

# 資訊保安標準簡介

2008 年 2 月

© 香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

**免責聲明：**政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

## 目錄

摘要.....	2
I. 介紹.....	3
II. 資訊保安標準.....	4
ISO 標準.....	4
支付卡行業數據安全標準（PCIDSS）.....	6
資訊系統稽核與控制標準（COBIT）.....	7
資訊科技架構集成（ITIL 或 ISO/IEC 20000 系列）.....	7
III. 有關資訊保安之規例.....	9
SOX.....	9
COSO.....	9
健康保險便利及責任法案（HIPAA）.....	10
聯邦資訊安全管理法案（FISMA）.....	10
聯邦資訊處理標準（FIPS）.....	11
香港規例.....	11
IV. 推行.....	12
V. 結論.....	13

## 摘要

資訊保安在保護機構資產上扮演著重要的角色，因為沒有單一方法可以保證百份之百安全，所以我們需要一套基準或是標準，以確保達到適合程度的保安水平，並有效使用資源，以及採用最佳的保安作業實務。在本文中，我們將簡略介紹各式不同的資訊保安標準和規例，包括 ISO 標準、COBIT 和沙賓法案（Sarbanes-Oxley Act）等等。

## I. 介紹

當資訊保安在保護資料和機構資產上扮演著重要角色的同時，我們經常聽到有關保安事故的新聞，例如網站遭篡改（defacement）、伺服器遭入侵和資料外洩等保安事故。因此，機構必須全面意識到投入更多資源來保護資訊資產的需要，而資訊保安也必須是政府和企業<sup>2</sup>的首要考慮。

為了解決此問題，許多政府和機構已經建立了基準和標準，因此，堅持遵守資訊保安的法定規則將有助確保一定水平的保安，且確保正確地使用資源，以及採用最佳的保安作業實務守則。一些行業如銀行便受到嚴格的規管，再加上指引或最佳作業實務守則作為保安規例的一部份，便成為業界成員間事實上（De Facto）的標準。

本文將簡略介紹最普遍採用的資訊保安標準和規例。

---

<sup>1</sup> <http://www.networkworld.com/news/2006/030706-government-cio-survey.html>

<sup>2</sup> [http://www.deloitte.com/dtt/press\\_release/0,1014,sid%253D1000%2526cid%253D171269,00.html](http://www.deloitte.com/dtt/press_release/0,1014,sid%253D1000%2526cid%253D171269,00.html)

## II. 資訊保安標準

此節將介紹不同的資訊保安標準。

### ISO 標準

於 1947 年建立的國際標準化組織（International Organisation for Standardisation, ISO）是一個非官方國際組織，與國際電工技術委員會（International Electrotechnical Commission, IEC）<sup>3</sup>和國際電信聯盟（International Telecommunication Union, ITU）<sup>4</sup>合作，以制定 information and communications technology（ICT）標準<sup>5</sup>。以下是幾項常見的 ISO 保安標準：

#### 1. ISO/IEC 27002:2005（資訊保安管理的作業實務守則）

ISO/IEC 27002:2005（2007 年 4 月取代 ISO/IEC 17799:2005）<sup>6</sup>起源於 BS7799-1 的國際標準，而 BS7799-1 原本是由英國標準協會（BSI）提出的。ISO/IEC 27002:2005 可被視為資訊保安管理的作業實務守則，並預期為發展機構保安標準和有效管理實踐的共同原則與作業實務指引<sup>7</sup>。

該標準包含了 10 項保安領域的指引和最佳作業實務建議：(a) 保安政策；(b) 資訊保安組織；(c) 資產管理；(d) 人力資源保安；(e) 實體和環境保安；(f) 通訊和操作管理；(g) 接達控制；(h) 資訊系統的採購、發展和維護；(i) 資訊保安事故管理；(j) 持續業務運作管理；(k) 法規遵循。

