 份）、登入記錄的保留時限（1 份）、何謂「系統運行的正常行為基準」（1 份）、會否在保密性和保密協議管理方面訂立要求（1 份）、是否覆蓋攻擊面管理（即實時持續發掘潛在攻擊面）（1 份）。 (f) 建議傳統（legacy）或隔離互聯網系統毋須連續監察（1 份）。 (g) 建議在以下方面提升基線以上要求，內容包括： - 實施最先進的網絡安全技術，例如先進的加密和以人工智能為基礎的威脅偵測系統（1 份）。 - 實施資產管理，以確保「關鍵電腦系統」的最新庫存（1 份）。 - 引入情報主導的「紫隊」（1 份）。 - 使用安全的私有雲或混合雲解決方案來儲存和管理關鍵資料與服務（1 份）。
4	就**風險評估**方面，收到以下意見或詢問： (a) 建議採取風險為本模式進行評估、制定保安控制、審計及測試（4 份）。

序號	意見和備註
	(b) 建議按照國際標準及框架制定範圍（2 份）；清楚指明範圍和準則以覆蓋關鍵範圍，包括處理在營運科技（Operation Technology，下稱 OT）上進行滲透測試的挑戰（1 份）、是否覆蓋第三方服務供應商（1 份）、是否只針對「關鍵電腦系統」（1 份）、會否按界別覆蓋內部和外部風險（1 份）；提供指引及樣本（1 份）。 (c) 建議接納由機構內審部門進行評估（1 份）、接納現有由獨立第三方的認證和報告（2 份）、合併風險評估和審計（2 份）、與金管局的「網絡安全風險評估框架」（Cyber Resilience Assessment Framework，下稱 C-RAF）看齊，減少評估頻率為兩年一次（1 份） (d) 詢問如果機構進行風險評估的頻率高於規定的每年一次，是否每次評估後均需要提交報告（1 份）。 (e) 詢問「關鍵電腦系統」 進行重大改變後，是否需要進行漏洞評估和滲透測試。（1 份）
5	就**保安審計**方面收到 12 份問題或建議，內容包括： (a) 建議列明審計人員資歷（2 份）、其資歷需與現行監管框架看齊（1 份）。 (b) 建議列明審計人員的獨立性（即是否接受由機構內審部門人員或主題專家進行）（2 份）、特別接達管理（Privileged Access Management）審計接受由機構內審部門人員進行（2 份）。 (c) 建議確保營運者和業界採用一致標準和品質，例如按照《資訊科技保安政策》（下稱 S17）、《資訊科技保安指引》（下稱 G3）、Council of Registered Ethical Security Testers（下稱 CREST）、MITRE Adversarial Tactics, Techniques, and Common Knowledge（下稱

序號	意見和備註
	MITRE ATT&CK）框架、ISO 27001、第二類服務組織控制報告（Service Organization Control Type 2，下稱 SOC2）等標準（1 份）。 (d) 建議列明評估風險是否審計的一部份（1 份）、審計是否著重於測試控制的有效性或識別與評估內在風險（1 份）。 (e) 建議營運者必須負責瞭解獨特的安全弱點，而非僅遵循監管機構或審計人員提供的指引（1 份）。 (f) 建議列明完成審計的定義（完成審計實地工作與簽發審計報告之間通常會有時間差距）（1 份）。 (g) 詢問在進行獨立審計的年度，可否使用該報告來滿足年度評估要求（1 份）。 (h) 建議增加審計頻率至每年一次（1 份）。 (i) 詢問如有理據支持，可否申請豁免審計（1 份）。
6	就**提升基線要求**收到以下問題或建議，內容包括： (a) 建議制定前瞻性網絡安全策略，包括風險評分、風險優先順序和風險暴露分析（1 份）； (b) 建議持續監察風險（1 份）； (c) 建議鼓勵或強制使用紅隊（攻擊隊）（1 份）； (d) 建議進行情報主導的網絡攻擊模擬測試（intelligence-led cyber attack simulation testing，下稱 iCAST）（1 份）； (e) 建議着重營運商的事故復原能力（1 份）； (f) 建議考慮制裁風險（1 份）； (g) 建議加入人工智能元素（1 份）； (h) 建議考慮 24×7 品牌聲譽保障（1 份）； (i) 建議鼓勵營運者和供應商協助管理和減低網絡風

