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。