在這 10 項保安領域當中，建議給機構 39 項控制目標和數百件最佳資訊保安控制措施的最佳作業實務，以達到控制目標和保護資訊資產免受保密性、完整性和可用性上的威脅<sup>8</sup>。

#### 2. ISO/IEC 27001:2005（資訊保安管理系統要求）

ISO/IEC 27001:2005 國際標準是從 BSI 制定的標準 BS7799 Part 2:2002 所衍生而來的，它明確指出機構內已文件化的資訊保安管理系統（ISMS）在發展、

---

<sup>3</sup> <http://www.iec.ch/>

<sup>4</sup> <http://www.itu.int/net/home/index.aspx>

<sup>5</sup> [http://www.iso.org/iso/iso\\_catalogue/faq\\_standards\\_2.htm](http://www.iso.org/iso/iso_catalogue/faq_standards_2.htm)

<sup>6</sup> [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=50297](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297)

<sup>7</sup> [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=39612](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612)

<sup>8</sup> <http://www.iso27001security.com/html/27002.html>

推行、操作、監察、覆檢、維護和改善上的要求，並確保選用合適和均衡（Proportionate）的保安控制，以保護資訊資產<sup>9</sup>。該標準經常應用於各種機構，包括企業公司和政府機構等等。

該標準引進一項名為計劃-執行-檢查-反應（Plan-Do-Check-Act, PDCA）的循環模式，目的是建立、推行、監察和改善機構 ISMS 的效能。PDCA 周期有四個階段：

- 計劃（Plan）階段- 建立 ISMS
- 執行（Do）階段- 推行和操作 ISMS
- 檢查（Check）階段- 監察和覆檢 ISMS
- 反應（Act）階段- 維護和改善 ISMS

ISO/IEC 27001:2005 經常與 ISO/IEC 27002:2005 一起推行，ISO/IEC 27001 定義 ISMS 的要求，並使用 ISO/IEC 27002 來列出 ISMS 中最適合的資訊保安控制<sup>10</sup>。

ISO/IEC 27002 是一套提供建議控制措施的作業實務守則，機構可採用來處理資訊保安風險。這些控制並非強制性，因此 ISO/IEC 27002 並無認證，但是假如管理程序遵守 ISMS 標準，公司即可被認證為遵守 ISO/IEC 27001。有許多被認可的認證機構可替機構是否遵守 ISMS 標準作出認證服務，這些被認可的認證機構名單可從英國的 UK Accreditation Service 網站中找到<sup>11</sup>。

### 3. ISO/IEC 15408（資訊科技保安評估標準）

ISO/IEC 15408 是一項國際標準，一般稱為通用條件（CC）<sup>12</sup>，包括三個部份：ISO/IEC 15408-1:2005（介紹和一般模式）、ISO/IEC 15408-2:2005（保安功能要求）和 ISO/IEC 15408-3:2005（保安保證要求）。該標準有助評估、確認和認證科技產品的保安保證，檢視這些科技產品是否有遵守一連串的要求，例如在標準中訂明的保安功能要求。

在認可的測試實驗室中，可評估硬件和軟件是否遵守通用條件（CC），以認證產品和系統可達到準確的評估保證水平（Evaluation Assurance Level, EAL），包括 7 個 EAL：EAL1-功能測試（Functionally tested）、EAL 2-結構測試（Structurally tested）、EAL 3-有條理的測試和檢查（Methodically tested and checked）、EAL 4-有條理的設計，測試和覆檢（Methodically designed, tested

<sup>9</sup> [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=42103](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103)

<sup>10</sup> <http://www.iso27001security.com/html/27002.html#RelationTo27001>

<sup>11</sup> [http://www.ukas.com/about\\_accreditation/accredited\\_bodies/certification\\_body\\_schedules.asp](http://www.ukas.com/about_accreditation/accredited_bodies/certification_body_schedules.asp)

