數字政策辦公室

資訊保安

雲端運算保安

實務指引

[ISPG-SM04]

第 2.1 版

2024 年 7 月

©中華人民共和國
香港特別行政區政府

中華人民共和國香港特別行政區政府保留本文件內容的所有權，未經中華人民共和國香港特別行政區政府明確批准，不得翻印文件的全部或部分內容。

版權公告

© 2024 中華人民共和國香港特別行政區政府
除非另有註明，本出版物所載資料的版權屬中華人民共和國香港特別行政區政府所有。在符合下列條件的情況下，這些資料一般可以任何格式或媒介複製及分發：

(a) 有關資料沒有特別註明屬不可複製及分發之列，因此沒有被禁止複製及分發；
(b) 複製並非為製造備份作售賣用途；
(c) 必須準確地複製資料，而且不得在可能誤導他人的情況下使用資料；以及
(d) 複製版本必須附上「經中華人民共和國香港特別行政區政府批准複製／分發。中華人民共和國香港特別行政區政府保留一切權利」的字眼。

如須複製資料作上述核准用途以外的用途，請聯絡數字政策辦公室尋求准許。

修改記錄				
修改次數	修改詳情	經修改頁數	版本編號	日期
1	增加關於資訊科技保安管理的新章節，及維持與其他實務指引有一致的參考，在第5節、第5.7節、第5.9.2節及附件B增加對新興雲端技術及服務的介紹。	整份文件	1.1	2018年7月
2	在第5節、第5.1節、第5.3節、第5.4節、第5.5節及第5.7節更新對雲端服務供應商提供適當數據保護的要求；在第5.4節及附件B更新對個人資料保護的去識別化技術介紹；以及在附件B更新新興解決方案的介紹。	15-18, 20-22, 26, 42, 44, 49	1.2	2021年6月
3	在第 3.1 節更新有關雲端服務模式的內容。 在第 4.1 節加入共同責任概念。 在第 4.2 節更新雲端推行情景。 在第5 節、第5.1 節、第5.2 節、第5.3 節、第5.4 節、第5.5 節、第5.7 節、第5.8 節、第5.9 節、第5.12 節和第5.14 節更新保安考慮事項及控制。	6, 9-15, 16-37, 43, 47, 附件 A, 附件B	2.0	2024年4月
4	將「政府資訊科技總監辦公室」更改為「數字政策辦公室」		2.1	2024年7月

目錄

1. 簡介 1

1.1 目的 1
1.2 參考標準 1
1.3 定義及慣用詞 2
1.4 聯絡方法 2

2. 資訊保安管理 3

3. 雲端運算保安的介紹 5

3.1 雲端運算 5
3.2 雲端平台的基礎設施 6
3.3 雲端服務的模式 6
3.4 雲端平台部署的模式 6
3.5 四種部署模式的比較 7

4. 雲端平台保安概覽 8

4.1 雲端服務模式及資訊保安 8
4.2 雲端平台推行情景及資訊保安 10

5. 雲端服務的保安考慮及控制 13

5.1 管理職責 14
5.2 資訊科技保安政策 16
5.3 人力資源保安 16
5.4 資產管理 17
5.5 接達控制 20
5.6 加密方法 22
5.7 實體及環境保安 22
5.8 操作保安 24
5.9 通訊保安 25
5.10 系統購置、發展及維護 30
5.11 外判資訊系統的保安 31
5.12 資訊保安事故管理 32
5.13 資訊科技保安方面的業務持續運作管理 33
5.14 遵行要求 34

附件 A: 不同雲端平台部署情景的保安控制概覽 36

附件 B: 新興雲端保安技術 39

1. 簡介

本文件旨在提供指引，予負責評估使用雲端運算模式以儲存、處理或傳遞政府資訊所帶來保安影響的不同組別人士，如管理人員、資訊科技管理員、系統擁有者及資訊保安持份者。

隨著雲端運算急速發展，雲端形態不斷推陳出新，現有系統或亦因此結合演變成新的雲端形式。本文件的內容大致可應用於不同雲端運算技術。由於每個雲端運算部署都有各自的特徵，推行者應考慮及應按其環境而選擇適合的作業模式。

注意：對於本文內所提及之供應商的產品或服務，本文件的作者並無作出使用的認可或暗示任何的取向。另外，本文件並非要取代政府保安規例、政策、指引和決策局／部門的部門資訊科技保安政策。

1.1 目的

鑒於全球採用雲端運算的趨勢日益普及，本文件的訂立旨在為決策局／部門提供相關的指導說明，目的如下：

- 加強決策局／部門對基本雲端保安的理解；以及
- 協助決策局／部門在建立自己的私人雲端平台，或外聘雲端服務時，安全使用雲端運算。

本文件重點介紹當採用雲端運算時常見的保安考慮及業界的良好保安作業模式。

1.2 參考標準

以下的參考文件為應用本文件時必不可少的參考：

- 香港特別行政區政府《基準資訊科技保安政策》[S17]
- 香港特別行政區政府《資訊科技保安指引》[G3]
- Information technology - Security techniques - Information security management systems - Requirements (second edition), ISO/IEC 27001:2013
- Information technology - Security techniques - Code of practice for information security controls (second edition), ISO/IEC 27002:2013
- Information technology – Security techniques – Governance of information security, ISO/IEC 27014:2013
- Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services, ISO/IEC 27017:2015

- Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, ISO/IEC 27018:2014
- Information technology – Security techniques – Information security for supplier relationships, ISO/IEC 27036:2014
- Information technology – Security techniques – Storage security, ISO/IEC 27040:2015

1.3 定義及慣用詞

本文件將會採用《基準資訊科技保安政策》和《資訊科技保安指引》內所使用，以及以下的定義及慣用詞。

縮寫及術語	
雲端服務供應商	通常收費為其他機構和／或人士，提供基於雲端的平台、基礎設施、應用系統或儲存服務的公司。

1.4 聯絡方法

本文件由數字政策辦公室編製及備存。如有任何意見或建議，請寄往：

電郵： it_security@digitalpolicy.gov.hk

Lotus Notes 電郵： IT Security Team/DPO/HKSARG@DPO

CMMP 電郵： IT Security Team/DPO

2. 資訊保安管理

資訊保安是關於保安控制和措施的規劃、實施和持續提升，以保護資訊資產的機密性、完整性和可用性，適用於資訊的存儲、處理或傳輸過程及其相關資訊系統中。資訊保安管理是一套有關規劃、組織、指導、控制的原則和應用這些原則的法則，以迅速有效地管理實體、財務、人力資源和資訊資源，以及確保資訊資產和資訊系統的安全。

資訊保安管理涉及一系列需要持續監測和控制的活動。這些活動包括但不限於以下的範疇：

- 保安管理框架與組織；
- 管治、風險管理和遵行要求；
- 保安操作；
- 保安事件和事故管理；
- 保安意識培訓和能力建立；以及
- 態勢感知和資訊共享。

<u>保安管理框架與組織</u>

決策局／部門須根據業務需要和政府保安要求，制定和實施部門資訊保安政策、標準、指引和程序。

決策局／部門亦須界定資訊保安的組織架構，並為有關各方就保安責任提供清晰的定義和適當的分配。

<u>管治、風險管理和遵行要求</u>

決策局／部門須採用風險為本的方法，以一致及有效的方式識別資訊系統的保安風險、訂定應對風險的緩急次序和應對有關風險。

決策局／部門須定期和在必要時對資訊系統和生產應用系統進行保安風險評估，以識別與保安漏洞相關的風險和後果，並為建立具成本效益的保安計劃和實施適當的保安保護和保障措施提供依據。

決策局／部門亦須定期對資訊系統進行保安審計，以確保當前的保安措施符合部門資訊保安政策、標準和其他合約或法律上的要求。

保安操作

為保護資訊資產和資訊系統，決策局／部門應根據業務需要實施全面的保安措施，涵蓋業務上不同的技術領域，並在日常操作中採取「預防、偵測、應變和復原」原則。

- 預防措施避免或阻止不良事件的發生；
- 偵測措施識別不良事件的發生；
- 應變措施是指在發生不良事件或事故時，採取協調行動來遏制損害；以及
- 復原措施是將資訊系統和／或數據的機密性、完整性和可用性恢復到預期狀態。

保安事件和事故管理

在現實環境中，由於存在不可預見並致服務中斷的事件，故此保安事故仍可能會發生。若保安事件危及業務的連續性或引起數據保安風險，決策局／部門須啟動其常規保安事故管理計劃，以實時識別、管理、記錄和分析保安威脅、攻擊或事故。決策局／部門亦應準備與有關各方適當地溝通，透過分享對有關保安風險的應變以消除不信任或不必要的猜測。當制定保安事故管理計劃時，決策局／部門應規劃和準備適當的資源，並制訂相關程序，以配合必要的跟進調查。

保安意識培訓和能力建立

因為資訊保安是每個人的責任，所以決策局／部門應不斷提升機構內的資訊保安意識，透過培訓及教育，確保有關各方了解保安風險，遵守保安規定和要求，並採取資訊保安的良好作業模式。

態勢感知和資訊共享

因應網絡威脅形勢不斷變化，決策局／部門亦應不斷關注由保安行業和政府電腦保安事故協調中心發布的現時保安漏洞訊息、威脅警報和重要通知。應將即將或已經發生具威脅的保安警報傳達及分享給決策局／部門內的負責同事，以便採取及時的應對措施來緩解風險。

決策局／部門可以利用威脅情報平台接收和分享保安事務、保安漏洞和網絡威脅情報的訊息。

3. 雲端運算保安的介紹

3.1 雲端運算

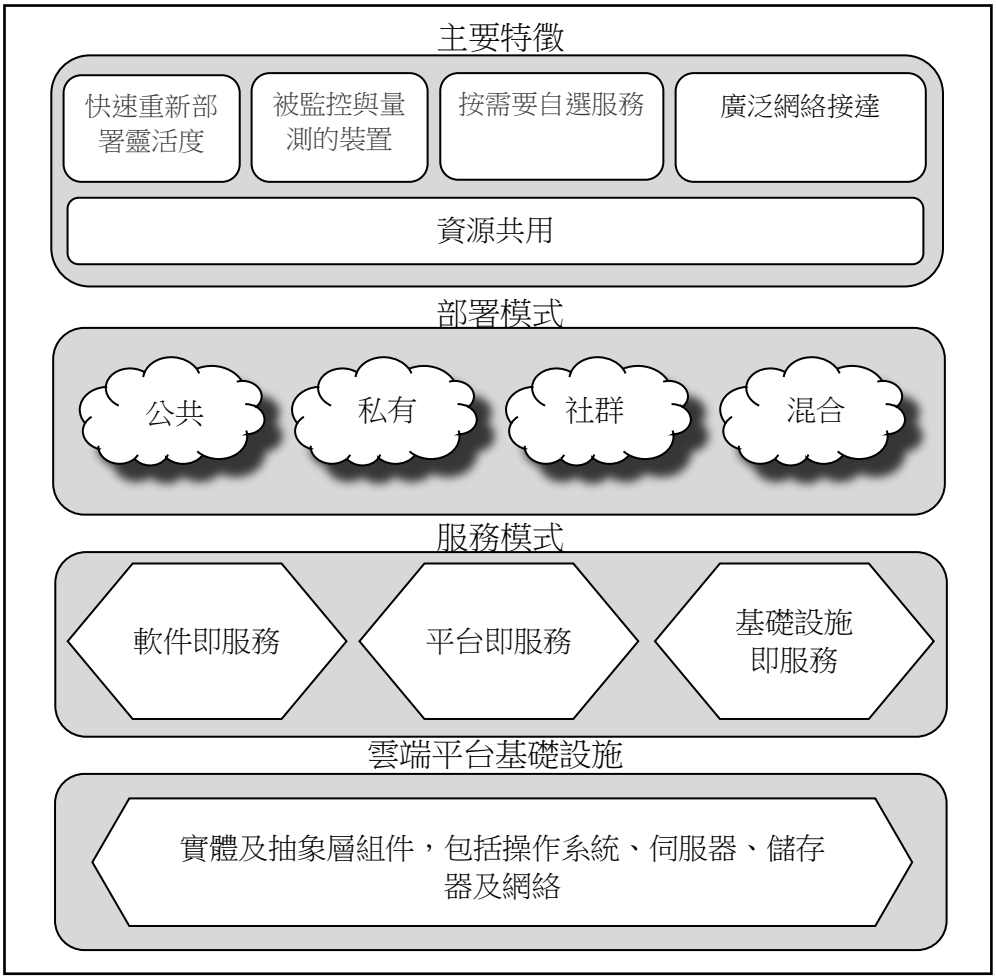

圖 3.1 雲端模式

雲端運算模式能讓用戶隨時隨地、便捷地、按需要地透過網絡接達一系列可配置的電腦運算資源（例如網絡、伺服器、儲存器、應用系統及服務），這些資源只需透過少量的管理工作或與服務供應商少量的互動，便能迅速地準備妥當及發佈。如上圖3.1 所示，雲端平台基礎設施下的雲端運算大致上可以分為三個服務模式及四個部署模式。

3.2 雲端平台的基礎設施

雲端平台的基礎設施由軟件及硬件所組成，用以提供雲端計算的重要特性，包括資源共用、快速重新部署的靈活度、可監控與量測的服務、按需要的自助服務，以及寬帶網絡接達。雲端平台的基礎設施可被視為同時包含實體層及抽象層。實體層由支援雲端服務的硬件資源組成，一般包括伺服器、儲存器及網絡組件；抽象層由軟件所組成，部署在實體層上，這也是雲端平台的重要特徵。在概念上，可以理解為抽象層設於實體層之上。

3.3 雲端服務的模式

雲端服務有以下三種典型的模式：

- 基礎設施即服務：雲端服務供應商向決策局／部門提供一項包括基本運算資源／設備（儲存器、硬件、伺服器及網絡組件）的服務，決策局／部門仍控制所安裝的操作系統及應用系統；
- 平台即服務：雲端服務供應商向決策局／部門提供一項包括基本運算資源／設備，及虛擬環境的服務，然後由決策局／部門於供應商提供的環境或雲端平台的基礎設施上，部署本身的應用系統；以及
- 軟件即服務：雲端服務供應商向決策局／部門提供一項包括基礎設施、平台（或虛擬環境），以及軟件的服務。決策局／部門的用戶連接到這個環境，並經定制後運行資訊科技應用系統。