序號	意見和備註
	險（1 份）； (j) 建議採用 MITRE ATT&CK 框架，以更好應對已知風險（1 份）； (k) 建議考慮採取雲端備份代替異地（off-site）磁帶備份（1 份）；及 (l) 詢問是否需要設立全天候保安運作中心（SoC）、採用端點偵測與回應（endpoint detection and response，下稱 EDR）系統（1 份）、全天候監察暗網的網絡風險情報（1 份）； (m) 詢問就風險評估，會否就所發現的風險按嚴重程度制定等級。如有，是否應按等級設定修復時限（1 份）。 〔**註**：保安局將會參照最新科技及國際標準，制定《實務守則》的相關內容，提供符合法定要求的建議標準。 擬議條例並非針對「關鍵基礎設施營運者」系統內的個人資料和商業機密。專責辦公室要求營運者提供的資料，旨在確保營運者妥善履行保護其「關鍵電腦系統」的責任，並確保其「關鍵電腦系統」遇到事故時，專責辦公室能有效評估事故對社會的嚴重性和對其他營運者的威脅。因此，專責辦公室在執行擬議條例下的職能時，會按法例要求「關鍵基礎設施營運者」提供必須的資料。 我們認為獨立性是審計其中一個基本的原則，而審計人士應該獨立於被審計方，以避免任何利益衝突，確保審計公正客觀。專責辦公室會參考國際認可的標準和相關專業資格，在《實務守則》詳細列明對審計人員資歷的要求。〕

III. 事故通報及應對

序號	意見和備註
1	就**安全演習**方面收到 12 份問題或建議，內容包括： (a) 建議或查詢能否訂立最低要求或規模以盡量減少服務中斷，包括接受營運者恆常進行而規模相近的演習（4 份）、由營運者自行或「指定監管機構」舉辦演習（2 份）、豁免在營運科技（OT）系統進行流動掃描或滲透測試（2 份）。 (b) 建議以風險為本原則舉辦演習（2 份）。 (c) 詢問演習是按照白盒測試（基於充分瞭解系統內部運作設計的測試）或黑盒測試（按照現實網絡攻擊手段進行測試，無需預先了解系統內部運作）（1 份）。 (d) 詢問是否會在基線以上，按營運者的威脅概況進行模擬情境測試（1 份）。
2	**就「嚴重事故」的定義**，有 11 份建議更清晰解說「嚴重事故」的定義或提供評估矩陣（assessment matrix）作為參考。
3	就「**其他須匯報事故**」的定義，收到以下意見或詢問： (a) 認為有需要進一步細化「其他須匯報事故」的定義，例如清晰列明由系統錯誤、人為錯誤、停電等非網絡攻擊所引致的事故、不涉及必要服務受阻的資料洩漏事故和營運者認為風險在可控範圍內的事故是否需要通報（17 份）。 (b) 認為無須通報不影響系統安全及提供必要服務的資料洩漏事故（1 份）。 (c) 詢問營運者在哪些資料外洩的情況下需要作出報

序號	意見和備註
	告，例如資料數量、來自「關鍵電腦系統」等（1份）。 (d) 詢問如資料外洩源於非「關鍵電腦系統」（而該資料來自「關鍵電腦系統」）時是否需要作出報告（1份）。
4	就「**得悉**」／「**短期調查**」的定義，收到以下意見： 認為有需要進一步細化「得悉」和「短期調查」的定義，以防出現因為未能在法定時限內確定事故起因所作出的過度匯報（8份）。
5	就**應急計劃**方面，收到2份問題，包括： (a) 查詢是否需要由營運者的主題專家參與數碼法理鑑證和調查工作（1份）。 (b) 查詢專責辦公室在事故中提供協助為何，以供考慮納入應急計劃（1份）。
6	在**事故通報**時限方面，收到以下意見或詢問： (a) 認為在得悉嚴重事故後兩小時內匯報時間並不足夠（8份），建議延長至24小時（1份）。 (b) 認為在得悉其他事故後24小時內匯報時間並不足夠（2份），建議延長至72小時（3份）。 (c) 認為通報時限與金管局（1份）和通訊事務管理局（1份）定立的準則不一致。 (d) 建議訂明容許延長通報時限的情況（2份），並為營運科技（OT）系統的事故訂定另一套通報時限。 (e) 建議豁免涉及第三方（尤其位處境外）服務供應商的事故的通報時限（1份）。