<sup>12</sup> [http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf\\_Home/PubliclyAvailableStandards.htm](http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm)

and reviewed)、EAL 5- 半正式設計和測試 (Semi-formally designed and tested)、EAL 6- 半正式核對,設計和測試 (Semi-formally verified, designed and tested)、和 EAL 7- 正式核對,設計和測試 (Formally verified, designed and tested)。在通用條件網站<sup>13</sup>可找到認可的實驗室名單和已被評估產品名單。在美國已被確認的產品可在通用條件評估 (Common Criteria Evaluation) 網站和 IT 保安確認方案 (Validation Scheme for IT Security, CCEVS) 網站中找到<sup>14</sup>。

#### 4. ISO/IEC 13335 (資訊科技保安管理)<sup>15</sup>

在 ISO/IEC 13335 變成完整 ISO/IEC 標準之前,原本只是一份技術報告 (Technical Report, TR),包含一連串的技術保安控制措施指引:

- ISO/IEC 13335-1:2004 提供資訊和通訊科技保安管理的概念和模式之文件。
- ISO/IEC TR 13335-3:1998 提供資訊科技保安管理技術的文件,這份文件仍在覆檢中,且可能會被 ISO/IEC 27005 所取代。
- ISO/IEC TR 13335-4:2000 涵蓋保障措施的選擇 (也就是技術保安控制),這份文件仍在覆檢中,且可能會被 ISO/IEC 27005 所取代。
- ISO/IEC TR 13335-5:2001 涵蓋網絡保安管理指引,這份文件也正在覆檢中,且可能與 ISO/IEC 18028-1 和 ISO/IEC 27033 合併。

### 支付卡行業數據安全標準 (PCIDSS)

支付卡行業數據安全標準 (Payment Card Industry Data Security Standard, PCIDSS)<sup>16</sup>是由一些大型的信用卡公司 (包括 American Express、Discover Financial Services、JCB、MasterCard Worldwide 和 Visa International) 所發展出來以加強付款帳戶的資訊保安,這些信用卡公司都是 PCI 標準會議 (Standards Council) 的會員,該標準含 12 項核心要求,包括保安管理、政策、程序、網絡設計、軟件設計和其它重要措施。這些要求可分類為以下幾項:

1. 建立和維護保安網絡
2. 保護持卡人資料
3. 維護漏洞管理程式
4. 推行嚴格的接達控制措施
5. 定期監察和測試網絡
6. 維護資訊保安政策

---

<sup>13</sup> <http://www.commoncriteriaportal.org/public/consumer/>

<sup>14</sup> <http://niap.bahialab.com/cc-scheme/vpl/>

<sup>15</sup> <http://www.iso27001security.com/html/others.html>

<sup>16</sup> <https://www.pcisecuritystandards.org/tech/index.htm>

## 資訊系統稽核與控制標準 (COBIT)

資訊系統稽核與控制標準 (Control Objectives for Information and related Technology, COBIT) 是「*a control framework that links IT initiatives to business requirements, organises IT activities into a generally accepted process model, identifies the major IT resources to be leveraged and defines the management control objectives to be considered*<sup>17</sup>」。即 COBIT 是一項控制架構，以連結資訊科技於商業需求的倡議，並安排資訊科技活動納入於一般接受的流程模型，確定主要的資訊科技資源能夠被好好利用，並訂立管理控制目標。IT Governance Institute (ITGI)於 1995 年首次發布這標準，目前更新至 2007 年發布的版本 4.1。

COBIT 4.1 由 7 個部份組成，分別是 (1) 行政概覽 (Executive overview)，(2) COBIT 架構 (COBIT framework)，(3) 計劃和組織 (Plan and Organise)，(4) 採購與推行 (Acquire and Implement)，(5) 傳送與支援 (Deliver and Support)，(6) 監察與評估 (Monitor and Evaluate)，(7) 包含詞彙表的附錄 (Appendices, including a glossary)。其主要內容可依 34 項資訊科技流程劃分。

