2007 年 4 月
參考文件

立法會
資訊科技及廣播事務委員會

資訊保安

A. 目的

本文件旨在向委員報告公營機構及規管機構所執行資訊保安改善措施的中期進展。

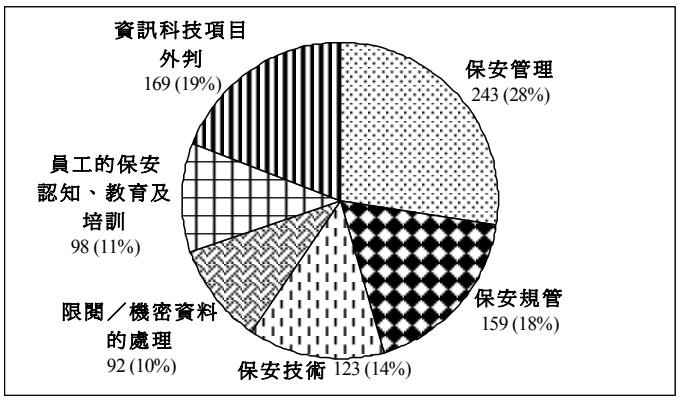
B. 背景

2. 政府資訊科技總監辦公室已於 2006 年 7 月及 8 月，就政府決策局及部門（“各局及部門”）、公營機構及規管行業的資訊保安狀況，完成有關調查。根據調查結果，立法會資訊科技及廣播事務委員會(“委員會”)在 2006 年 12 月 11 日會議席上建議盡快執行有關改善措施，並要求當局在 2007 年 7 月向委員會匯報工作進度，以及在 2007 年 3 月提交中期報告。

C. 改善範圍

3. 關於公營機構，上述調查把需執行的資訊保安改善措施分爲 6 個類別，合共 884 個工作項目，其分布如下:

圖表 1 – 公營機構改善項目的分布



4. 調查顯示，受規管行業的資訊保安措施亦存在一些改善空間。因此，有關規管機構已收到要求考慮加強規管制度，關注資訊保安及保護個人私隱的重要性，以預防資料泄漏等事故的發生。

5. 政府資訊科技總監已於 2006 年 12 月 27 日以書面通知各局及部門的首長，就其轄下公營機構及規管機構的改善範圍提出建議，並要求各局及部門協調有關的資訊保安改善計劃。此外，又建議各局及部門，提供政府資訊保安政策及相關的指引，給其轄下公營機構及規管機構作參考，以加強資訊保安。

D. 工作進度

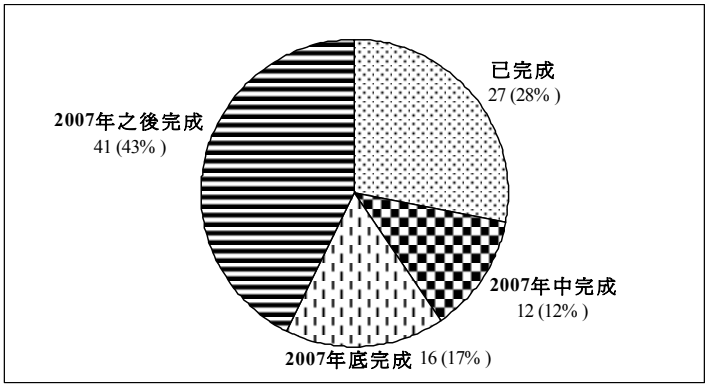
工作進度匯報

6. 政府資訊科技總監辦公室已於 2007 年 2 月 13 日，要求各局及部門協調及收集轄下公營機構及規管機構執行改善措施的進度。截至 2007 年 3 月 12 日，在 104 個公營機構及 58 個規管行業中，分別收到 96 個公營機構(92%)及 43 個規管行業(74%)的回覆。

7. 政府資訊科技總監辦公室其後分別在 2007 年 3 月 16 日及 3 月 23 日，發出便箋給有關各局及部門，提醒其轄下還有 8 個公營機構及 15 個規管行業仍未作出回覆。有關各局及部門正與這些機構商討及跟進。

公營機構的實施進度

圖表 2 – 公營機構改善計劃的實施進度



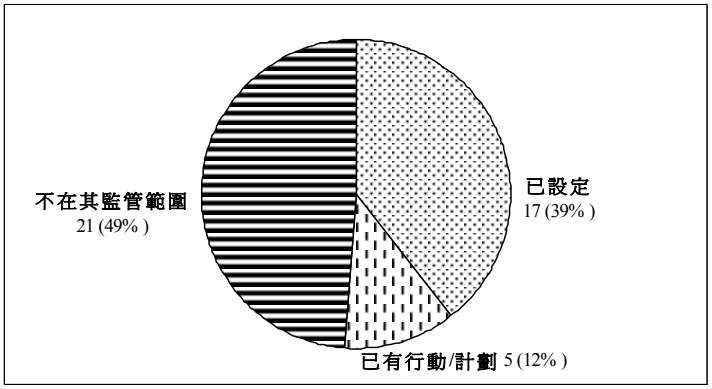
8. 從收到的回覆中，27 個公營機構(28%)已完成資訊保安改善計劃，餘下的機構(69 個)已開展實施工作，其中 12 個(12%)及 16 個(17%)分別計劃在 2007 年中及 2007 年底完成所需的改善措施。