序號	意見和備註
	(f) 詢問如未能找到事故原因，是否不需要匯報(1份)。
7	在**通報對象**方面，收到7份問題或意見，包括：
	(a) 除了向專責辦公室通報事故外，是否仍須通知其他相關機構（如警方、金管局、通訊事務管理局等）（3份）。
	(b) 建議定立清晰通報機制提升應對速度（2份）。
	(c) 建議制定協調機制，以確保精簡流程，避免雙重報告（2份）。
8	在**通報資訊**方面，收到以下問題或意見：
	(a) 建議定立清晰指引或範本(5份)，列明各類事故所需匯報內容的最低要求（1份）。
	(b) 建議需報告在系統中發現的漏洞（1份）。
	(c) 詢問是否須向專責辦公室及可能受影響的用戶報告及披露保安漏洞？如是，專責辦公室會否推出協調漏洞揭露與支援的計劃，以協助並促進營運者揭露事故後的緩解程序（1份）。
	〔**註**：保安局理解營運者在通報時可能遇到的實際困難，並參考了英國、歐盟及美國的相關要求，會積極考慮把通報嚴重電腦系統保安事故的時限，由得悉後兩小時放寬至12小時，而其他事故則由得悉後24小時放寬至48小時。同時，為確保有效及早應對事件，我們參考了新加坡和澳洲的做法，建議賦權專責辦公室在營運者賴以提供必要服務的「關鍵電腦系統」已經或可能受干擾或服務中斷時，可主動向營運者調查其原因以確定是否由攻擊引致。

序號	意見和備註
	擬議條例中，電腦系統保安事故是指未經合法授權在電腦或電腦系統上或透過電腦或電腦系統進行，而對其網絡安全或另一台電腦或電腦系統的網絡安全構成危害或不良影響的行為或活動。《實務守則》將會詳細說明「須匯報事故」的涵蓋範圍及列舉例子。 擬議條例建議要求營運者至少每兩年一次參與由專責辦公室舉行的電腦系統安全演習，該要求參考了不同司法管轄區包括新加坡的做法和國際標準而釐定，我們認為有關電腦系統安全演習的要求和安排是合適的。〕

E. 專責辦公室

序號	意見和備註
1	就**書面指示**方面，收到以下詢問或建議： (a) 關於書面指示(「指示」)，詢問在甚麼情況下專責辦公室會發出指示（1份）、指示的內容為何（1份）、營運者收到指示後的責任（1份）、預計回應時限（1份）。 (b) 建議避免發出臨時緊急書面指示（例如要求儘快修復最新發現的漏洞）（1份）。
2	就**資料保密性**方面，收到以下建議或問題，包括： (a) 詢問專責辦公室有何措施確保收集、保存、銷毀所收到的資料（5份）。 (b) 詢問專責辦公室的保密責任為何（2份）。

序號	意見和備註
	(c) 建議除得到營運者同意外，專責辦公室從營運者收集的資料不得與其他政府部門分享（1份）。 (d) 建議訂立保密協議和溝通指引（1份）。
3	關於**收集網絡風險情報**，收到以下建議： (a) 建議或詢問專責辦公室會否透過主動持續收集網絡風險情報及整合營運者匯報的情報，並與營運者分享，提升整體抵禦網絡風險的能力（4份）。 (b) 建議與持份者協作，建立保安營運中心（SoC）、網絡營運中心（Network Operation Center，下稱 NoC）等提升網絡安全水平（1份）。 (c) 認為傳統的安全信息和事件管理（SIEM）系統或保安營運中心（SoC）缺乏事故應變或情報獵取的能力（1份），營運者需要採取主動及情報獵取模式進行事故應變調查（1份）。
4	關於**與警方之間的分工**，收到以下詢問： (a) 詢問專責辦公室與警方在進行調查時的分工（1份）。 (b) 是否需要同時匯報事故給警方及／或其他單位（如私隱公署）、香港網絡安全事故協調中心）（2份）。 (c) 警方在何情況下會進入營運者處所進行保安檢查（1份）。
5	就與**私隱公署分工**方面，收到以下建議或問題： (a) 查詢就涉及個人資料外洩事件，是否需要同時匯報私隱公署（2份）。