3.4 雲端平台部署的模式

雲端的部署有以下四種典型的模式：

- 公共雲端平台：雲端平台基礎設施開放予公眾使用。基礎設施支援多租戶特性，並可以由第三方擁有、管理及運作（或這三種方式的任何組合）。雲端部署於雲端服務供應商處所；
- 私有雲端平台：雲端平台基礎設施只供由數個決策局／部門組成的單一機構獨立使用。基礎設施可以由該機構（即內部私有雲端平台）或第三方（即外判私有雲端平台）擁有、管理及運作（或這三種方式的任何組合）。雲端部署於機構自己的處所或供應商處所；
- 社群雲端平台：雲端平台基礎設施只供來自有共同目標、興趣及／或關注的機構的特定用戶羣組專用。基礎設施可以由用戶羣組內的一個或多個組織擁有、管理及運作（或這三種方式的任何組合）。雲端部署於機構自己的處所或供應商處所；以及
- 混合雲端平台：雲端平台基礎設施由兩個或多個不同雲端平台基礎設施（私有、社群或公共）組成，並可由不同雲端服務供應商提供。這種模式令數據及應用系統具有可攜性。

3.5 四種部署模式的比較

四種部署模式在資訊保安不同層面的比較如下：

層面	公共雲端平台	私有雲端平台	社群雲端平台	混合雲端平台
服務提供	透過互聯網提供服務	透過（虛擬）私有網絡提供服務	透過（虛擬）私有網絡提供服務	混合使用互聯網及私有網絡
服務水平協議	由雲端服務供應商訂立服務水平協議	由機構訂立服務水平協議	由參與機構共同訂立服務水平協議	混合不同服務水平協議
可使用情況	生產力、業務及社交媒體應用系統，及其他雲端資訊科技服務	寄存於專為政府使用而設的基礎設施內的政府內部服務	向政府與擁有相同業務需要的非政府組織所形成的社群提供的服務	因為私有雲端平台不能滿足容量需要，而連接到公共雲端服務的私有雲端應用系統

是否採用雲端運算是一個業務上的決定，除保安因素外，決定過程亦應考慮如轉移成本、生命周期成本及應用系統的準備程度等有關因素。除此以外，決策局／部門應評估數據的敏感程度，選擇適當的部署模式處理及儲存數據。決策局／部門須確保符合所有政府的保安要求及滿足業務的需要。決策局／部門亦應透過對可能採用的雲端平台作全面保安評核，識別雲端服務供應商在資訊保安的差距，並採取有效的方法以減低對數據造成的風險。

4. 雲端平台保安概覽

一如任何新的運算模型或技術，雲端運算亦可能構成新的保安風險。在考慮採用雲端運算時，應使用風險為本的方法。重要的是，決策局／部門必須考慮各種保安範疇，例如數據保密性、完整性、額外設置、復原能力、管轄權等。另外，亦需要知道何種數據會被考慮轉移至雲端平台、這些數據對風險的承受力，以及選擇的服務和部署模式。雲端服務用戶或其潛在用戶必須明白雲端運算當中的挑戰及風險，讓自己能為緩解或控制這些挑戰及風險而作出更好準備。應就評估得出的風險水平及數據價值，部署適當的保安控制及措施。

4.1 雲端服務模式及資訊保安

作為一般原則，在從軟件即服務移至平台即服務，再移至基礎設施即服務的過程中，決策局／部門可以對更多資源有更大的保安控制。圖4.1展示在雲端平台上，不同負責方的控制範圍：

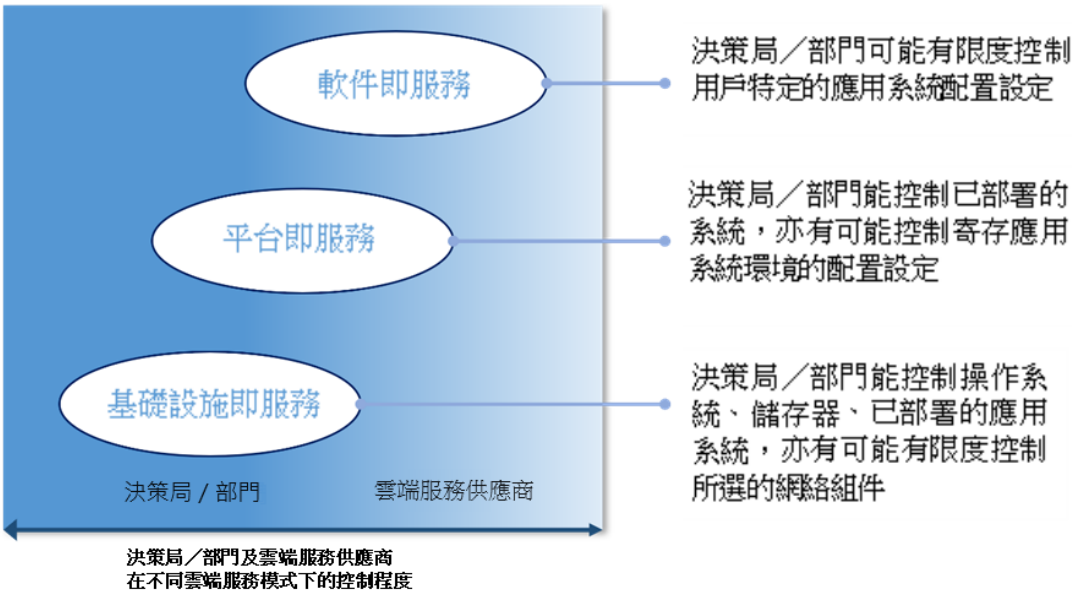

圖 4.1 決策局／部門及雲端服務供應商
在不同雲端服務模式下的控制責任程度

雲端服務模式不存在其中一方承擔所有責任的情況。不論採用哪種模式，共同責任都是一個重要的概念，而責任程度的劃分取決於雲端服務模式。決策局／部門須確保已明確界定並明白雙方的責任。儘管特定雲端服務供應商可能會因商業考慮而採用不同的方式，圖4.2展示了在雲端中責任方之間通常採用的共同責任:

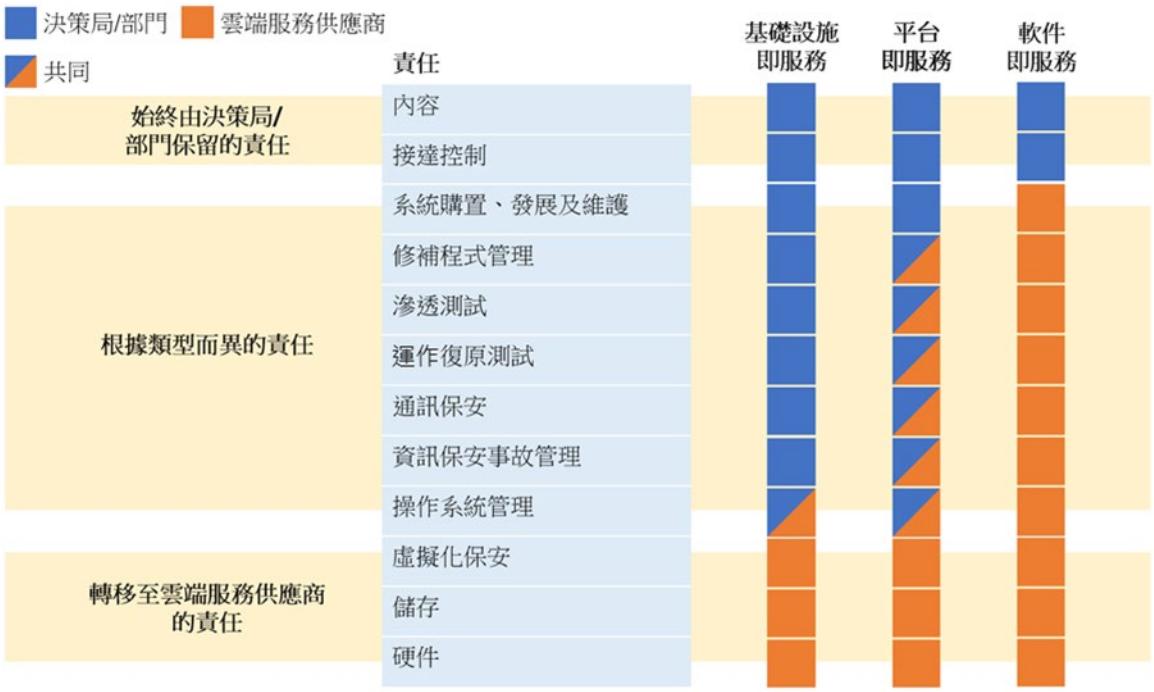

圖4.2 決策局／部門及雲端服務供應商
在不同雲端服務模式下的共同責任

軟件即服務一般由客戶端使用瀏覽器經互聯網接達，而客戶不會管理或控制下層的雲端平台及基礎設施。於軟件即服務模式下，決策局／部門通常對雲端保安及服務域持有甚少的直接控制權。他們只負責管理內容和接達控制。

平台即服務於中層提供雲端設施。透過減少一些給予客戶的現成功能，平台即服務一般比軟件即服務有更大的擴充能力。決策局／部門對平台有更多的控制權, 包括內容，接達控制和修補程式管理。而雲端服務供應商負責操作系統管理、虛擬化保安、儲存和硬件。在此模式中，決策局／部門和雲端服務供應商必須進行討論、界定和達成協議以管理其餘的保安範疇。

基礎設施即服務要求決策局／部門推行本身的應用系統，以及在基礎設施即服務雲端服務供應商所提供的基礎設施之上設立自己的操作平台。決策局／部門有權靈活地管理和控制雲端環境中的大部分保安範疇，包括內容，接達控制、系統購置、發展及維護、修補程式管理、滲透測試、運作復原測試、通訊保安和資訊保安事故管理。而雲端服務供應商負責管理虛擬化保安、儲存和硬件。操作系統管理的責任需要決策局／部門和雲端服務供應商進一步討論並達成一致。

無論服務是屬於何種雲端服務模式，雲端服務供應商亦要負責控制及保護下層的基礎設施組件，如內容，接達控制。決策局／部門則負責管理儲存內容和接達控制。決策局／部門和雲端服務供應商應了解各自的責任，並密切合作和溝通以確保雲端環境的保安和可靠性。

4.2 雲端平台推行情景及資訊保安

決策局／部門的保安控制程度因公共雲端平台模式和私有雲端平台模式的不同而有異。公共雲端平台是提供給一般公眾，並且由多個租戶使用。而私有雲端平台是由單一機構專用的。私有雲端平台可以讓機構有更嚴謹的接達控制，從而更好地控制網絡基礎架構和安全策略。因此如果配置不當，公共雲端平台有可能面臨類似的保安風險。值得注意的是私有雲端平台提供的任何好處都僅限於其實施方法。雲端服務具有不同的推行情景，它可由內部提供或是外判，可部署於機構處所或非機構處所。這些推行情景對雲端環境的保安尤關重要。

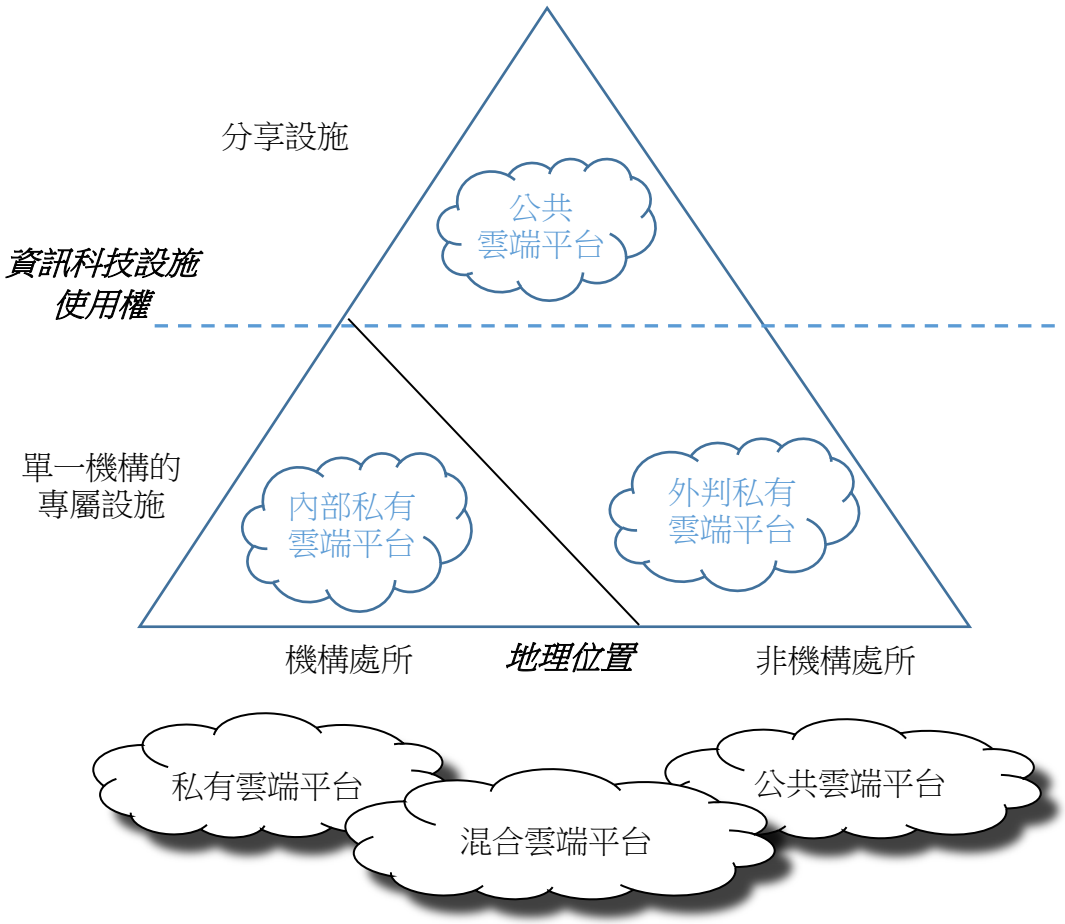

圖 4.3 雲端平台推行情景

為更深入討論決策局／部門內推行雲端平台的保安考慮事項及控制，本文將會參考圖4.3中的四種情景：

- 「內部私有雲端平台情景」由政府擁有及在政府處所的數據中心運作。
- 「外判私有雲端平台情景」包括給政府專用的設施，並由外聘雲端服務供應商於非機構處所的數據中心運作，例如政府雲端平台（GovCloud）。
- 「公共雲端平台情景」 由外聘雲端服務供應商提供服務給公眾使用。
- 「混合雲端平台情景」由兩個或以上的雲端平台情景（公共或私有）組成。