COBIT 在國際間日益被接受為 IT Governance 的指引，使管理人員在控制要求、技術議題和企業風險間減低差距。根據 COBIT 4.1 的規定，COBIT 保安基準著重於資訊科技保安的特定風險，因此，無論大型或小型企業，都能簡單地遵守和推行 COBIT。有關 COBIT 的資料可在 ITGI<sup>18</sup>或國際資訊系統審計協會 (ISACA)<sup>19</sup>的網站中找到。

## 資訊科技架構集成 (ITIL 或 ISO/IEC 20000 系列)

資訊科技架構集成 (Information Technology Infrastructure Library, ITIL) 匯聚了資訊科技服務管理 (ITSM) 的最佳作業實務，著重資訊科技的服務流程，並以用戶為中心。ITIL 是由英國政府商貿辦事處 (Office of Government Commerce, OGC)<sup>20</sup>所發展的，自 2005 年以來 ITIL 已演進至 ITSM 的一項國際標準 ISO/IEC 20000<sup>21</sup>。

ITIL 服務管理自我評估可在 IT Service Management Forum 網站中的網上問卷<sup>22</sup>執行，該自

---

<sup>17</sup>

[http://www.isaca.org/Content/NavigationMenu/Members\\_and\\_Leaders/COBIT6/Obtain\\_COBIT/Cobit4.1\\_Brochure.pdf](http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/Cobit4.1_Brochure.pdf)

<sup>18</sup> <http://www.itgi.org>

<sup>19</sup> <http://www.isaca.org/bookstore>

<sup>20</sup> [http://www.ogc.gov.uk/guidance\\_ital\\_4438.asp](http://www.ogc.gov.uk/guidance_ital_4438.asp)

<sup>21</sup>

<http://www.iso.org/iso/search.htm?qt=20000&searchSubmit=Search&sort=rel&type=simple&published=true>

<sup>22</sup> <http://www.itsmf.com/bestpractice/selfassessment.asp>

我評估問卷可幫助評估以下幾項管理領域：(a) 服務水平管理 (Service Level Management)，(b) 財務管理 (Financial Management)，(c) 容量管理 (Capacity Management)，(d) 服務無間斷管理 (Service Continuity Management)，(e) 可用性管理 (Availability Management)，(f) 服務台 (Service Desk)，(g) 事故管理 (Incident Management)，(h) 問題管理 (Problem Management)，(i) 配置管理 (Configuration Management)，(j) 變更管理 (Change Management)，(k) 發布管理 (Release Management)。

### III. 有關資訊保安之規例

除了各式行業標準組織和指引外，一些受規範的行業例如銀行，須注意其業界或專業規管機構所訂明的規例和指引。在此節中，我們將簡略討論美國的規例，如 SOX、COSO、HIPAA 和 FISMA，以及香港所實行的規例。

#### SOX

在一連串如安隆（Enron）和世界通訊（WorldCom）等美國知名企業醜聞發生之後，美國在 2002 年頒布了沙賓法案(Sarbanes-Oxley Act, SOX)，該法案也被稱為「Public Company Accounting Reform and Investor Protection Act」，其用途是「*protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes*」<sup>23</sup>，意即透過證券法規的依據，改善企業披露的準確性和可信賴性。沙賓法案可保護投資人及用作其它用途，該規例影響了所有在美國上市的公司。

在 SOX 中的 404 節要求「*each annual report ... contain an internal control report ... [that] contains an assessment of ... the effectiveness of the internal control structures and procedures of the issuer for financial reporting*」，即每一份年報（包含內部控制報告）須包含內部控制結構和財務報告發程序之有效評估。因資訊科技在財務報告流程中扮演著重要的角色，因此需要評估資訊科技控制是否符合 SOX 的要求。

雖然資訊保安要求仍未直接列入法案中，但若無適當的保安措施和控制，無論流程中是否發生可能的未授權交易或是數字竄改，財務系統都無法繼續提供可靠的財務資料。SOX 的要求間接強迫管理部門考慮機構中系統的資訊保安控制，以符合 SOX 的要求<sup>24</sup>。