序號	意見和備註
	(b) 建議若事故涉及個人資料外洩，須通知受影響的資料當事人（1 份）。 (c) 建議與私隱公署更好協調（1 份），避免因重複匯報或調查帶來混淆（2 份）。 (d) 建議考慮看齊《私隱條例》日後可能作出的修訂（1 份）。
6	就**多邊協作**方面，建議專責辦公室考慮與內地簽訂雙邊協議，以確保跨境服務在網絡安全方面的合規與合作（1 份）。
7	就處理**域外法例兼容性**方面，收到 2 份問題或建議，包括： (a) 詢問假如跨國規模的供應商遵守本條例而導致與某些境外法例或國際標準出現衝突，專責辦公室如何處理（1 份）。 (b) 建議與內地網絡安全標準及國際良好作業保持一致性（1 份）。 〔**註**：擬議條例並非針對「關鍵基礎設施營運者」系統內的個人資料和商業機密。專責辦公室會按照相關法例和內部指引處理有關資料，亦會設立內部保密系統以確保資料傳送及貯存的安全性。 專責辦公室及公署要求事故通報的目的及內容有所不同，前者負責找出發生洩露的原因並儘快堵塞漏洞，後者則著重保障個人資料的私隱；故此，若發生的事故涉及網絡攻擊電腦系統引致洩露個人資料，營運者確然需要同時向專責辦公室及公署報告，但並不存在「重複」工作，

序號	意見和備註
	因兩類報告要求的目的及跟進工作並不相同。〕

F. 個別行業的指定監管機構

序號	意見和備註
1	就「指定監管機構」方面，收到以下建議或詢問： (a) 建議每個界別都應設有「指定監管機構」(1份)。 (b) 詢問何時會公布「指定監管機構」名單（1份)。
2	就「**部份相關服務提供者**」的定義方面，有建議澄清金管局是否只會監管其界別內的銀行實體，而不包括其他屬於銀行及金融服務界別內的非銀行實體（1份)。
3	就**個別界別**的規管事宜方面，收到以下建議或詢問： (a) 就**銀行和金融界別**，詢問會否或建議指明證監會、保險業監管局和積金局為「指定監管機構」及指明/不指明的相關考慮因素（1份)。 (b) 詢問現時非金管局監管的營運者於法例生效後會否改由金管局規管（1份)。
4	就**協調個別行業需求**方面，收到以下問題或意見： (a) 建議按行業需要制定《實務守則》和進行風險評估等，而非一刀切制定要求（6份)。 (b) 詢問可否跟隨母公司看齊被金管局監管（該機構現時不屬金管局監管)(1份)。 (c) 建議沿用現存監管機制以簡化要求，避免同時向多個監管者匯報（2份)。

序號	意見和備註
	(d) 建議考慮最大兼容性，以避免重複或不一致要求（3份）。 (e) 建議僅納入整體原則，細節交由業界監管機構制定（1份）。 (f) 詢問如何取得平衡確保現時對電腦系統保安要求較低的界別不會成為惡意行為者的目標（1份）。
5	就**航空交通業**，有建議指明民航處為「指定監管機構」（1份）。 〔**註：**指定界別的「關鍵基礎設施營運者」將透過遵循由該界別指定監管機構所發出的指引，履行擬議條例的「架構」及「預防」法定責任。此外，《實務守則》除引入各界別通用的基線要求外，亦會透過與不同界別保持緊密溝通及風險評估，制定並詳細列出相關營運者適用的標準及方法，協助其滿足法定要求。〕