4.2.1 內部私有雲端平台情景

內部私有雲端平台寄存於機構處所內，並由機構內部員工管理。縱使部分非技術性保安問題，如外判要求、數據位置及服務終止未必適用，值得注意的是機構可能仍然高度依賴商業供應商提供軟件／韌體升級、更換伺服器、資訊科技設備等中有缺陷的資訊科技組件等。從供應鏈的角度來看，這種對商業供應商的依賴仍然會帶來保安漏洞的挑戰。決策局／部門應了解其管理供應鏈風險的責任，例如對維護和系統升級的供應商管理，並定期進行審核和評估，以確保商業供應商遵守機構的保安政策及指引。

4.2.2 外判私有雲端平台情景

外判私有雲端平台是由第三方完全管理的單一租戶環境，以達至較高的成本效益或運作效率。外判私有雲端平台的額外好處，包括決策局／部門的資訊科技基礎設施可以由第三方機構在其數據中心購買和維護。第三方提供私有雲端資源的維護、升級、支援和遠程管理。

決策局／部門應利用雲端服務供應商提供的第三方認證報告（例如服務組織控制報告第二類）作為基準，以了解哪些保安範疇已由獨立第三方審核員進行檢查。由於服務組織控制報告第二類提供了有關雲端服務供應商在保安、私隱、處理完整性、機密性和可用性領域的表現的資訊，決策局／部門可以通過覆檢此類報告，更好地了解雲端服務供應商在運營有效性方面的表現。隨後，決策局／部門應決定是否需要雲端服務供應商提供澄清和更多資訊，以了解合規程度。這符合成熟的雲端服務供應商所採用的行業最佳實踐，使決策局／部門能夠專注於雲端環境中工作的保安，而不是雲端基礎設施的保安。由於雲端服務供應商所使用的數據中心並非位於決策局／部門的處所，決策局／部門應要求雲端服務供應商採用完善的接達記錄機制，以便及時獲得潛在未經授權的數據接達的警報。雲端服務供應商越積極偵測潛在的未經授權的數據接達嘗試，就越能有效防止保安事故的發生。對於雲端服務的購買者而言有一個常見的誤解，在外判安排下，雲端服務供應商會負責雲端環境的所有持續管理職責。事實上，雲端服務購買者仍有責任定期監控雲端服務供應商的表現。

4.2.3 公共雲端平台情景

公共雲端平台由第三方雲端服務供應商管理底層的電腦資源。雲端服務供應商負責資源維護並通過服務水平協議確保其可用性，可靠性和保安性。決策局／部門不會購買、擁有或維護實體數據中心和伺服器。取而代之，決策局／部門是基於需求取得技術服務。由於平台是由出售雲端服務的雲端服務供應商所擁有，所以顧名思義，它不屬於決策局／部門。雲端基礎設施和雲端原生服務的保安性由雲端服務供應商全面管理。因此，了解雲端服務供應商提供的公共雲端環境並確保雲端運算解決方案能夠滿足機構的保安和私隱要求至關重要。

由雲端服務供應商提出的標準服務水平協議記錄了雙方對服務、優先次序、責任、保證及保用的共同理解。服務水平協議通常只有有限或沒有任何商議空間。決策局／部門應留意在違反服務水平協議時，對保安的影響及相關罰則。

4.2.4 混合雲端平台情景

混合雲端平台情景是在上述三種推行情景之上尚存的另一種可行推行情景。在第3.4節所提及，混合雲端基礎設施普遍由兩個或以上不同的雲端基礎設施（例如私有及公共）組成。因此，混合雲端平台推行情景是由其他三種推行情景（內部私有雲端平台、外判私有雲端平台及公共雲端平台情景）組成。

雲端服務供應商所提供，從雲端環境連接到決策局／部門網絡的連接不應削弱現有的保安水平。決策局／部門應在取得雲端服務時評估當中的保安風險，並應用「若雙方保安水平不同，則雙方都要採用較強的保安」的原則。

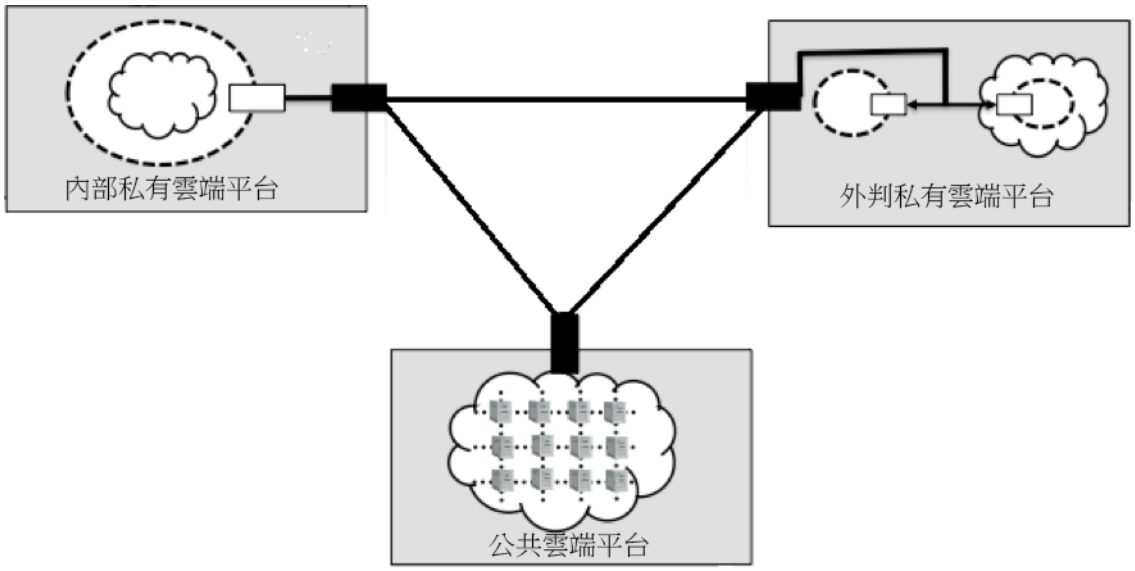

圖 4.4 混合雲端平台情景

「雲爆發」是混合雲端平台情景經常採用的方式。「雲爆發」是指企業利用內部私有雲端平台進行基本操作，但在平台需求高峰時期，則可選擇接達一個或多個的外判私有雲端平台，以平衡平台的負載量。

5. 雲端服務的保安考慮及控制

在明白雲端運算及雲端保安的基本概念後，本節將討論相應的保安控制。雲端運算可視為向企業提供以資訊科技為本的服務新方法，而非一種獨立的新科技。當然，部分技術，如虛擬化，在雲端運算上具有顯著的重要性。由於雲端運算大部分採用與傳統資訊科技環境相類似的管理工具、操作系統、數據庫、伺服器平台、網絡基建、網絡規約及儲存器組等，雲端平台的保安控制亦因此與傳統資訊科技環境大致相似。故此，在政府的保安文件包括《基準資訊科技保安政策》[S17]及《資訊科技保安指引》[G3]內的保安控制仍然適用。可是，根據所採用雲端服務及部署模式的特徵，以及部署雲端服務所使用的技術，雲端環境的某些風險將或多或少變得更為顯著（例如透過正確配置進行自動保安修補），而在傳統資訊科技環境未遇過的新風險亦可能隨之出現。以下的部分將會集中在保安範疇，描述雲端保安的挑戰及提供處理這些風險的保安作業實務。

- 管理職責
- 資訊科技保安政策
- 人力資源保安
- 資產管理
- 接達控制
- 加密方法
- 實體及環境保安
- 操作保安
- 通訊保安
- 系統購置、發展及維護
- 外判資訊系統的保安
- 保安事故管理
- 資訊科技保安方面的業務持續運作管理
- 遵行要求

在每個保安考慮事項及控制的說明旁邊，都附有一個標籤，標示該控制應該最適合應用於哪種部署情景。對於混合雲端平台，應根據當中的組合考慮其保安控制。若平台包括公共及內部私有雲端平台，則應保留該兩種部署情景的保安考慮事項及控制。標籤只標示一般關聯，欠缺某種部署情景標籤並不代表該控制與這些部署情景完全無關。

決策局／部門在考慮選用雲端服務時，應採取風險為本的方法、評估業務需要及數據的保密類別，並確保雲端服務供應商的保安措施、服務水平及管理要求符合政府的數據保密類別及業務要求，並遵行政府的保安要求。由於不同的雲端服務供應商的保安等級有所不同，各決策局／部門應全面審視和仔細考慮雲端服務供應商在各方面處理數據的方式。以下有關雲端的保安作業模式適用於一般的雲端部署方案。隨着雲端技術的發展，雲端服務供應商會

在市場提供新的雲端解決方案和服務。決策局／部門應進行內部研究及評估，識別潛在的風險，並採取相應的良好作業模式和最合適的部署模式。由於每種安裝都可能有各自指定的部署情景，推行者應自行判斷並選出最適合的保安控制。決策局 / 部門應確保雲端服務供應商在必要的控制和服務上提供適當的保護，使其在基礎設施的設計、開發、部署和配置過程中，能夠對政府數據（尤其是涉及敏感數據）提供適當保護，以便把政府數據與其他客戶環境適當隔離。

各標籤的意思如下：

「保安考慮事項及控制名稱」[I] [O] [P]

[I] - 「內部私有雲端平台」
[O] - 「外判私有雲端平台」
[P] - 「公共雲端平台」

附件A概括在不同範疇內，雲端平台推行的保安控制，以方便決策局／部門參考。

根據《基準資訊科技保安政策》第17.3節雲端運算保安，限閱或以上保密類別的資料不得利用公共雲端服務儲存或處理。

5.1 管理職責

機構所屬之數據的保安管理和控制最終須由該機構的用戶負責。應採用風險為本方法，於機構的資訊系統策略計劃及／或機構資訊科技計劃中加入雲端運算策略，並應採用及嚴格推行合適的保安管理作業實務及控制。要操作和維持一個安全的雲端運算方案需要嚴謹的管理作業實務，而良好的作業實務牽涉監管機構資訊系統資產，以及推行為建立和保存資訊系統資源機密性、完整性及可用性而制訂的政策、指引及程序。

在雲端環境內，許多雲端服務供應商或會容許使用者決定其數據的地理儲存位置。此外，未經同意，數據不能被移出使用者選擇的位置。如果沒有足夠的使用者監督，對維持可審計的數據位置記錄及確定數據在不同管轄範圍內可得到足夠的保護並不容易。此外，雲端服務供應商的服務牽涉使用嶄新科技包括先進的硬件基建及複雜的管理工作。若雲端服務供應商未能正確配置及處理其中任何部分，系統將可能出現故障或者導致保安事故。對於外判私有或公共雲端平台，「雲鎖定」是另一個挑戰。「雲鎖定」是指由於轉用另一雲端服務供應商將要面對的複雜性和困難，導致決策局／部門只可依靠現有的雲端服務供應商。這情況可能令業務難以轉移到新的雲端服務供應商。因此，建議決策局/部門採取措施應對此挑戰，包括：

- 確保實施數據備份、數據刪除和數據可攜性的最佳實踐；

- 確保選定的雲端服務供應商為決策局／部門提供可行的解決方案，以便從選定的雲端服務供應商遷出；以及
- 與多個雲端服務供應商合作，確保資料可攜性和配置已最佳化，以便從目前的雲端服務供應商遷移到新的雲端服務供應商。

- 依照不同管轄範圍分析對保安程序的影響 [O] [P]

決策局／部門應該確保他們能夠了解雲端服務供應商的雲端基礎設施中的數據儲存位置。所有合約應明確說明規管法律和司法管轄權條款。決策局／部門應注意保存在另一個司法管轄區的數據受該司法管轄區的法律約束。此外，不論數據儲存在甚麼地方，某些雲端服務供應商可能受其註冊所在的司法管轄區的法律約束。即使合約或服務水平協議規定了數據接達的限制，但仍不能凌駕該司法管轄區的法律。因此，決策局／部門應考慮到自身的權利可能受雲端服務供應商註冊管轄權管轄的風險。。而由於不同的法律和監管遵行要求，將數據及應用系統移至雲端服務亦可能對保安程序帶來影響。決策局／部門須根據儲存或處理數據的性質評估相關安排的風險。應詳細分析凡此的潛在影響，並制訂相關程序。如有必要，應就合約安排尋求法律意見，以確保敏感數據得到充分保護，免遭不自主披露。亦應考慮加強保安措施，例如數據加密和數據掩蓋 (請參閱第 5.4 節資產管理)，以彌補決策局／部門未能直接控制的範圍。受影響的程序可能包括事故報告、活動記錄、數據保存及應用系統測試。

- 核實對業界保安標準的遵行 [O] [P]

保安認證是對外聘雲端服務供應商保安管理、所需成熟程度及確保質素保證的證明。應檢查從而明瞭雲端服務對國際認可業界保安標準的遵從，例如

- ISO 27001（資訊保安管理）
- ISO 27017（雲端服務之資訊保安控制實務守則）
- ISO 27018（個人可識別訊息處理者在公共雲端保障實務守則）
- 服務組織控制報告 第二類（保安性、可用性、處理完整性、機密性和隱私控制的證明和保證）