9. 共有 41 個公營機構(43%)回覆未能在 2007 年內完成所有改善項目，理由是需待政策批准、項目撥款、計劃協調或選定技術方案及培訓課程。然而，這些回覆顯示，必須的改善項目都已經完成或展開。

10. 實施進度摘要載於本文**附件**。

規管行業的實施進度

圖表 3 – 規管行業改善工作的完成狀況



11. 從收到的 43 份回覆中，17 個規管機構(39%)表示已設定規管制度，關注資訊保安及保護個人私隱的重要性，而另外 5 個(12%)則已擬定行動計劃，改善轄下行業的資訊保安。

12. 餘下的 21 個規管機構(49%)認爲，現行的規管制度並無條文規定必須規管其轄下行業的資訊保安範疇。儘管如此，其中 9 個規管機構表示仍會採取行動，改善轄下行業的資訊保安。

E. 未來路向

13. 我們會繼續促請有關決策局及部門，跟進其轄下未有回覆進度的公營機構及規管機構。我們會向這些決策局及部門提供所需建議，以協調資訊保安改善計劃。我們會於 2007 年 7 月向委員會提交工作進度報告。

F.　　徵詢意見

14.　　請委員察悉本文報道的內容。

工商及科技局

政府資訊科技總監辦公室

2007 年 4 月

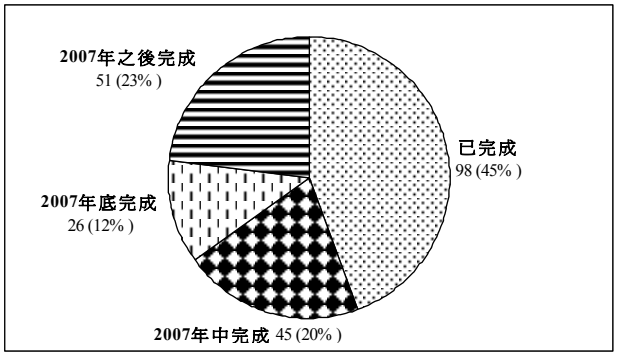
附件

實施進度摘要

保安管理

1. 220個改善項目的進度如下:

圖表4 – 220個有關*保安管理*項目[1]的完成狀況

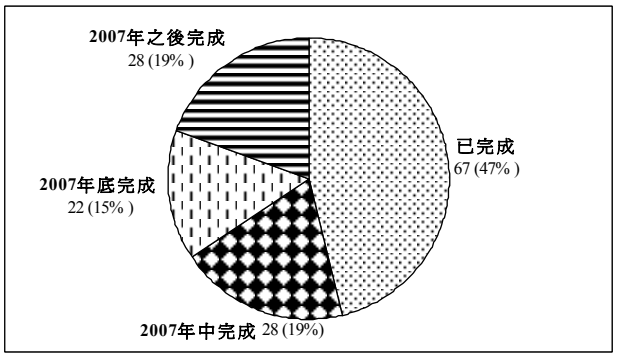


2. 51個項目需要在2007年以後才能完成，原因包括需待政策及財政支持、資訊科技保安政策的制定及管理架構的設立。

保安規管

3. 145個改善項目的進度如下:

圖表5 – 145個有關*保安規管*項目[2]的完成狀況



4. 28個項目需要在2007年以後才能完成，原因包括需待機構於2008年完成資訊保安風險評估及審計的結果。

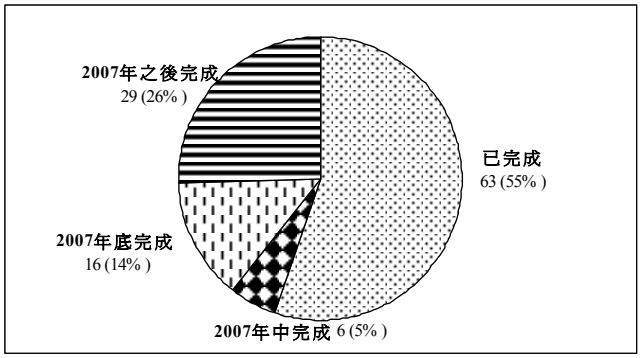
---

[1] **保安管理**項目的例子包括：設立適當管理架構、制定資訊保安政策和指引、提升營運保護措施、設計應變措施、強制員工對資訊保安的認知，以及進行資訊保安風險評估及審計。