G. 罪行及刑罰

序號	意見和備註
1	就**罰則**方面，收到以下建議或問題： (a) 建議着重提高營運者的網絡韌性和復原能力而非予以懲罰（2份），避免營運者流於形式上合規（1份）。 (b) 建議清晰列明須負上個人刑責的情況（2份）、釐清公司董事或管理層會否因疏忽而負上個人刑責（1份）、列明不會負上個人刑責的情況（1份）；限制個人刑責（2份）。

序號	意見和備註
	(c) 詢問或建議清晰列明可接受為「合理辯解」的情況和例子（3份）、為第三方不遵守規定或已盡最大努力的安全港條款（3份）、免除自我舉報不合規情況的刑責（2份）。 (d) 建議清晰列明如何計算罰則（6份），釐清最高罰款屬單次或累計罰款（2份）、會否按公司規模或財政狀況而異（2份）、有否加重或減輕刑責的因素（1份）、招致每日罰款的罪行（1份）。 (e) 詢問如子公司干犯罪行，母公司會否受影響（1份）。 (f) 詢問與「指定監管機構」予以罰則有何不同（1份）；會否導致雙重懲罰（1份）。 (g) 認為罰款太輕（1份），建議按公司規模和財政能力罰款（1份）；建議延伸罰則至供應鏈上游（1份）；認為罰款太重（1份）；建議取消每日罰款（1份）；建議減輕對輕微不合規的罰則（1份）。
2	就**第三方服務法律責任**方面，收到以下問題或建議： (a) 認為儘管第三方服務供應商身處香港或境外，營運者亦難以對其作出控制，確保其遵守協議和法規（8份）。 (b) 建議法例指名第三方服務供應商需分擔的責任（4份）、賦權營運者監督第三方服務供應商（2份）或要求把第三方服務納入風險評估範圍（1份）。 (c) 建議免除營運者對第三方服務供應商不合規行為的責任（2份）。 (d) 建議容許按「需要知道」的原則向第三方服務供應商披露營運者指名的身份（3份）。

序號	意見和備註
	(e) 建議定立清晰管理第三方服務的指引(6份),包括: - 需執行的措施(1份)。 - 可接受的國際標準或框架(1份)。 - 是否適用於外判員工(1份)。 - 如規定與海外法例不兼容時的處理方法(1份)。 - 如營運者同時擁有第三方服務供應商的身份(1份)。 - 營運者對第三方服務商提供責任指派(RACI)矩陣(負責者 Responsible、問責者 Accountable、諮詢者 Consulted 和知情者 Informed)(1份)。
3	就法例**生效時間**方面,收到以下建議或問題: (a) 設寬限期予業界評估系統風險、制定事故應變計劃、聘請人才、與第三方服務(14份)供應商(在合約期間或待合約完成後)磋商條款等;建議寬限期至少為12個月(1份)。 (b) 建議按風險為本準則,法例分階段先覆蓋較關鍵的第一類服務、容許營運商先處理較關鍵的電腦系統(7份)。 (c) 建議明確公布時間表(1份)。
4	就**檢討法例和政策**方面,收到以下建議或意見: (a) 建議成立領導委員會、顧問委員會、專案小組、工作小組、平台等提升專責辦公室和業界溝通和經驗分享,以制定更佳政策和完善《業務守則》(5份)。 (b) 詢問有否機制聽取或邀請個別營運者提供意見(2份)。 (c) 建議與營運商、網絡安全專家及業界法規主管持續對話並參考國際標準,以收集持續的回饋並釋除疑慮(2份)。