此外，還應對雲端服務供應商進行檢查，以確保其遵守國家認可的行業保安標準，例如：

- TRUCS（可信雲服務，雲服務評估架構）
- ITSS（信息技術服務標準，雲端運算服務能力評估）
- DJCP（中國內地的網絡安全等級保護制度）

參考和基準測試這些標準將確保符合政府保安要求以及滿足營運效率和業務需要。由雲安全聯盟制訂的共識評估倡議問卷提供了一系列評核雲端服務供應商的參考問題。應要求外部雲端服務供應商出示有關合格證明書及報告以作核實。如果核實有效，這些認證可用於評估和驗證雲端服務供應商的基礎設施、服務以及所有準備就緒或正在使用的保安控制措施的保安性和合規性。

5.2 資訊科技保安政策

- 覆檢部門保安政策 [I] [O] [P]

應覆檢部門保安政策，並作出所需調整，以保障業務應用系統在雲端環境中，在部署保安控制以保護數據時仍然有效。調整範圍可以包括全新或經修訂而又針對雲端相關範疇（如多租戶特性、數據位置、虛擬化，以及雲端服務的安全使用等）的保安要求及控制。這些調整應與雲端服務供應商所採用，由第三方報告發布並可公開存取的行業最佳實踐保持一致。

5.3 人力資源保安

- 界定資源控制及資訊保安中的職務及責任 [I] [O] [P]

應清晰界定及記錄（例如服務水平協議）支援雲端服務運作及負責雲端服務資訊保安人員（包括但不僅限於決策局 / 部門和雲端服務供應商）的職務及責任，特別是外判的多租戶雲端環境數據中心。決策局 / 部門須要求雲端服務供應商確保負責處理包含政府數據的外判資訊系統的員工和承辦商，適合擔任該職務。應要求雲端服務供應商清楚分隔工作職責，例如同一人不應同時擔當系統及保安管理工作。須嚴格執行「有需要知道」原則，而且應備存負責監管機構的最新聯絡資料。

- 要求不可披露協議及確保適當人力資源管理 [O] [P]

在合適情況下，雲端服務供應商的人員及其分判商應同意及簽署不可披露協議。決策局／部門亦可透過合約形式（如雲服務合約）以確保雲端服務供應商的人員及其分判商履行保密責任。除非獲得授權，否則雲端服務供應商須承諾不會向任何第三方傳送或披露政府資料。如第三方要求存取有關資料，而該等要求不能直接拒絕，除非法律禁止，雲端服務供應商須立即通知決策局／部門，並將有關要求轉交他們處理。甄選雲端服務供應商時，應考量供應商向所屬而又擁有高接達權限的人員所作的背景審查程序，以及清晰的終止僱用過程和程序。在適用法律允許的情況下以及在適用政府機關提供的範圍內，背景審查宜按需要地包括相關人士過往的教育履歷、工作及犯罪紀錄。終止僱用程序宜要求相關人員歸還所有資產，尤

其是與其工作有關的重要資料、鑰匙及權標，亦必須刪除所有有關的接達權限。

- 發出指引或通知以提醒用戶 [I] [O] [P]

  應定期發出針對個別雲端應用系統的指引或通知，以確保雲端服務終端用戶全面留意數據的敏感程度，並對潛在的保安威脅保持警覺，使用戶能於數據生命周期中採取適當行動，例如在雲端系統刪除不再使用或不再需要保留的數據。

- 確保給予有關人員適當的保安訓練 [I] [O] [P]

  應定期為內部及外部人員，包括雲端服務供應商的分判商的員工，提供資訊保安意識培訓，以確保他們對保安保持警覺及理解保安要求（例如現行政府資訊科技保安要求），注意資訊保安風險和事故應變處理程序，以及明白不遵守雲端服務供應商制定的資訊科技保安規定時須承擔的責任和後果。負責保安管理及操作的人員宜持有國際、本地或業界認可的知名專業資歷，例如 CCSK[1]、CCSP[2]、 CISM[3]、CISP[4]、CISSP[5]、ITIL[6]或同等程度。

5.4 資產管理

非機構處所、外判數據中心、多租戶特性、互聯網的使用及其他許多雲端平台特性，再加上透過實體或網絡連接以未獲授權的方式來接達敏感數據，都造成保安風險。數據的機密性可能因為客戶配置錯誤和雲端網絡供應商對保護客戶的數據缺乏承擔而蒙受風險，進而令客戶應用系統及數據曝露於各種來自網絡威脅中。此外，在預期以外的服務中止情況下，例如公司合併、雲端服務供應商破產的狀況、服務關閉及任何其他預期以外的事件，決策局／部門可能難以或甚至不可能從外聘雲端服務供應商取回數據。

- 透過加密保護數據 [I] [O] [P] [7]

  數據加密能增強數據的機密性。決策局／部門應確認雲端服務所提供的加密功能能夠符合加密控制使用的加密政策。重要數據無論在靜止或傳遞中，都必須根據政府保安要求和業務需要採用嚴謹的加密方式以作保護。為避免受專有算法所綑綁，應使用開放和可靠的加密算法。而加密匙亦應

[1] CCSK －國際雲端安全證書
[2] CCSP －雲端資安專家認證
[3] CISM － 國際資訊安全經理人認證
[4] CISP － 註冊信息安全專業人員
[5] CISSP －資訊保安系統專家認證
[6] ITIL － 信息技術基礎架構庫
[7] 雖然沒有針對非保密數據加密的規定，但為更好地保障數據私隱，決策局／部門宜在使用公共雲端服務時，使用加密保護非保密數據。

在整個密碼匙生命週期中得到適當的保護和管理（參考第 5.6 節加密方法）。

- 遵守有關外判數據中心的數據保護及私隱法例 [O] [P]

須遵守資料保護和私隱法規。為保障個人私隱而又位於香港境內的個人資料，須遵守《個人資料（私隱）條例》（第486章），特別是保障資料第四原則（個人資料的保安）。

為追求更高成本效益，有些外判數據中心是設置於海外。跨境儲存於海外數據中心，或與海外數據中心作轉移的數據，因跨境的原因，此類數據中心可能受到當地法例規管，因此，資料存放可以考慮採用海外外判服務。然而，重要資料交易應在配備適當保安控制的本地數據中心內進行。

《個人資料（私隱）條例》（第 486 章）第 33 條雖然尚未頒布，但應在合適情況下參考該章節。第33條規管個人資料從香港特別行政區轉移至其他缺乏保護數據機制的地方，除非符合條例列明的例外情況。個人資料私隱專員公署已發表《將個人資料移轉至香港以外地方資料概覽》，提供相關參考資料。決策局／部門須確保雲端服務供應商會在轉移資料離開香港特別行政區前得到決策局／部門的批准。

- 個人資料去識別化 [I] [O] [P]

考慮將資訊系統的數據（包括收集、處理、存儲、歸檔及披露資料當事人的資料）去識別化，藉此加強數據保護。資料去識別化是指用於替換原始數據集的算法和過程，可在不影響業務目的的情況下，防止經處理的結果泄露資料當事人的身份。

除為了保護數據外，另一個實施個人資料去識別化的原因是政策合規。顯而易見，法規和私隱框架均著重對個人私隱的保護，並要求實施不同程度的數據去識別化[8]，以便更妥善保護個人數據。

去識別化並沒有一個劃一的做法可遵從。視乎獲取個人數據的數量、應用程式的敏感度，以及涉及個人私隱的事故對政府聲譽的影響等因素而定，

[8]《通用數據保障條例》Recital 28 規定「對個人數據應用假匿名可以降低有關資料當事人的風險，並幫助管制者和處理者履行其數據保護的責任。」

保護措施可從「假匿名」[9]開始擴展到「匿名化」[10]，以作全面保護。技術措施可考慮使用一般化[11]、隨機化[12]、標記化[13]及合成數據[14]等。

風險為本的方法有助確定所需的去識別化程度。私隱影響評估等評估工具如有助確保遵行並找出未處理的殘留風險。在設計系統時，須盡可能納入「貫徹私隱設計」的概念。

- 追蹤數據位置 [O] [P]

大多雲端平台用戶選擇私有雲端方案而非公共雲端方案的其中一個原因是數據位置。決策局／部門應注意雲端服務供應商在其雲端採用過程中提供的雲端服務，並確保他們完全了解其內容在虛擬雲端環境中進行架構處理的位置。應該讓客戶明白數據在靜止、傳遞時，以及備份的位置。亦應要求雲端服務供應商作出承諾，以確保當涉及敏感資料（特別是個人資料）時，除非得到決策局／部門同意，數據不會轉移到其它地區。

- 偵側及防止未經授權的數據遷移至雲端平台 [O] [P]

除了傳統的數據保安控制（如接達控制或加密方法）外，決策局／部門應避免政府數據，在未得到許可前移到雲端平台。決策局／部門可使用數據庫活動監察工具與檔案活動監察工具以監察有否大量的內部數據遭遷移；或使用網址過濾方法與數據遺失保護工具以監察數據有否移至雲端平台。

- 備存最新的資產清單 [I] [O] [P]

資產包括所有在雲端環境內的軟件及硬件元素，而決策局／部門的資產種類則因雲端服務模式而有所不同。決策局／部門須訂立及備存一份雲端環境內的最新資產清單。資產應包括以下：

(i) 業務資訊
(ii) 法律／合約文件（例如公共域名註冊和相關互聯網規約地址、數據儲存的實體位置等）
(iii) 虛擬設備
(iv) 虛擬儲存器
(v) 軟件

[9]數據假匿名是以一個或多個人工標識符（即假名）取代數據記錄中的可識別個人資料的方法。假名令個人資料不易從數據記錄中識別，但亦可用作數據分析和數據處理。
[10]數據匿名化是將數據轉化成不能識別個人身份的一種方法。
[11]數據一般化降低數據的精確度，同時在記錄層面保留數據真實性。通過減少數據集的所選屬性或一組相關屬性內包含的資料粒度以完成操作。
[12]數據隨機化增加歸檔數據的噪音。它不能在記錄層面保留數據真實性，但會降低單選標識屬性的風險。一般來說，數值會被修改，以使它們的新數值以隨機方式與其真實數值有差別。
[13]數據標記化以非敏感的數據元素取代敏感的數據元素。這種沒有外在意思的非敏感數據元素通常被稱為標記。該標記能隨後找出敏感數據。
[14]合成數據生成具有某些統計特徵的人工數據以作為目標數據。合成數據集不包含從現有數據主體收集或與之相關的任何數據，但對於預期目的而言看起來是真實的。

- 確保已達到使用壽命的電腦設備的棄置或重用控制是合適及得到妥善推行 [I] [O] [P]

  因為有些多租戶環境（如公共雲端服務）難以支援安全銷毀數據，所以應加倍留意棄置或重用電腦設備（如硬碟及備份媒體）前定位數據及安全刪除數據機制的完整性及效用。在甄選外聘雲端服務供應商時，在對電腦設備於有關服務期滿或終止時或政府提出要求時棄置或重用的要求中，應加入安全銷毀數據作為其中一個甄選的準則。決策局／部門應與雲端服務供應商合作，並考慮確保敏感數據依照行業最佳實踐例如 ISO 27001 安全清除或重複使用設備和 YDB144-2014（雲端運算服務協定參考架構）5.2 數據銷毀。雲端服務供應商須訂立在其所有平台上安全刪除政府資料的程序，並在資料刪除後以書面確認。亦應定期從雲端服務供應商取得相關的保安審計報告作分析，以確保符合所需的保安要求。

5.5 接達控制

決策局／部門使用任何類型的雲端模式都可能會質疑接達數據和系統的人員以及管理數據的人員。由於接達控制是系統保安的第一道防線，對接達和管理系統和數據的人員可見性和管理的不足將嚴重影響系統保安。在採購和部署雲端服務之前，應該充分理解用以監控和防範的未授權接達（特別是雲端服務供應商所提供的特權帳戶）的保安控制。並應該建立機制，在特權用戶被拒絕接達的情況下，容許恢復特權用戶的接達。

由於雲端平台多租戶的環境，存在第三方可透過雲端平台網絡接達共同資訊儲存服務的可能，導致數據外泄的風險。如果欠缺更細緻的資料接達控制，由未授權人士泄露敏感數據的相關風險將會提高。

決策局／部門應意識到多租戶雲端環境所帶來的風險，並與雲端服務供應商合作，了解為減輕未經授權的數據接達風險而實施的邏輯隔離控制。另外，若雲端應用系統存有與企業不同的一套用戶身分，用戶權限被解除時，由企業用戶目錄更新到雲端應用系統之間將會出現時間差。這時間差可能讓未授權人士在修改生效前接達敏感數據。

決策局／部門應推行密碼匙管理程序，以便涉及重要資料時，密碼匙不會與雲端服務供應商共享。簡而言之，在包含重要資料的公共雲端環境進行數據儲存加密時，決策局／部門應採用自己的密碼匙管理或單獨及獨特的密碼匙管理服務。決策局／部門還可以利用雲端服務供應商提供的雲端原生硬體保安模組（HSM）服務來實施緊密結合的保安雲端環境，而無需與其他第三方供應商建立額外的保安依賴性。雲端服務供應商提供的HSM服務應符合國家密碼管理局（SCA）測試認證的合規標準，並符合以下要求：

- （GM/T 0030 服務器密碼機技術規範）

- （GM/T 0045 金融數據密碼機技術規範）
- （GM/T 0029 簽名驗簽服務器技術規範）

無論哪種類型的雲端模式，決策局／部門都應實施上述數據保安控制措施，作為額外的保安層，以減輕未經授權的數據接達的風險。

- 清晰訂立邏輯控制 [I] [O] [P]

  雲端環境的運作可能牽涉不同的單位，包括操作小組、應用系統支援小組、基本設施支援小組及數據中心維修小組，而授權人士亦可能是內部或由雲端服務供應商或其分判商聘用。由於未獲授權接達數據的風險隨着獲准處理資訊資產人士數目的增加而提升，所以需要清晰確立邏輯接達控制內的認證及授權機制，例如誰應獲准接達數據、他們又有哪些接達權限，以及在甚麼情況下給予什麼接達權限。對於人員接達雲端平台數據，應採用「預設全部拒絕」政策及須遵循最小權限原則。