[2] **保安規管**項目的例子包括：定期進行覆檢和復原演習，以測試是否符合保安管理規定，以及進行支援及隨機抽查。

保安技術

5. 114個改善項目的進度如下:

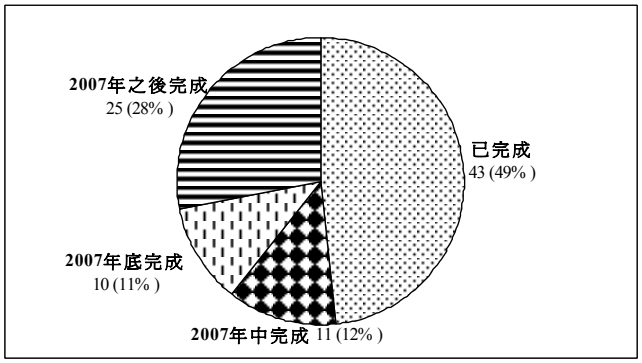


圖表6 – 114個有關*保安技術*項目[3]的完成狀況

6. 29個項目需要在2007年以後才能完成，原因包括需要選定適合的技術解決方案，例如修補程式管理工具及防禦間諜軟件工具。

限閱/機密資料的處理

7. 89個改善項目的進度如下:



圖表7 – 89個有關*限閱/機密資料的處理*項目[4]的完成狀況

8. 25個項目需要在2007年以後才能完成，原因包括需要選定適合的加密工具。

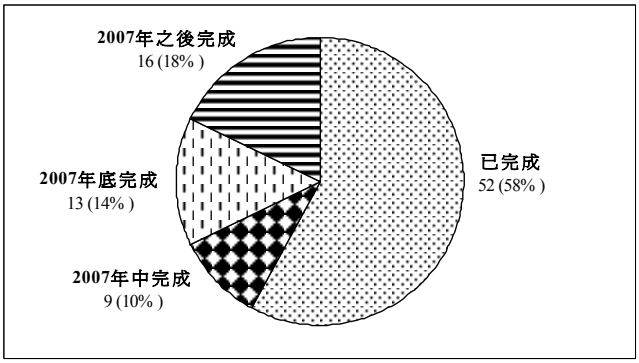
---

[3] **保安技術**項目的例子包括：採納保安修補程式應用和管理工具、防禦間諜軟件工具、檔案／數據加密工具、穩妥數據移除工具、入侵偵察／防範工具，以及推行備份和運作復原。

[4] **限閱/機密資料的處理**項目的例子包括：提升營運保護措施如定義數據的分類、制定批授接達權的程序、設立員工接達的控制程序，以及加密數據。

員工的保安認知、教育及培訓

9. 90個改善項目的進度如下:

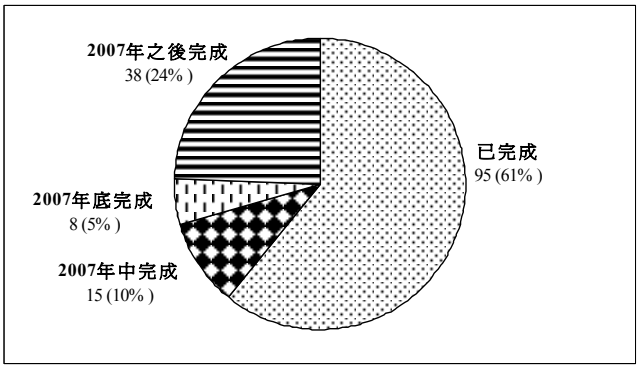


圖表8 – 90個有關*員工的保安認知、教育及培訓*項目[5]的完成狀況

10. 16個項目需要在2007年以後才能完成，原因包括需要在市場中選定適合的培訓課程。

資訊科技外判

11. 156個改善項目的進度如下:



圖表 9 – 156 個有關*資訊科技外判*項目[6]的完成狀況

12. 38個項目需要在2007年以後才能完成，原因包括需要在簽訂新合約或續約時，才能引入新的合約條款。

[5] **員工的保安認知、教育及培訓**項目的例子包括：舉辦內部培訓和外間培訓、鼓勵員工考取資訊保安方面的專業資格，以及定期發出提示便箋。

[6] **資訊科技外判**項目的例子包括：改善合約條款，與外判商界定職務和責任包括數據保密、接達控制、更改控制、升級處理和事故應變；加強不同測試階段的質素保證及控制，以及定期查核對保安規定的遵行情況。