#### COSO

COSO 協會（Committee of Sponsoring Organizations of the Treadway Commission）所提出的架構是倡議一種整合的內部控制流程，藉著有效地評估內部控制來改善對企業的控制。其架構包含了五項要素<sup>25</sup>：

1. 控制環境，包含如機構內員工的誠信、管理人員的責任等因素；
2. 風險評估，目標是確定和評估企業風險；

---

<sup>23</sup>

[http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107\\_cong\\_bills&docid=f:h3763enr.txt.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf)

<sup>24</sup> [http://www.sans.org/reading\\_room/whitepapers/legal/1426.php](http://www.sans.org/reading_room/whitepapers/legal/1426.php)

<sup>25</sup> [http://www.coso.org/publications/executive\\_summary\\_integrated\\_framework.htm](http://www.coso.org/publications/executive_summary_integrated_framework.htm)

3. 控制活動，包含機構政策和流程；
4. 資訊與通訊，包括確定企業重要的資訊，及管理人員傳遞控制措施給員工的通訊渠道；
5. 監察，包含監察流程和持之以恆地評估所有內部控制系統的品質；

以上所述之 COSO 架構和 COBIT 架構皆被用來滿足 SOX 的要求。

## 健康保險便利及責任法案（HIPAA）

美國於 1996 年提出的健康保險便利及責任法案（ Health Insurance Portability and Accountability Act, HIPAA），主要是設計來改善團體和個人市場上，健康保險保障範圍的可轉移性（Portability）和持續性（Continuity），且防止浪費、詐騙和濫用的行為發生在健康保險、實施醫療護理及其它用途上<sup>26</sup>。此法案制訂了健康護理資訊的保安標準，考慮因素包含維護健康資訊記錄系統的技能、保安措施成本、人員訓練的需求、電子記錄系統審計追蹤的價值，及小型醫療護理提供者的能力和需求。

一個維護或傳遞健康資訊的人，需維護合理和適當的管理、技術和實體保障措施，以確保資訊的完整性和保密性。此外，應適當保護資訊以免受到威脅，例如資訊的安全性和完整性、未授權使用或未經授權披露。

電子健康資訊<sup>27</sup>和個人健康資訊私隱<sup>28</sup>均採用 HIPAA 保安標準，兩者的整套規例可在美國健康和個人服務部門（US Department of Health and Human services）網站上找到。

## 聯邦資訊安全管理法案（FISMA）

聯邦資訊安全管理法案（Federal Information Security Management Act, FISMA）是美國於 2002 年立法通過的電子政府法案（Public Law 107-347）的一部份<sup>29</sup>，其要求美國聯邦行政機構發展、編制和推行跨部門（agency-wide）計劃，在支援機構操作和資產的資訊（和資訊系統）方面提供資訊保安。相關要求如下：

1. 對資訊和支援機構運作及資產的資訊系統進行定期風險評估
2. 設計風險政策和程序，使資訊保安風險可降低至可接受水平
3. 提供適當的網絡和資訊系統保安計劃
4. 對全體人員（包含承包商在內）進行保安意識訓練
5. 對保安政策、流程和控制的有效性進行定期性評估。評估頻率不得少於每年一次，並應妥善管理對評估之後所提出的改善行動

<sup>26</sup> <http://aspe.hhs.gov/admsimp/pl104191.htm>

<sup>27</sup> [http://www.cms.hhs.gov/SecurityStandard/02\\_Regulations.asp#TopOfPage](http://www.cms.hhs.gov/SecurityStandard/02_Regulations.asp#TopOfPage)