- 建立身分及接達管理架構 [I] [O] [P]

  應考慮使用身分及接達管理架構。身分及接達管理架構容許透過使用公開標準如 OpenID，擴展身分及接達管理實務，藉此於雲端平台管理用戶帳戶的設置、認證及授權。成熟及業界認可的認證及授權標準如安全斷言標記語言、可擴展接達控制標記語言都可以更進一步改善保安狀況，應適當應用這些標準的保安功能，例如安全斷言標記語言的可擴充標示語言簽署及可擴充標示語言加密。於身分及接達管理中採用聯合身分，能夠有助不同身分儲存庫互相聯結，容許用戶透過單一登入接達不同的應用系統。

- 採用接達控制標準 [I] [O] [P]

  一旦採用雲端服務，用戶身分將可能因為身分儲存庫或目錄管理服務連接至雲端服務供應商而延伸至雲端平台。在選擇雲端服務時，宜考慮到服務應利用業界標準（例如安全斷言標記語言），推行安全單一登入方案，以傳遞用戶身分及屬性，以及執行授權政策。

- 要求嚴謹的認證選項 [I] [O] [P]

  雲端服務可以透過不同裝置及渠道接達，因此簡單的用戶登入名稱及密碼的認證未必足夠保障帳戶免受入侵。在選擇雲端服務時，應考慮支援雙重認證（2FA）的雲端服務，並應盡可能為衆多用戶，特別是特權帳戶啟用雙重認證。常用的雙重認證有一次性密碼、生物特徵和數碼證書等。

  為了進一步提供保護，用戶接達（尤其是特權帳戶）應限制於指定的電腦、網絡或位置。數字政策辦公室發表的電子認證架構 [15]為評估風險、決

[15] https://www.infosec.gov.hk/tc/best-practices/person/securing-access-using-e-authentication

定保安要求，以及推行適當認證方法提供基礎。應跟從該架構，決定及推行雲端服務上電子交易的電子認證要求。

- 管制及控制高權限實用程式 [I] [O] [P]

  於雲端環境內執行未授權的高權限實用程式，可能會令系統及應用系統的控制失效。決策局／部門應向雲端服務供應商要求提供高權限實用程式的功能規格，以確定在使用這些程式接達雲端服務時，保安控制仍然生效。

5.6 加密方法

- 管理及保護密碼匙 [I] [O] [P] [16]

  密碼匙應根據保安規定及政策得到妥善管理及保護。應切實執行密碼匙儲存管理，密碼匙應由決策局／部門保管。須界定密碼匙生命周期的管理流程：密碼匙如何產生、使用、儲存、備份、復原、流轉及刪除。加密操作及密碼匙管理宜限制於身份及接達管理系統之下以加強保護。決策局／部門不應在不同的雲端平台重複使用同一個密碼匙，以避免當密碼匙被破解後，所有雲端平台（特別是混合雲端的情況下）亦因此遭到入侵。

5.7 實體及環境保安

一如外判私有雲端平台，公共雲端平台的數據中心位於客戶機構處所以外，雲端平台亦可能跨越數個位處不同地理位置的數據中心。當數據移到非決策局／部門的雲端平台數據中心，數據的實體控制將交到雲端服務供應商。由於公共雲端平台的多租戶特性，其中一項主要的保安關注便是數據受同平台不明租戶或第三方未授權的實體接達的風險。

於雲端數據中心推行充足的實體保安措施，能防範於實體層面運算資源遭入侵的活動。有些雲端服務供應商只提供沒有上鎖的電腦機架。這顯然不足以應付多租戶環境，因為任何能出入數據中心的人士都有機會接觸到存有租戶數據的電腦裝置。處於非機構處所的雲端平台數據中心的環境及設備保安，以及實體接達控制都是實體保安範疇上主要關注的地方。

由公共雲端服務供應商提供的服務通常不是針對單一租戶環境。隨着服務的不斷更新，這些雲端服務供應商可提供新的解決方案和服務給雲端平台用戶，例如單一租戶解決方案，以迎合市場的需求。建議決策局／部門在選擇適當的部署模式時透過仔細檢查有效的合規性認證，以研究和驗證整個雲端解決方案，包括基礎設施的構建和雲端服務供應商保安控制的運作有效性。例如，如果決策局／部門考慮使用私有雲端平台來滿足業務需求和保安要求，那麼單一租戶方案只是其中一個考慮因素。決策局／部門亦應評估雲端基礎設施需否專用，

[16] 雖然現時的規定沒有涵蓋非保密數據需要加密，但作為保障數據私隱的良好作業實務，決策局／部門宜在使用公共雲端服務時，對非保密數據，採用加密技術，並同時對密碼匙作管理及保護。

以滿足私人雲端解決方案的要求。據此，決策局／部門應根據業務需要和政府保安要求，評估在整體架構上推行何種保安控制措施。

- 選擇場地位置及設施的風險分析 [O] [P]

  處於非機構處所的數據中心的設計和管理在實際上未必將保安放在最優先次序。事實上大部分雲端服務供應商都將焦點放在成本效益上。因此，在合適的情況下，不間斷電源供應器、空氣調節及通風系統、滅火系統、水災損害及水浸控制系統等相關設施的運作控制有效性應被適當的全球認可的行業保安標準（即 ISO27001、ISO 27019、GB/T 22239、DJCP 等）驗證。應根據地方的自然災害、地區（例如當地管轄權）、網絡依賴程度（例如互聯網網絡樞紐）等，評核數據中心、運作復原中心的選址及運作。在不能進行實地考察的情況下，決策局／部門應審視表明由獨立第三方審計員對雲端服務供應商進行的年度審計的第三方報告，以確保這些實體保安控制措施符合認證審計要求（即 ISO 27001、服務組織控制報告第二類等）。

- 為外判數據中心的所有資訊科技設備及數據儲存媒體採取適當實體保護 [O] [P]

  由於外判雲端平台的多租戶特性，可能會於外判雲端平台數據中心發生未授權接達，所以應對共享數據中心內，所有資訊科技設備及數據儲存媒體，並所有場外備份媒體訂立保安要求，以給予合適的實體保護。雲端服務供應商所推行的保安措施應合乎這些保安要求。

- 有需要時劃出獨立區域作專門用途 [I] [O]

  若因為數據的敏感程度或其他保安要求，而有特別需要不與其他租戶共享設備或載有其他租戶應用系統的設備架，可考慮設立獨立區域，將應用系統擁有人的數據及資源，通常包括伺服器、網絡設備、儲存器、電源及訊號電線，與其他租戶分隔。應清楚界定應用系統擁有人在數據中心內的獨立區域範圍，並應只容許獲授權人士接達該區域。另外，數據中心亦不應向公眾開放，令公眾可以容易進出。為減少未授權或無可避免的接達，獨立區域不宜設於公用區域如走廊及主要出口附近。所有數據中心的實體接達都應得到數據中心經理批准並記錄在案。

- 限制獨立區域的出入 [I] [O]

  應使用電子控制接達系統或其他同級的接達控制措施嚴格控制獨立區域的出入。即使在有人的情況下，獨立區域應長期保持上鎖。應使用雙重控制於授權及審批獨立區域的出入，包括授權及批准增減長期出入人員名單。長期出入人員名單應由應用系統擁有人或其他獲授權人士審批。所有有需要到達獨立區域或設備架的出入人士都應先得到批准並記錄在案。應定期（如每季度）覆檢區域出入人士的記錄，確保記錄完整準確，亦應定期覆檢長期出入人士名單。

- 考慮為受控制區域訂立不同的保安級別 [I] [O]

  對於包含敏感或保密資料的外判資訊系統，決策局／部門須確保服務供應商已採用適當的控制措施，以管理對設有資訊系統的實體區域的接達，以及限制未經授權的其他客戶或外人的接達，並僅允許政府批准的人員或訪客進入。

  為提高保安水平，值得考慮為數據中心不同區域推行不同程度的控制。一般而言，可以根據寄存於區域內應用系統的重要性及數據的敏感程度，決定該區的出入控制程度。應清楚記錄及標記受控制區域的實體及管理控制。
- 確保為共用相同設備架的多個應用系統採取合適接達控制 [I] [O]

  在不同應用系統共用設備架的情況下，應於設備層面，而非設備架層面，訂定實體接達審批。此外，為減低共享設備架的風險，亦應推行其他接達控制，例如獨立鑰匙鎖、帳戶鎖定政策及定期覆檢系統記錄。

5.8 操作保安

5.8.1 資訊備份

- 定期為數據備份 [I] [O] [P]

  因為客戶數據存於雲端服務供應商的備份媒體時，可能會和其他雲端平台租戶數據混在一起，雲端服務供應商未必能提供分離或專用的備份媒體予個別雲端平台租戶。對業務具有重要影響的系統，決策局／部門應確保最少保留一份定期營運數據的離線備份，以便可以復原至最新狀態。在此情況下，須定期進行備份測試，確定復原程序合乎現況並且是有效的。應穩妥儲存備份，以及日誌、接達記錄及任何因法律和規管原因而需要的相關資訊的副本，並應只容許獲授權人士接達。

5.8.2 記錄

- 為審計、分析和調查保存及保護記錄 [I] [O] [P]

  對於無論公共或私有雲端平台，取得關鍵記錄數據對清晰瞭解操作及保安事件尤其重要。部分類型的記錄數據有助減低操作及保安風險。決策局／部門應界定記錄種類及內容，如網絡、系統、應用程式、管理和變更管理活動的審核記錄。記錄資訊應全面，而且能夠反映雲端平台的動態特性，例如增減虛擬機器執行個體。應妥善訂明記錄的保存期，記錄亦應能防範干擾。對於公共雲端服務，決策局／部門應要了解雲端服務供應商會否容許用戶修改記錄設定及會否提交所需記錄數據，而且應有與系統關鍵程度相稱的記錄覆檢程序。可以使用事件關聯工具加強記錄分析功能。

5.8.3 配置管理及控制

- 確保妥善執行保安程序 [I] [O] [P]

  應建立程序收集及儲存審計記錄、活動報告、系統配置副本、修改管理報告及其他測試程序結果。視乎雲端服務模式，雲端服務供應商應在有需要時應提供這些資訊。

5.8.4 修補程式管理

- 確保修補程式管理過程有足夠控制 [I] [O] [P]

  修補程式賦予程式新功能，並解決程式內的錯誤或保安漏洞，但由於修補程式是額外／經修改的編碼，它亦可能為程式帶來不可預計的不良副作用，造成重大風險及嚴重影響數據的機密性、完整性及可用性。因此，決策局／部門應瞭解雲端服務供應商如何處理以減少不明朗因素，例如雲端服務供應商如何釐定修補優先次序，以及執行修補程式的時間表。另外，修補程式管理應得到決策局／部門及雲端服務供應商雙方同意。

5.9 通訊保安

於雲端平台數據中心，實體伺服器及網絡組件都被虛擬化，並可能由數個租戶共用。傳統網絡的保安措施未必能有效防範雲端環境內，同一伺服器上虛擬機器的攻擊。由於部分保安威脅只針對某些虛擬化基本設施，例如通訊盲點、虛擬機器間攻擊，及虛擬機器混合信任水平，加上虛擬機器變化不定的特性，都會令維持保安水平及確保記錄可被審計的工作變得困難。複製伺服器影像並發佈到其他實體伺務器的過程十分方便，但亦導致配置錯誤及其他漏洞借此傳播。當採用及推行雲端平台基礎建設時，需要處理這些由虛擬化帶出的保安威脅及問題。建議決策局／部門透過檢視雲端服務供應商所獲得的有效合規認證來驗證保安控制措施的運作有效性。

此外，由於數據在分散式雲端平台部署中會被共用，數據在雲端服務中可能會於不可信網絡（例如互聯網、公共網絡）及／或政府網絡間傳遞，所以應妥善保護傳遞中的數據。網絡及通訊的安全作業對雲端服務非常重要。

5.9.1 一般網絡保護

- 於傳遞時保護數據 [I] [O] [P]

  決策局／部門應於多租戶或外判數據中心環境內，加強對在伺服器及網絡組件之間傳遞的任何重要數據的網絡保安水平。為避免竊聽，應為在數據中心內的通訊網絡上進行的數據傳輸進行加密，例如傳輸層安全性規約

（TLS）。建議在連接到雲端服務時採用保安措施（如虛擬私有網絡、傳輸層安全性規約）保護在公共網絡（如互聯網）或政府網絡上以保障傳遞數據的機密性及完整性。在適用的情況下，亦可考慮使用數據層面的加密方法，令數據在傳遞前可被加密。

- 保護網絡上的運算資源 [I] [O] [P]

  很多裝置，例如伺服器、桌上及手提電腦、智能手機及平板電腦都能利用互聯網連接雲端伺服器。外來入侵者可能透過系統漏洞對雲端環境的網絡組件及伺服器發動攻擊。另外，亦不容忽視在多租戶環境內，藉著雲端間通訊進行的內部入侵。應推行適當的網絡保安措施，令運算資源在有關的措施下得到保護，例如網絡防火場、應用系統防火牆、入侵偵測系統／入侵防禦系統及記錄監察。應留意要成功抵禦攻擊，就需要保護雲端運算的客戶端及伺服器端雙方。

5.9.2 虛擬化的保安

虛擬化技術是讓雲端平台實現多租戶或多應用系統環境靈活部署及提供按需要服務的主要機制。虛擬化能讓雲端服務供應商從實體伺服器的剩餘能力取得更多運算資源，但亦同時帶來保安風險。雲端運算的特性令決定如何處理保安事故、數據外泄或其他需要調查的保安問題變得困難。

正如第5.7節所述，由公共雲端服務供應商提供的服務通常不是針對單一租戶環境或單一應用環境。隨着科技和市場發展，一些雲端服務供應商可能在行業中提供新的服務和方案。有些公共雲端服務供應商也可能擴展他們的方案，容許租戶對雲端服務資源有更多的控制，因此有些原本對私有雲端適用的虛擬化的保安考慮也擴展至適用於公共雲端。