序號	意見和備註
	〔**註**：是次立法的原意並非懲罰營運者，訂立罪行及罰則旨在確保條例能有效實施及執行。擬議條例的罪行及罰則是考慮到香港的情況及參考了其他司法管轄區的相關法律後制定的。因此，我們認為現時的罰則是合適的。專責辦公室會積極協助營運者提升架構及預防保安事故的水平，避免觸犯法例。 擬議條例容許「關鍵基礎設施營運者」聘用第三方服務提供者，但營運者仍需要負起履行條例下的相關法定責任。保安局會積極參考其他司法管轄區的經驗，在《實務守則》提供更多如何完善履行「盡責查證」(Due Diligence)及「合理努力」(Reasonable Endeavour)的指引，為「關鍵基礎設施營運者」在聘用第三方服務提供者時訂定及履行合約提供參考。 政府的目標是在擬議條例通過的一年內成立專責辦公室，以期讓法例可於其後半年內正式生效。期間，保安局和專責辦公室會與有機會被指明的營運者保持緊密溝通，按風險和機構準備程度分階段指明「關鍵基礎設施營運者」及其「關鍵電腦系統」，並制定《實務守則》的相關內容。條例中附設期限的法定要求，例如進行風險評估或獨立審計，以及提交相關報告等，將會由指明後才開始計算。因此，有機會被指明的營運者應有充足時間準備。〕

H. 專責辦公室的調查權力

序號	意見和備註
1	就「**處所**」的定義方面，認為英文版本「relevant premises」的定義不清晰（註：中文版本只有「處所」一詞（3份）。

序號	意見和備註
2	就「**相關資料**」的定義方面，認為用詞含義太廣（2份）。
3	就**賦權**專責辦公方面，收到以下意見或建議： (a) 建議只賦予最少調查權、需有法律授權、可上訴及覆核（2份）。 (b) 詢問授予調查權的客觀門檻或條件為何（2份）。 (c) 建議移除連接關鍵電腦系統或在系統安裝程式的權利，除非有足夠的法律授權（2份）。 (d) 詢問專責辦公室有否權力進行現場檢查（包括隨機抽查）（2份）。 (e) 詢問調查期間會要求哪類型資料（1份）。 (f) 詢問如何處理涉及受法律專業保密權的資料（1份）及有否權利要求取得法律特權（1份）。 (g) 建議就記錄和保存數碼法理證據提供指引（1份）。 (h) 建議專責辦公室在緊急情況下可授權發出手令或遙距控制關鍵電腦設施（1份）。 (i) 詢問如何進行跨境調查（1份），例如境外第三方雲端服務供應商（1份）。 (j) 詢問如營運商要從海外取證或與海外分享資訊，有否任何指引（1份）。
4	關於**營運者權責**方面，收到以下詢問或建議： (a) 詢問被調查方是否有權尋找律師代表（1份）。 (b) 詢問進入數據中心的標準與程序為何（資料中心可

序號	意見和備註
	能不知道客戶所犯的罪行）（1 份）。 (c) 詢問專責辦公室各人員的職能、會否尋找第三方擔任主題專家或諮詢委員（1 份）。 (d) 建議修復工作由最熟悉「關鍵電腦系統」的營運者進行（1 份）。 〔**註**：擬議條例訂明，只有當發生嚴重事故時，營運者不願意或未能自行應對事故，專責辦公室才會考慮向裁判官申請手令，因應必要性、適當性、相稱性及公眾利益，在「關鍵電腦系統」連接設備或安裝程式，以應對事故。其他司法管轄區（如澳洲和新加坡）的相關監管機構也擁有類似的權力。〕

I. 上訴機制

序號	意見和備註
1	就**上訴機制**收到以下建議或詢問： (a) 詢問上訴委員會的組成方法（3 份）：包括成員是否有界別專業知識（1 份）、如何同時合乎保密性和維持獨立性（1 份）。 (b) 詢問有否進行上訴的指引（1 份）、服務承諾（1 份）、上訴委員會的決定是否最終決定，及可否尋求進一步覆核（2 份）。 (c) 詢問上訴會否涉及費用（1 份）。 (d) 詢問營運者在上訴進行時是否仍需遵從專責辦公室指令（1 份）。