<sup>28</sup> <http://www.hhs.gov/ocr/hipaa/finalreg.html>

<sup>29</sup> <http://csrc.nist.gov/groups/SMA/fisma/overview.html>

6. 一個已測試和可執行的保安事故處理流程
7. 支援機構操作的持續業務運作計劃

## 聯邦資訊處理標準 (FIPS)

由 NIST (National Institute of Standards and Technology) 發表的聯邦資訊處理標準 (Federal Information Processing standards, FIPS) 發行系列 (Publication Series), 是有關標準和指引的官方期刊, 該標準和指引在 FISMA 規定下被採用和執行<sup>30</sup>。FIPS Publication 199 名為 *Standards for Security Categorisation of Federal Information and Information Systems* 是 FISMA 法案下第一個強制規定的保安標準。FIPS Publication 200 名為 *Minimum Security Requirements for Federal Information and Information Systems* 則是第二個強制執行的保安標準, 其指出美國聯邦資訊和資訊系統就 17 個保安相關領域之最低保安要求。美國聯邦行政機構必須選擇適當的保安控制, 並確定該要求符合 NIST Special Publication 800-53 (建議的聯邦資訊系統保安控制), 以求符合該標準的最低保安要求。

17 個保安相關領域包括如下: (a) 接達控制; (b) 意識和訓練; (c) 審計和責任; (d) 認證、認可和保安評估; (e) 配置管理; (f) 應變計劃; (g) 識別和認證; (h) 事故應變; (i) 維修; (j) 媒體保護; (k) 實體和環境保護; (l) 計劃; (m) 人員保安; (n) 風險評估; (o) 系統與服務採購; (p) 系統和通訊保護; 和 (q) 系統和資訊完整性。

## 香港規例

香港目前並無類似 SOX 的規例。儘管如此, 香港特別行政區政府已發布基準資訊科技保安政策 (Baseline IT Security Policy) 和一系列有關資訊科技保安的指引, 作為政府政策局和各部門保護政府資訊系統的參考和指引, 相關文件發布於政府網站<sup>31</sup>上, 以供大眾參考。

此外, 香港各行業監管機構已為其會員制定保安控制要求和資訊科技系統管治 (Governance) 要求, 舉列說, 香港金融管理局已發布一份電子銀行服務指引, 此份文件名為「TM-E-1 Supervision of E-Banking」<sup>32</sup>, 目的為設立管理電子銀行風險的方法和一般原則, 涵蓋範圍有資深管理人員的疏忽、有關電子銀行主要的技術控制議題及顧客保安。

---

<sup>30</sup> <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>

<sup>31</sup> <http://www.ogcio.gov.hk/eng/prodev/eseccpol.htm>

<sup>32</sup> <http://www.info.gov.hk/hkma/eng/bank/spma/attach/TM-E-1.pdf>

## IV. 推行

雖然目前有許多可用的資訊保安標準，但這些標準通常只是一般指引或原則，並不能適用於特定機構。

假如機構決定致力推行一項特定保安控制標準，或是推行一整組標準，此時便需要上層管理人員至下層終端用戶共同努力來達到此目標。因各部門的一致努力是發展和推行流程中的一部份，且必須特別注意使用標準化政策或指引，而該標準化政策或指引必須適用於特定機構文化、業務和機構作業實務。

採用任何標準前，機構應先執行差距分析（**Gap Analysis**），以確定目前機構內的保安控制、潛在問題和議題、成本與效益、操作的影響、以及應採用的建議。制定保安政策和指引應只遵守差距分析的結果。管理人員的全力支持是很重要的，另外，在部署新的保安政策和指引之前，也須執行用戶認知計劃，以確認所有員工了解保安政策的好處和影響。

在執行標準化實務之後，資訊科技服務用戶的抱怨增加是一個常見的問題，而該抱怨起因是新保安控制所帶來的限制。要成功推行任何資訊保安標準或控制，關鍵在於保安要求、功能要求和用戶要求三者之間是否達到平衡。

## V. 結論

雖然有許多可用的資訊保安標準，但只有適當執行這些標準，機構才能受惠，且所有部門皆須參與其中。資深經理、資訊保安從業員、資訊科技專家和用戶在保護機構資產中皆扮演其角色。唯有機構內外共同合作，資訊保安才能成功。