同樣，建議決策局／部門在選擇適當的部署模式時，應檢視雲端服務供應商所獲得的有效合規認證以仔細研究及驗證雲端服務供應商整個雲端基礎設施及保安控制措施的運作有效性。例如，如果決策局／部門考慮使用私有雲來滿足業務需求，那麼在評估其是否為專用雲端基礎架構時，無論是否使用虛擬化，單一租戶環境只是其中一個考慮因素。因此，決策局／部門應根據業務需要和政府的保安要求，對整體基礎設施應該推行何種保安控制措施進行評估。關於虛擬化的保安實踐，請參考以下要點：

- 保持主機操作系統精簡及堅固 [I] [O] [P]

  為減少受攻擊風險及修補次數，主機操作系統應配置最少所需功能。應強化及盡量精簡已安裝的主機操作系統，例如停用不必要的服務和通訊埠，務求減低載入任意組件、軟件庫和軟件的能力。

- 部署高可用性技術 [I] [O] [P]

為應付單點故障，應考慮復原能力如主機上的虛擬機器集群。例如當一個主機失去供電時可能會影響數個虛擬機器。在硬件故障的情況下，受影響的虛擬機器可以利用剩餘能力於集群節點中自動重啟，令服務影響減至最低。

- 為虛擬化中的每個獨立組件訂立保安要求及鞏固組件 [I] [O] [P]

  整體虛擬化方案的保安非常依賴當中每個組件的個別保安。從虛擬機器管理程式和主機操作系統，到客戶操作系統、應用系統及儲存服務，所有這些組件都應根據相關的保安政策及標準而強化。應使用涵蓋所採用虛擬化技術的漏洞掃瞄工具定期掃瞄主機及客戶操作系統，並應制訂及推行配置管理程序，將虛擬環境內，實體及虛擬機器的所有保安設定納入管理。

- 啟用虛擬機器專屬的網絡保安功能 [I] [O] [P]

  虛擬機器可以於硬件底板上作通訊，而非透過連線網絡。底板上的通訊並不能夠被監察，或在有可疑通訊時線內攔截。應採用虛擬機器專屬的保安機制，例如虛擬網絡及虛擬機器管理程式層的虛擬防火牆，對虛擬機器底板上的通訊進行更仔細監察。應只容許獲授權人士遠端接達虛擬機器的管理控制台。

- 執行最小權限原則及工作分隔 [I] [O] [P]

  在分散及虛擬化環境內，如何制定細分電腦用戶（包括不同的管理員）的角色和職責頗具挑戰。雲端、虛擬機器架構、儲存器、網路和系統的管理員應能執行他們的職務而無法接達到他們所管理的系統中的敏感資料。決策局／部門應嚴格執行職務分工，並定期檢討以防範不同的攻擊，包括外部攻擊（例如：進階持續性滲透攻擊）或內部攻擊。此外，應將保安管理工作的帳戶、職務及人士與其他行政活動分開，防範未授權修改，進一步保護電腦資源及審計追蹤。

- 建立安全區域分隔不同信任水平的虛擬機器 [I] [O] [P]

  應在發展虛擬機器環境初期，探討分隔虛擬機器的效用及可行性。建議依據發展階段（如設計、測試及投入運作）、數據重要性、架構層（例如網絡、應用程式、數據庫和檔案）或系統關鍵性（關鍵系統及非關鍵系統），於不同的實體伺服器上建立安全區域。若不能避免於同一實體伺服器上分享不同類型的數據／系統，則可同時利用虛擬局部區域網絡、防火牆及入侵偵測系統／入侵防禦系統，分隔虛擬機器作為對策。連接虛擬化環境到內部網絡不應削弱現有保安水平。

- 於較關鍵系統考慮使用裸機（類型 I）虛擬機器管理程式 [I] [O]

一般而言，有兩類虛擬機器管理程式 —裸機（類型 I）及寄存式（類型 II）。裸機虛擬機器管理程式於硬件產品上運行，而寄存式虛擬機器管理程式則安裝在主機操作系統（例如 Linux）之上。寄存式虛擬機器管理程式有可能會繼承主機操作系統的漏洞，以及在相對複雜環境內面對更多保安威脅。相對地，裸機虛擬機器管理程式一般提供更精簡及安全的硬件操作系統，而且這類虛擬機器管理程式直接與硬件作溝通，減少保安問題。一般而言，與私有雲端平台相比，決策局／部門在與其他使用者共享公共雲端基礎架構時可能需要考慮其他因素。因此，即使公共雲端服務供應商提供裸機虛擬機器管理程式時，公共雲端平台仍可能不適用於關鍵系統，特別是當涉及保密資料時。因此，這項保安考慮和控制不應用於公共雲端平台情景。

- 分析相關保安風險 [I] [O] [P]

  在推行虛擬化前，應先與沒有虛擬化的選項比較，分析當中保安風險。這應成為選出雲端服務供應商或產品前的風險管理程序的一部分。

- 覆檢虛擬機器及應用系統的資源要求 [I] [O] [P]

  為避免資源衝突，應妥善計劃及檢討資源的運作，例如中央處理器、記憶體、輸入／輸出流量、磁碟空間，以及網絡容量。

- 防範兩個虛擬機器之間的未授權接達 [I] [O] [P]

  應對虛擬機器間的溝通採取最小權限原則。例如虛擬機器應適當配置，收緊主機防火牆規則及關掉不必要的網絡規約，以防範未獲授權接達。

- 備存資產記錄 [I] [O] [P]

  已部署的虛擬化環境需要記錄在案。由於在虛擬化環境內，有些網絡組件（如虛擬交接器／防火牆）未必能容易地利用線上工具辨認，因此需要準備一份可供審計的完整虛擬機器及基本設施組件詳細清單，並應保持更新。

- 確保軟件使用證有效及足夠 [I] [O] [P]

  虛擬化正改變軟件授權方式。不同軟件供應商可能採用不同授權方法，例如按個體（實體或虛擬）、硬件（實體或虛擬）、用途，或客戶（例如人數或同時連接數目）等。在很多情況，決策局／部門需要評估、商議及優化與主要供應商訂製在虛擬化環境內的使用協議。

- 為離線虛擬機器安裝最新的保安修補程式及病毒識別碼 [I] [O] [P]

  休眠中的虛擬機器容易被保安及監察作業忽略，導致虛擬機器曝露於已知的威脅中。決策局／部門應就此強制要求更新休眠虛擬機器的保安修復程

式及病毒識別碼。在合適情況下，可以考慮使用一些先進的保安工具以應對休眠中而又有修補需要的虛擬機器。

- 檢驗快照復原後的虛擬機器保安狀況 [I] [O] [P]

  大部分的虛擬機器容許建立「快照」，儲存不同時間的機器設定及配置狀態，作備份及維修之用。若有需要從過往一段時間的快照復原虛擬機器，必須查核快照的修補程度以及其保安設定及配置。應開啟虛擬機器的審計追蹤功能，包括修補工作，以追踪不同活動。

- 保護虛擬化影像及配置檔案 [I] [O] [P]

  因為虛擬機器連內在的數據及應用系統能夠從一個主機被複製到另一主機上，入侵者可將虛擬機器副本帶到另一個不安全的虛擬機器管理程式，從而接達原本虛擬機器內的數據及配置檔案。決策局／部門應收緊具審計功能的邏輯及實體接達控制，防範未授權接達及修改資源池，例如中央處理器、記憶體及儲存輸入／輸出裝置。

- 關掉不必要的通訊埠、服務及虛擬硬件 [I] [O] [P]

  應關掉所有不必要的通訊埠、服務及虛擬硬件例如通用串列匯流排埠、虛擬機器間的剪貼簿功能及虛擬網絡適配器等，令各元件間互相被邏輯性隔離，防範因其中一個虛擬機器受到入侵，而洩露數據至其他虛擬機器。

- 按需要地為每個虛擬機器或相關虛擬機器集群推行基於虛擬機器管理程式、基於網絡及基於主機的保護方案 [I] [O] [P]

  基於網絡的防火牆（或入侵偵測系統）能於多租戶環境有效運作。而基於主機的防火牆則提供較細緻的網絡控制，能在虛擬環境內運作，但在大型雲端環境可能有工作量及管理問題。基於虛擬機器管理程式的防火牆為動態雲端環境提供保安自動化功能，監察及欄截虛擬機器間的惡意通訊。應小心選擇以上的防火牆，以符合業務需要，並為防火牆配置嚴謹的防火牆規則。防火牆亦應能在重置虛擬機器時，便携到新環境上。

- 記錄虛擬機器管理程式和虛擬機器上，高權限帳戶的活動 [I] [O] [P]

  為追蹤保安事故的源頭及事件，需要記錄高權限帳戶在虛擬機器上的所有活動。同樣地，由於虛擬機器管理程式擁有管理及配置轄下虛擬機器的能力，因此亦需要記錄虛擬機器管理程式的高權限帳戶。保安記錄應包括例如接達虛擬機器影像及快照、變動用戶接達權限，及修改檔案權限等事件。應考慮使用防竄改記錄工具及完整性監察工具以確保記錄檔案完整，亦應定期監察及覆檢保安記錄。

- 小心管理虛擬機器影像及快照 [I] [O] [P]

虛擬機器的影像及快照可能收集了在取得影像／快照一刻，出現在系統內的政府資料。因為快照記錄了拍照一刻活躍記憶體的內容，所以快照比影像的風險更高。若不能防範影像／快照被修改，入侵者就有可能接達，並注入漏洞或惡意軟件，然後於虛擬環境內重新部署。應刪除不再使用的影像副本及快照。應確實執行與虛擬機器所處理數據的重要性同級的保安措施，以保護相關的虛擬機器影像和快照。

- 安全清除虛擬機器數據 [I] [O] [P]

  當在實體伺服器刪除虛擬機器，或將虛擬機器移到另一實體伺服器時，決策局／部門應確保磁碟上沒有殘留任何可作復原之用的數據。應使用安全刪除方案清除虛擬機器。

- 保護管理界面 [I] [O] [P]

  應在虛擬機器以外執行保安控制，以免管理界面（例如網上管理界面及應用程式界面）受到未授權接達。應在啟用審計追蹤功能的情況下，控制和監察所有管理對話，以盡早偵測並阻截未授權或可疑的對話。

5.10 系統購置、發展及維護

隨着雲端運算的興起，保安架構亦趨高度多變。雲端特徵，例如於一個數據中心內與多租戶共享電腦資源，令配置管理及持續服務供應亦比傳統資訊科技環境更見複雜。雲端運算影響著軟件發展周期的各個方面，亦為建立及維持現行應用系統的工具和服務帶來一些新挑戰。

對於一些軟件即服務的應用系統，雲端服務供應商將多個租戶數據儲存至應用系統數據庫，並在每個數據庫表加入額外屬性如「租戶名稱」識別租戶。惡意租戶可以透過軟件漏洞，例如手稿程式錯誤或經特製結構化查詢語言的查詢，入侵應用系統，並接達其他租戶數據。此外，保安弱點諸如過時網頁瀏覽器和未受保護的網頁對話，都可能導致應用系統的完整性和數據機密性受損害。所有與應用系統保安有關的保安問題在應用系統移至雲端平台後仍然適用。

- 在雲端應用系統上，應用安全軟件開發周期[I] [O] [P]

  雲端平台上建立應用系統時，應該採用安全的軟件開發周期程序（或其他合適的開發方法），例如保安設計覆檢及軟件測試，務求減少應用系統在發布後面對的潛在威脅。通過在開發周期的積極檢查，以解決整個開發過程中的保安威脅。這包括：

  (i) 在設計階段建立威脅模型，於早期識別及減少潛在保安問題；
  (ii) 依循編寫程式的良好作業模式及安全編碼標準（例如源始碼審查、個人資料去識別化、數據輸入確認及輸出編碼要求），防範網上應用系統漏洞；以及

(iii) 於部署前要求使用不同工具（例如程式碼掃描和分析工具、測試工具和源始碼混淆工具）作測試、驗証及程式碼保護。

- 管理及保護憑證 [I] [O] [P]

  雲端技術令應用系統部署變得容易，而部署工作亦一般由雲端平台的開發人員專責。管理及保護進入運作環境的憑證亦變得重要。應小心保管憑證，以協助防範未授權接達及非法竄改應用系統程式及控制檔案。應訂立周詳的政策及程序並嚴格遵守，以維持應用系統環境的完整性。

5.11 外判資訊系統的保安

公共及外判私有雲端平台的雲端服務都並非經內部人員管理或操作。就外聘雲端服務供應商管理的雲端服務的相關保安作業，須考慮以下方面：

- 在決定開始使用處於外判數據中心的外判雲端服務前，分析保安風險[O] [P]

  應依據資訊科技保安要求分析所有保安風險。分析結果將為管理層提供基礎以就開展外判雲端服務作出合適決定。

- 在準備外判標書時，清楚界定外判範圍的保安要求 [O] [P]

  在準備外判標書時，應清楚界定業務及保安範疇內的相關要求，如實體保安、管理職責、保安事故管理及保安風險評估及審計，並列明可量度的表現指標。應在定制的服務水平協議內列明要求。亦如任何外判安排一樣，應清晰釐清數據擁有權，並得到雲端服務供應商同意。

- 制定服務水平協議及監察修改 [O] [P]

  應充分留意由服務水平協議條款引起的後續效應，例如數據位置、不同方面的職務和責任、遵行要求，以及數據備份及復原等。有需要時，修改服務水平協議以解決任何可能導致保安事故的保安問題。決策局／部門應評估及確定服務水平協議內的條款合乎自身業務及保安要求。對於公共雲端服務，由於雲端服務供應商可保有權利於任何時間更改一些服務水平協議內的條文，並只有限度提早作出通知，因此應定期訪問雲端服務供應商網站，檢查通用條文有否任何改動。

- 確保外聘雲端服務供應商提供符合政府保安要求的保安控制 [O] [P]