序號	意見和備註
	(e) 建議在兼容性方面考慮現行私隱公署處理上訴事宜的機制（按《行政上訴委員會條例》（第 442 章）處理）（1 份）。 (f) 詢問如營運者不同意法庭手令內容或專責辦公室行使的調查權，如何提出上訴（2 份）。 〔**註**：保安局參考了現時不同法定上訴委員會的安排，建議擬議條例下的上訴委員會由大約十五位來自業界、網絡安全及法律專業的專家組成團隊（包括一位委員會主席），並由特首委任。委員會成員須與專責辦公室保持獨立。每次進行上訴聆訊時，會由三位委員進行聆訊。三位成員必須申報沒有利益衝突（例如行業競爭者），並對聆訊內容簽署保密協議。〕

J. 附屬法例

序號	意見和備註
1	就**附屬法例**方面，收到以下建議或意見： (a) 建議澄清行使附屬法例擴大界別等的時間和機制（1 份）。 (b) 擔憂訂立附屬法例會繞過立法程序（2 份）。 〔**註**：附屬法例的制定或修訂有既定和相當嚴謹的程序，確保公平、公開、公正和透明，並且由立法會監察。〕

K. 《實務守則》

序號	意見和備註
1	在**電腦系統保安管理計劃**下的**監察和偵測機制**方面，收到建議列明「隔離」是指開發（development）環境與測試（testing）環境隔離、與生產（production）環境隔離，還是兩者（1份）。
2	在**電腦系統保安管理計劃**下有關**電腦系統保安培訓**方面，收到以下問題或建議： (a) 建議清楚列明訓練範圍、深度、方法及受訓人員類別（如操作員、維護人員、供應商、承包商和服務供應商）（2份），澄清是否需要為承包商和服務供應商提供培訓（此舉並非業界主流）（1份）。 (b) 詢問培訓是否需要按受訓人員職能制定（1份）；是否需包含理論和實踐訓練（1份）。 (c) 建議強制進行網絡安全培訓（1份）、要求營運者投入更多培訓資源（1份）。 (d) 建議專責辦公室協助營運者制定網絡安全訓練或提供支援（1份）。 (e) 詢問本地是否有足夠網絡安全審計人員和紅隊（攻擊隊）以外的網絡安全保衛人才（1份）。 (f) 找不到香港互聯網註冊管理有限公司提供的培訓（1份）；詢問除該公司提供的培訓以外還有何員工培訓支援（1份）。 (g) 詢問政府有否計劃加強網絡安全人才供應（1份）。 (h) 建議為中小企提供更多培訓（1份）。
3	在**事故應變**責任下，就**委任24/7聯絡人**方面，詢問聯

序號	意見和備註
	絡人是否必須在香港工作，能否由代表辦公室代表（2份）；建議可由安全營運中心（Security Operation Center，下稱 SOC）作為聯絡點（1份）；詢問可否由電腦系統安全管理部門兼任（1份）。
4	就**制定時間**方面，收到以下問題或意見：
	(a) 詢問發行《業務守則》時間（3份）和落實時間（1份），並建議盡早發行《業務守則》（1份）。
	(b) 發行《業務守則》後給予營運者充足時間準備細節（1份）。
5	就**制定內容**方面，收到以下問題或意見：
	(a) 建議邀請界別專家參與制定內容，並廣泛諮詢業界意見（5份），或由專業機構制定（1份）。
	(b) 建議及詢問會否按照國際標準，如 ISO、SOC2、美國國家標準技術研究所（National Institute of Standards and Technology，下稱 NIST）框架（4份）。
	(c) 詢問整體方向（1份）；建議包含詳盡內容，例如資產辨別和管理、風險評估、風險偵測、保安審計、滲透測試、設計、配置、營運、實施、事故應對和調查、保存證據、事故影響評估、事故復原等方面訂明要求、方法和標準，並提供指引（7份）。
	(d) 建議務實提供指引應對供應鏈問題（1份）、包含實施加密金鑰管理（1份）。
	(e) 建議容許彈性處理近年才倡議的「安全設計」要求（1份）。
	(f) 建議內容保持技術中性（1分）。