  應推行控制機制，以滿足政府的保安要求。決策局／部門應在適當情況下盡職審查及監督雲端服務供應商以滿足業務、保安及私隱需要。對於雲端服務供應商未能完全處理的風險，決策局／部門應提供額外的控制以減低該風險。

- 確保妥善解決外來威脅 [O] [P]

  外判雲端服務供應商應利用最佳作業實務保護本身提供的主機及應用系統，以防範外來威脅及未授權接達。在可行的情況下，作業實務可包括，但不限於，強化操作系統、以最新修補程式保持更新、適當安裝基於虛擬機器管理程式、基於網絡或基於主機的抗惡意軟件程式、入侵偵測系統／入侵防禦系統及防火牆。雲端服務供應商應定期進行保安風險評估，確保系統保持所需保安水平。決策局／部門亦應定期覆檢雲端服務供應商提交的保安風險評估及審計報告。

- 制訂退出策略 [O] [P]

  應於採用雲端服務早期制訂退出策略或退出計劃。退出計劃宜由雲端服務供應商或決策局／部門提供。退出計劃應包括如何將數據及虛擬環境從雲端服務供應商處提取，以及如何清除數據及虛擬環境。在制訂退出計劃過程中，亦需處理與單一雲端服務供應商捆綁的風險。通過對退出條款的再行商討亦有助減低風險。

5.12 資訊保安事故管理

即使資訊系統已採取所有必需的保安措施仍會偶爾發生保安事故。保安事故處理涉及保安事故發生前，發生途中及發生後的一系列連續的過程。雲端運算的特性令決策局／部門在保安事故、資料外泄或其他需要調查的保安問題上，更難決定該如何處理。例如，決策局／部門可能認定一宗保安事故為危急，但雲端服務供應商未必同意該分級，並因而只投放有限的工夫調查和跟進個案。

雲端運算的採用改變了事故應變的結構，尤其於公共雲端平台上，由於決策局／部門並不擁有該網絡，所以不能直接接達網絡記錄。一些雲端服務供應商在他們的通用水平服務協議上列明供應商並無責任調查任何可能導致保安事故的保安違規及服務濫用。決策局／部門應留意以下事故監察及應變的保安作業實務：

5.12.1 保安事故監察

- 界定事故監察及通報責任 [O] [P]

  在服務水平協議內，應訂明外聘雲端服務供應商在事故監察上，能給予決策局／部門的支援。源自雲端服務供應商基礎設施的資訊保安事故可能影響決策局／部門的資源，因此應向決策局／部門詳細通報。決策局／部門亦應與雲端服務供應商建立通訊計劃，於發生事故時通報及升級處理。服務水平協議應記載清晰的事故分類計劃、通報責任，以及雲端服務供應商應達到的服務水平。

- 提供資料作事故分析 [O] [P]

  決策局／部門應得允許接達與事故偵測有關的數據來源及資料，雲端服務供應商亦應為事故分析提供適當協助。備份及其他記錄副本、接達記錄，以及任何其他相關資料都應能被移離雲端環境。對於公共雲端服務，記錄資料的可用性會因用戶所選項而異。應開啟並適切配置審計追蹤及記錄功能。

5.12.2 保安事故應變

- 確保符合事故應變規定 [I] [O] [P]

  決策局／部門應留意雲端服務供應商整體事故處理的理念，以及確保供應商對保安事故所採取的行動及應變時間符合部門的要求。應清楚界定雲端服務供應商在事故應變中的職務。決策局／部門應與雲端服務供應商就如何收集、儲存及分享事故調查証據（例如保安記錄）達成共識。

- 覆檢雲端服務供應商往績 [O] [P]

  若有的話，應取得及覆檢雲端服務供應商的事故應變管理往績及經驗。現有用戶就事故應變計劃的推薦將有助參考。

- 為非機構處所雲端服務訂立事故應變管理及程序 [I] [O] [P]

  決策局／部門應就事故應變措施與雲端服務供應商緊密合作，並應已建立及備存處理雲端服務事故處理管理及程序。與一般系統相似，事故處理程序應包括向政府資訊保安事故應變辦事處匯報，以及根據《資訊保安事故處理實務指引》作出的採取行動。應制訂及建立有效機制來報告、通知、調查及處理資訊保安事故或保安違規。雲端服務供應商應於供應商及決策局／部門同意的時間，向決策局／部門指派的聯絡人報告所有有關保安的問題。應有一套內部升級程序處理事故，旨在能迅速應變及得出適當決議，以對決策局／部門運作的影響減至最低。有需要時，亦宜將以上安排所得的表現指標納入服務水平協議內。

- 與雲端服務供應商為事故應變進行演習 [I] [O] [P]

  決策局／部門須在可行的情況下與雲端服務供應商合作進行事故應變演習。可行的演習方法包括紙上演練、電話串聯演練，以及全面演習。應於新版本的事故應變計劃中記錄改善之處。

5.13 資訊科技保安方面的業務持續運作管理

- 確保有效的數據備份及運作復原安排 [I] [O] [P]

  無論由決策局／部門或雲端服務供應商管理運作復原安排，決策局／部門都應確保這些安排的效用與決策局／部門的要求一致；訂定復原點目標及

復原時間目標、運作復原中心位置、復原小組的職務和責任、運作復原事件用的通訊渠道，以及復原優先次序，並與服務水平協議互相聯繫。

- 制訂業務連續性計劃 [I] [O] [P]

  決策局／部門的業務連續性計劃應包括失去雲端服務供應商服務及失去需要倚賴的第三方支援。應與雲端服務供應商協調，測試計劃的這個部分。若情況許可，應檢視雲端服務供應商的業務連續性計劃。建議要求雲端服務供應商提供現行管理支援的証據，以及雲端服務供應商業務連續性計劃定期覆檢的証據。

5.14 遵行要求

在規模經濟的考慮下，雲端服務供應商推行多租戶環境及混合使用資源池。尤其在用戶共享的公共雲端平台、數據中心、運算裝置、數據儲存器及人力資源。而由於私隱問題，一般不會容許個別決策局／部門進行深入的評估及審計。在大部分的公共雲端平台，雲端服務供應商未必能夠同意個別決策局／部門自訂審計責任。若雲端服務供應商不允許客戶直接進行保安風險評估及審計，則應要求供應商提供符合業界標準及滿足決策局／部門要求的第三方審計報告。

須留意雲端運算可指不同的服務模式，包括軟件即服務、平台即服務及基礎設施即服務的模式。每個模式的風險和保安控制不同，外判的主要考慮因素亦各異，因此保安風險評估及審計的程序亦可能不盡相同。

5.14.1 保安風險評估

- 為雲端平台系統或應用系統評估風險 [I] [O] [P]

  一如傳統應用系統，在雲端平台系統或應用系統提供正式服務前，以及進行大規模升級和變更前，應進行保安風險評估。應評估雲端平台的保安風險，並推行合適的保安控制以減低風險。亦應定期檢討保安控制的成效，以及按需要改善控制，因為隨着新技術的出現，可能會對雲端服務提供更好的保護（**附件** B 提供了一些與雲端保安相關的新興技術）。若所需的保安控制應由雲端服務供應商推行，則應獲知雲端服務供應商的保安推行細節。

- 定期進行保安風險評估 [I] [O] [P]

  保安風險評估是一項持續的活動。對於私有雲端平台，保安風險評估的頻率應該根據資訊科技保安政策而訂定；對於公共雲端平台，決策局／部門則應確保雲端服務供應商按照與決策局／部門保安政策一致，或事前共同協定的時期，定期由外聘保安審計師進行保安風險評估，例如按系統的關鍵性，每年一次或每兩年一次重新評估保安風險及控制。

5.14.2 審計

- 達成審計共識 [O] [P]

  在可行的情況下，決策局／部門宜尋求審計權。為審計及核實於服務水平協議內列明的保安控制有否推行及是否有效，決策局／部門需要提早與雲端服務供應商，就決策局／部門可對雲端服務供應商接達的程度達成共識。簽署合約前的保安控制審計將因此成為雲端平台合約生效往後的審計基準。雙方應就如何收集、儲存及分享遵行證明（例如審計記錄、活動報告、系統配置）達成共識。

  決策局／部門亦應聘用獨立審計師定期進行審計，包括滲透測試和保安漏洞評估，並提供相關的理論依據和證據，以支持有關遵行安全要求的判斷。若不能夠對雲端服務供應商進行保安審計，則應要求雲端服務供應商提供第三方審計報告。

- 保持保安審計的寬度及深度一致 [O] [P]

  若可行的話，決策局／部門及雲端服務供應商應共同互相披露或提早選擇外聘核數師。決策局／部門與雲端服務供應商的保安審核寬度及深度應保持一致。應定期收集雲端服務供應商的審計報告以作分析，確保符合所需保安要求。

- 確保雲端平台上的保安遵行 [I] [O] [P]

  應檢查有否遵照政府保安規例及政策。在採用雲端服務前，應在服務合約及服務水平協議內清晰列明加入遵照政府保安規例及政策的規定。由雲端服務供應商提交，用以作遵行檢查的資料宜包括資訊保安政策、應變計劃及測試報告、事故應變程序、保安審計報告、授權覆檢報告、職務分工圖、資訊保安意識培訓記錄、系統基準配置標準文件、配置管理計劃，以及定期覆檢結果。

- 場內保安檢查 [I] [O] [P]

  雲端服務供應商應協助決策局／部門進行場內保安審計及讓決策局／部門瞭解數據中心內現行的保安措施。審計小組應由不同方面人士組成，包括資訊科技、資訊保安、業務連續性及實體保安。決策局／部門應在檢查訪問前，要求雲端服務供應商提交業務連續性計劃、運作復原計劃、相關證書（例如 ISO[17]、信息技術基礎架構庫標準）、審計報告及測試計劃。

完

[17] ISO － 國際標準化機構

附件 A: 不同雲端平台部署情景的保安控制概覽

保安控制	[I]	[O]	[P]
4.1 雲端服務模式及資訊保安			
• 界定並了解各方的共同責任	√	√	√
5.1 管理職責			
• 依照不同管轄範圍分析對保安程序的影響		√	√
• 核實對業界保安標準的遵行		√	√
5.2 資訊科技保安政策			
• 覆檢部門保安政策	√	√	√
5.3 人力資源保安			
• 界定資源控制及資訊保安中的職務及責任	√	√	√
• 要求不可披露協議及確保適當人力資源管理		√	√
• 發出指引或通知提醒用戶	√	√	√
• 確保給予有關人員適當的保安訓練	√	√	√
5.4 資產管理			
• 透過加密保護數據	√	√	√
• 遵守有關外判數據中心的數據保護及私隱法例		√	√
• 個人資料去識別化	√	√	√
• 追蹤數據位置		√	√
• 偵側及防止未經授權的數據遷移至雲端平台		√	√
• 備存最新的資產清單	√	√	√
• 確保已達到使用壽命的電腦設備的棄置或重用設備控制是合適及得到妥善推行	√	√	√
5.5 接達控制			
• 清晰訂立邏輯控制	√	√	√
• 建立身分及接達管理架構	√	√	√
• 採用接達控制標準	√	√	√
• 要求嚴謹的認證選項	√	√	√
• 管制高權限實用程式	√	√	√
5.6 加密方法			
• 管理及保護密碼匙	√	√	√
5.7 實體及環境保安			
• 為選擇場地位置及設施分析風險		√	√
• 為外判數據中心的所有資訊科技設備及數據儲存媒體採取適當實體保護		√	√
• 有需要時劃出獨立區域作指定用途	√	√	
• 限制獨立區域的出入	√	√	
• 考慮為受控制區域訂立保安級別	√	√	
• 確保為共用相同設備架的多個應用系統採取合適接達控制	√	√	

5.8 操作保安			
5.8.1 資訊備份			
• 定期為數據備份	√	√	√
5.8.2 記錄			
• 為審計、分析和調查保存及保護記錄	√	√	√
5.8.3 配置管理及控制			
• 確保妥善執行保安程序	√	√	√
5.8.4 修補程式管理			
• 確保修補程式管理過程有足夠控制	√	√	√
5.9 通訊保安			
5.9.1 一般網絡保護			
• 於傳遞時保護數據	√	√	√
• 保護網絡上的運算資源	√	√	√
5.9.2 虛擬化的保安			
• 保持主機操作系統精簡及堅固	√	√	√
• 部署高可用性技術	√	√	√
• 為虛擬化中的每個獨立組件訂立保安要求及鞏固組件	√	√	√
• 啟用虛擬機器專屬的網絡保安功能	√	√	√
• 執行最小權限原則及工作分隔	√	√	√
• 建立安全區域分隔不同信任水平的虛擬機器	√	√	√
• 於較關鍵系統考慮使用裸機（類型I）虛擬機器管理程式	√	√	
• 分析相關保安風險	√	√	√
• 覆檢虛擬機器及應用系統的資源要求	√	√	√
• 防範兩個虛擬機器之間的未授權接達	√	√	√
• 備存資產記錄	√	√	√
• 確保軟件使用證有效及足夠	√	√	√
• 為離線虛擬機器安裝最新的保安修補程式及病毒識別碼	√	√	√
• 檢驗快照復原後的虛擬機器保安狀況	√	√	√
• 保護虛擬化影像及配置檔安	√	√	√
• 關掉不必要的通訊埠、服務及虛擬硬件	√	√	√
• 按需要地為每個虛擬機器或相關虛擬機器集群推行基於虛擬機器管理程式、基於網絡及基於主機的保護方案	√	√	√
• 記錄虛擬機器管理程式和虛擬機器上，特權帳戶的活動	√	√	√
• 小心管理虛擬機器影像及快照	√	√	√
• 安全清除虛擬機器數據	√	√	√
• 保護管理界面	√	√	√
5.10 系統購置、發展及維護			
• 在雲端應用系統上，應用安全軟件開發周期	√	√	√
• 管理及保護憑證	√	√	√
5.11 外判資訊系統的保安			