序號	意見和備註
	(g) 建議在接達控制方面，只要求備存接達和嘗試接達系統的日誌合理時間，而非備存所有日誌（1 份）。 (h) 建議成立工作小組進一步了解第三方服務環境的獨特性，以完善守則內容（1 份）。 (i) 建議着重原則，無需指定和限制網絡安全產品（1 份）。 (j) 就提升基線要求收到 2 份問題及建議，內容包括： - 對於存取控制、帳戶管理、特權存取管理，是否需要類似 C-RAF 與 NIST 等更仔細要求，以強制執行良好作業。 - 對於基線維護，是否需要固化（hardening）檢查。 - 對於修補管理，會否擴展至威脅與漏洞管理。 - 會否建議推行漏洞獵取或漏洞揭露計劃。 - 對於修補管理，有否快速更新的明確指引。 - 如何定義備份與復原中的「充分」，是否需要後備場地。 - 如何推行安全工作前置（又稱「左移」shift left）並採用「開發、安全、營運」（development, security, operations，簡稱 DevSecOps） 方法來達至設計安全。 (k) 建議與業界持續對話，因應科技發展制定新的要求和完善實務守則（2 份）。 〔**註**：專責辦公室在制定《實務守則》時，會充分考慮業界持份者意見，按照界別的獨特性，以現行國際標準或行業獨特性，制定切實可行的要求。專責辦公室亦會持續檢視和完善《實務守則》的內容。 專責辦公室在制定《實務守則》時，會詳細列明

序號	意見和備註
	電腦系統保安培訓的要求和範圍，以及提供培訓的相關資料作參考。〕

L. 其他意見和建議

序號	意見和備註
1	就**財政支援**方面，收到以下問題或建議： (a) 建議為業界提供資助、津貼等（6 份）。 (b) 建議考慮成立網絡安全基金或資助計劃（2 份）。 (c) 建議鼓勵使用科技券（1 份）及優化科技券（1 份）。 (d) 詢問事故通報會否獲得專責辦公室的認可，並允許用作網絡保險索賠。（1 份）
2	就**業界資源**方面，收到 4 份問題或建議，包括： (a) 要求為營運者提供資源、指引和支援（1 份），例如網絡安全專家、技術援助和提升安全的資金（1 份）。 (b) 要求提供認可服務供應商名單、選擇服務供應商（及其是否需要購買保險）的指引（1 份）。 (c) 詢問作為營運者會否優先得到能源、食水、燃料等（1 份）。
3	就**提升香港整體網絡安全生態**方面，收到以下建議： (a) 為業界超越基準要求提供誘因，例如稅務減免、公眾表揚、鼓勵投入資源、展示承擔（2 份）。 (b) 鼓勵營運者分享有用的網絡威脅情報，讓專責辦公室及時與其他營運者分享以預防同類攻擊（2 份）。 (c) 為營運者提供資源和支援，而非着重懲罰（1 份）。 (d) 專責辦公室牽頭建構網絡安全生態（1 份）。 (e) 由中央機構協調大規模攻擊活動（1 份）。 (f) 考慮引入強制網絡安全認證（1 份）。 (g) 建立關鍵第三方服務框架，提升第三方服務供應商

序號	意見和備註
	的網絡復原能力（1份）。 (h) 鼓勵採用多元化供應商（1份）。 (i) 探討人工智能對網絡安全的影響（1份）。 (j) 訂立加密金鑰管理機制，讓香港實體維持本身的數碼主權（1份）。 (k) 預留預算提升公眾網絡安全意識（1份）。 〔**註**：大部份營運者已就電腦系統保安建立了一定的標準。個別規管機構亦已經就業界的電腦系統保安措施制定指引。因此，我們預計擬議條例的相關要求不會對大型營運者帶來太大影響。 現時，政府有科技券計劃，可協助合資格的營運者提升網絡安全水平。香港互聯網註冊管理有限公司亦為企業員工提供網絡安全訓練服務。此外，香港網絡安全事故協調中心（HKCert）亦有為企業提供網絡安全技術建議。 我們歡迎維護和強化香港網絡安全生態的建議。專責辦公室成立後會與數字政策辦公室、警方和業界持份者協作，共同推行有關資訊科技安全的公眾教育，持續加強提升營運者的資訊科技安全意識及提供技術支援。

保安局
2024 年 10 月