• 在決定開始使用處於外判數據中心的外判雲端服務前，分析保安風險		√	√
• 在準備外判標書時，清楚界定外判範圍的保安要求		√	√
• 制定服務水平協議及監察修改		√	√
• 確保外聘雲端服務供應商提供符合政府保安要求的保安控制		√	√
• 確保妥善解決外來威脅		√	√
• 制訂退出策略		√	√
5.12 資訊保安事故管理			
5.12.1 保安事故監察			
• 界定事故監察及通報責任		√	√
• 提供資料作事故分析		√	√
5.12.2 保安事故應變			
• 確保符合事故應變規定	√	√	√
• 覆檢雲端服務供應商往績		√	√
• 為非機構處所的雲端服務訂立事故應變管理及程序	√	√	√
• 與雲端服務供應商為事故應變進行演習	√	√	√
5.13 資訊科技保安方面的業務持續運作管理			
• 確保有效的數據備份及運作復原安排	√	√	√
• 發展業務連續性計劃	√	√	√
5.14 遵行要求			
5.14.1 保安風險評估			
• 為雲端平台系統或應用系統評估風險	√	√	√
• 定期進行保安風險評估	√	√	√
5.14.2 審計			
• 達成審計共識		√	√
• 保持保安審計的寬度及深度一致		√	√
• 確保雲端平台上的保安遵行	√	√	√
• 場內保安檢查	√	√	√

附件 B: 新興雲端保安技術

隨著雲端運算的廣泛應用、傳統保安控制可能不足以保護雲端環境中機構的資訊資產。正因為如此，保安服務供應商為了解決相關的保安問題，推出一些新的雲端運算保安措施。下面重點介紹與雲端保安相關的一些新興技術例子。

B.1 身份管理即服務（IDaaS）

隨着越來越多雲端服務的部署，用戶接達及接達記錄的管理工作變得日具挑戰。身份管理即服務（IDaaS）是一種基於雲端的服務，提供一系列針對雲端應用及客戶處所內的舊有系統的身份及接達管理功能。身份管理即服務的功能包括：

- 身份管治與管理 —這包括身份管理的能力，例如自助服務用戶配置、密碼同步
- 身份接達 —這包括用戶驗証、單一登入，以及政策執行
- 身份分析 —這包括記錄事件，以及接達報告

由於身份對平台或系統極為重要，雲端平台用戶在部署身份管理即服務時要注意以下事項：

- 身份管理即服務供應商的可靠性和誠信
- 身份管理即服務在雲端平台和網絡接達時的可用性
- 身份數據的復原能力和保護
- 對用戶身份的操作和接達控制
- 憑證管理

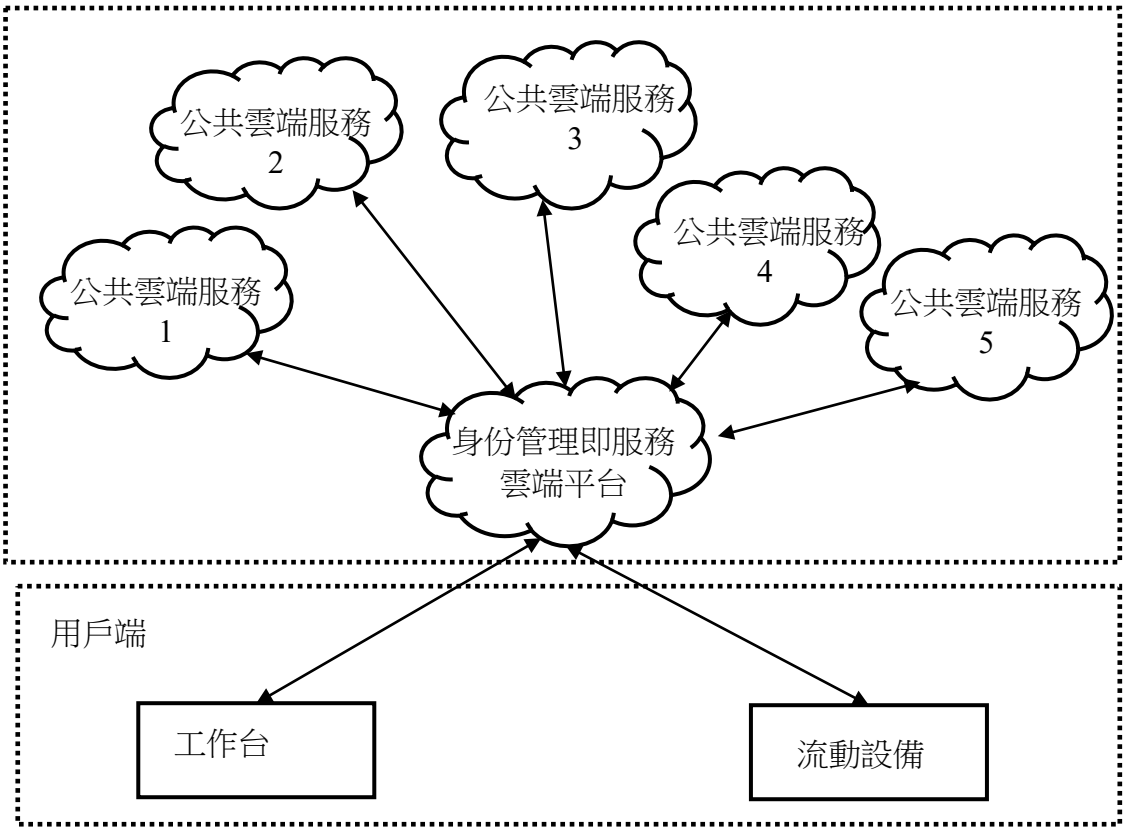

圖 B.1 身份管理即服務的使用情景

在使用這些雲端服務之前，應該進行關鍵風險分析和詳細的遵行覆檢。決策局／部門應確保在處理雲端平台的保密資料時，特別是在考慮使用身份管理即服務時，符合政府的保安要求。為了降低跨雲端平台被入侵的風險，應避免在不同雲平台之間重複使用身份。第5節 - 雲端服務的保安考慮和控制的良好作業模式也適用於身份管理即服務的雲端服務。

B.2 雲端接達保安代理（CASB）

雲端接達保安代理（CASB）作為一個控制點，可在多個雲端應用程式中確保保安政策、遵行和管治的執行。雲端接達保安代理具有以下功能：

- 雲端接達監控－提供機構的雲端服務使用情況和用戶接達的統一視圖，包括使用的設備和用戶位置
- 保安政策的落實執行－基於數據類型實施限制接達的保安政策，及監察保密數據接達或特權升級的用戶活動
- 雲端服務保護數據－提供檔案或欄位加密
- 威脅防護－防止那些尚未獲准接達的設備、用戶和應用系統版本的接達

當安裝於網絡周邊，雲端接達保安代理可用於監視雲端服務的使用情況，並可被視為額外的保安控制（參見圖B.2）。該軟件可以在機構處所、雲端平台或兩者混合。服務接達可以採取不同的方式，例如反向代理、轉發代理、API模式或混合／多模式。雲端接達保安代理可以包括在「安全接達服務前端」框架中，該框架可根據實體身份確保雲端為本網絡的安全接達，增強網絡保安，從而容許擴充安全基礎架構。由於雲端接達保安代理相對較新且仍在不斷發展，決策局／部門應在選擇合適的部署解決方案之前，根據業務需求、特性、支援、價格、與運作和基礎設施的整合等各種準則進行適當的市場研究和產品評估。

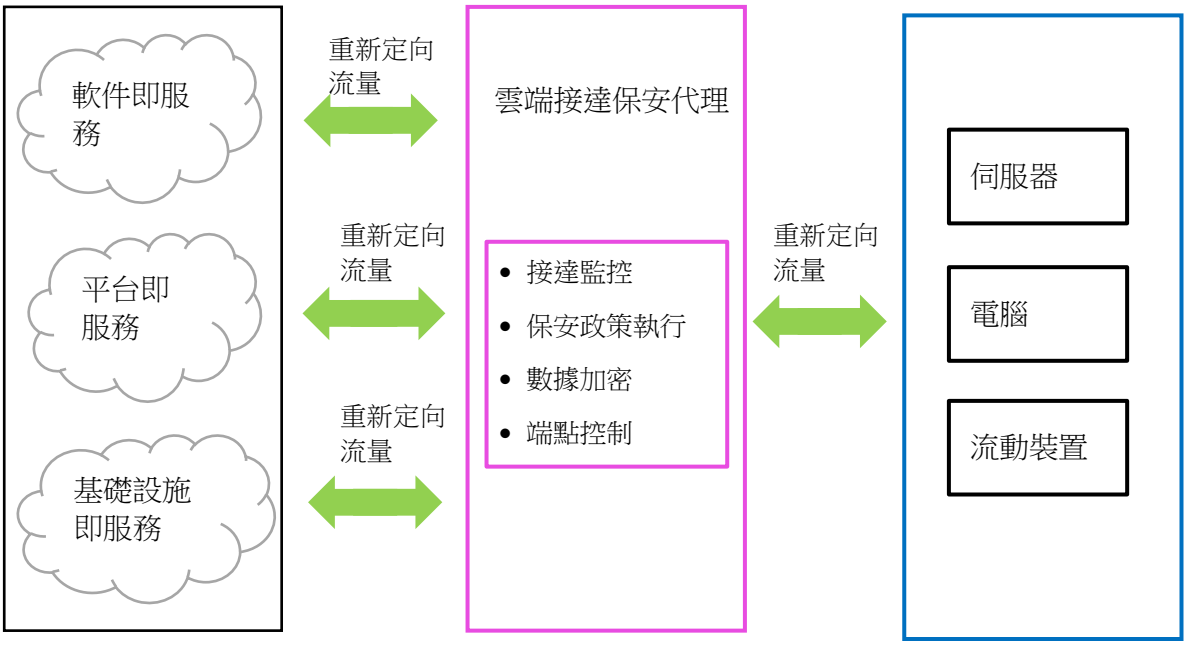

圖 B.2 透過雲端接達保安代理接達雲端服務

B.3 雲端工作負載保護平台（CWPP）

工作負載是一個通用術語，用於描述在實體伺服器、虛擬伺服器或容器[18]中執行的程式。隨著採用不同平台的雲端服務越來越多，各種工作負載也隨之被建立。因此，要保持在不同雲端平台之間各工作負載的安全水平一致，這令系統管理員的工作量和難度增加，特別是當涉及公共雲端服務時。

在公共雲端服務部署中，雲端平台用戶可能不可以像機構處所內部部署那樣實施保安控制，並且可能缺少對雲端服務的保安控制的監視。為了迎合這一需求，雲端工作負載保護平台包含一系列的軟件，用於簡化在各種雲端平台（包括機構處所內部、私有雲端平台和公共雲端平台）上部署工作負載保護的管理工作。雲端工作負載保護平台可以通過中央管理來監控混合雲端基礎設施中的保安政策，以確保執行一致的保安政策（圖B.3）。

[18]虛擬機器擁有操作系統的完整映像，而雲端容器只包含運行某個應用程式所需的相關程式、設置和存儲

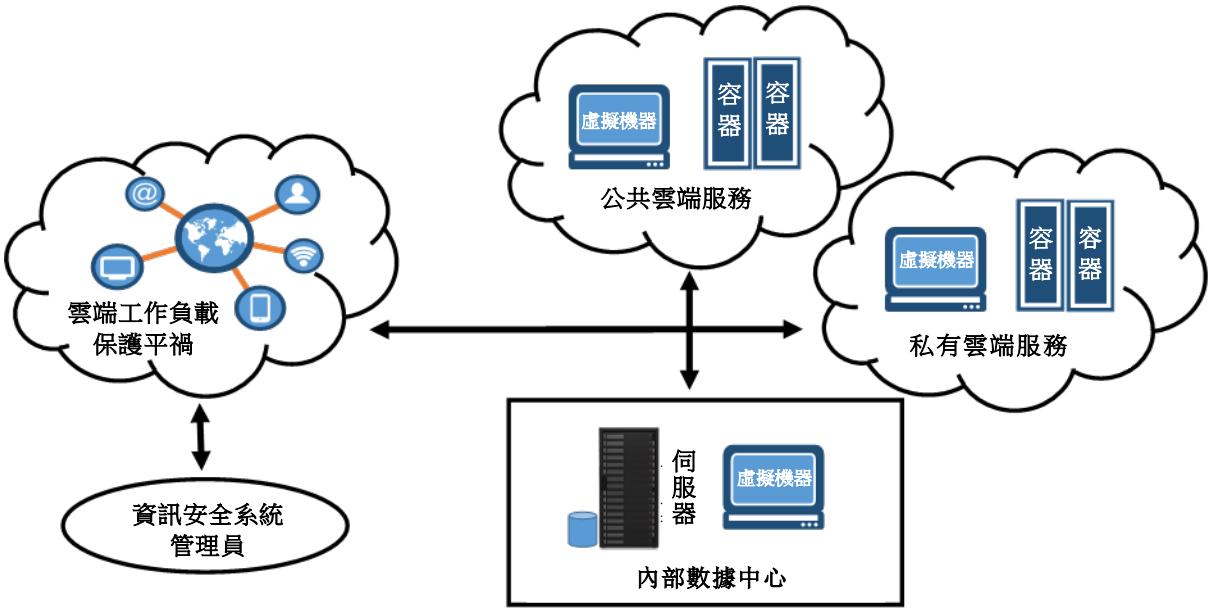

圖 B.3 雲端工作負載保護平台

雲端工作負載保護平台在混合雲端環境中提供以下工作負載的管理功能：

- 系統監視和管理
- 網絡防火牆和分隔
- 應用程式控制
- 配置和漏洞管理
- 內存記憶保護

一些雲端工作負載保護平台供應商會提供額外的保護功能，例如：

- 數據加密
- 主機入侵防禦系統 (HIPS)
- 端點保護，例如抗惡意軟件等

與雲端接達保安代理類似，雲端工作負載保護平台相對較新並且仍在不斷發展，決策局／部門應在部署前進行適當的市場研究和產品評估。尤其應該考慮不同環境中解決方案的兼容性（如伺服器和操作系統的支援、虛擬化、容器、API等）以及使用集中軟件管理各種雲端服務的風險。