政府资讯科技总监办公室

信息安全

云端运算安全

实务指南

[ISPG-SM04]

第 1.2 版

2021 年 6月

版权公告

修改记录

修改次数	修改详情	经修改页数	版本编号	日期
1	增加关于信息技术安全管理的新章节，及维持与其他实务指南有一致的参考，在第5节、第5.7节、第5.9.2节及附件B增加对新兴云端技术及服务的介绍。	整份文件	1.1	2018年7月
2	在第5节、第5.1节、第5.3节、第5.4节、第5.5节及第5.7节更新对云端服务供应商提供适当数据保护的要求；在第5.4节及附件B更新对个人资料保护的去识别化技术介绍；以及在附件B更新新兴解决方案的介绍。	15-18, 20-22, 26, 42, 44, 49	1.2	2021年6月

目录

1. 简介

本文件旨在提供指南，予负责评估使用云端运算模式以储存、处理或传递政府信息所带来安全影响的不同组别人士，如管理人员、信息技术管理员、系统拥有者及信息安全持份者。

随着云端运算急速发展，云端形态不断推陈出新，现有系统或亦因此结合演变成新的云端形式。本文件的内容大致可应用于不同云端运算技术。由于每个云端运算部署都有各自的特征，推行者应考虑及应按其环境而选择适合的作业模式。

注意：对于本文内所提及之供应商的产品或服务，本文件的作者并无作出使用的认可或暗示任何的取向。另外，本文件并非要取代政府安全规例、政策、指南和决策局 / 部门的部门信息技术安全政策。

1.1 目的

鉴于全球采用云端运算的趋势，本文件的订立旨在为决策局 / 部门提供相关的指导说明，目的如下：

- 加强决策局 / 部门对基本云端安全的理解；以及
- 协助决策局 / 部门在建立自己的私人云端平台，或外聘云端服务时，安全使用云端运算。

本文件重点介绍当采用云端运算时常见的安全考虑及业界的良好安全作业模式。

1.2 参考标准

以下的参考文件为应用本文件时必不可少的参考：

- 香港特别行政区政府《基准信息技术安全政策》[S17]
- 香港特别行政区政府《信息技术安全指南》[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 定义及惯用词

本文件将会采用《基准信息技术安全政策》和《信息技术安全指南》内所使用，以及以下的定义及惯用词。

缩写及术语	
云端服务供应商	通常收费为其他机构和／或人士，提供基于云端的平台、基础设施、应用系统或储存服务的公司。

1.4 联络方法

本文件由政府资讯科技总监办公室编制及备存。如有任何意见或建议，请寄往：

电邮： it_security@ogcio.gov.hk

Lotus Notes 电邮： IT Security Team/OGCIO/HKSARG@OGCIO

CMMP 电邮： IT Security Team/OGCIO

2. 信息安全管理

信息安全是关于安全控制和措施的规划、实施和持续提升，以保护信息资产的机密性、完整性和可用性，适用于信息的存储、处理或传输过程及其相关信息系统中。信息安全管理是一套有关规划、组织、指导、控制的原则和应用这些原则的法则，以迅速有效地管理实体、财务、人力资源和信息资源，以及确保信息资产和信息系统的安全。

信息安全管理涉及一系列需要持续监测和控制的活动。这些活动包括但不限于以下的范畴：

- 安全管理框架与组织；
- 管治、风险管理和遵行要求；
- 安全操作；
- 安全事件和事故管理；
- 安全意识培训和能力建立；以及
- 态势感知和信息共享。

安全管理框架与组织

决策局 / 部门须根据业务需要和政府安全要求，制定和实施部门信息安全政策、标准、指南和程序。

决策局 / 部门亦须界定信息安全的组织架构，并为有关各方就安全责任提供清晰的定义和适当的分配。

管治、风险管理和遵行要求

决策局 / 部门须采用风险为本的方法，以一致及有效的方式识别信息系统的安全风险、订定应对风险的缓急次序和应对有关风险。

决策局 / 部门须定期和在必要时对信息系统和生产应用系统进行安全风险评估，以识别与安全漏洞相关的风险和后果，并为建立具成本效益的安全计划和实施适当的安全保护和保障措施提供依据。

决策局 / 部门亦须定期对信息系统进行安全审计，以确保当前的安全措施符合部门信息安全政策、标准和其他合约或法律上的要求。

安全操作

为保护信息资产和信息系统，决策局 / 部门应根据业务需要实施全面的安全措施，涵盖业务上不同的技术领域，并在日常操作中采取「预防、侦测、应急和复原」原则。

- 预防措施避免或阻止不良事件的发生；
- 侦测措施识别不良事件的发生；
- 应急措施是指在发生不良事件或事故时，采取协调行动来遏制损害；以及
- 复原措施是将信息系统的机密性、完整性和可用性恢复到预期状态。

安全事件和事故管理

在现实环境中，由于存在不可预见并致服务中断的事件，故此安全事故仍可能会发生。若安全事件危及业务的连续性或引起数据安全风险，决策局 / 部门须启动其常规安全事故管理计划，以实时识别、管理、记录和分析安全威胁、攻击或事故。决策局 / 部门亦应准备与有关各方适当地沟通，透过分享对有关安全风险的应急以消除不信任或不必要的猜测。当制定安全事故管理计划时，决策局 / 部门应规划和准备适当的资源，并制订相关程序，以配合必要的跟进调查。

安全意识培训和能力建立

因为信息安全是每个人的责任，所以决策局 / 部门应不断提升机构内的信息安全意识，透过培训及教育，确保有关各方了解安全风险，遵守安全规定和要求，并采取信息安全的良好作业模式。

态势感知和信息共享

因应网络威胁形势不断变化，决策局 / 部门亦应不断关注由安全行业和政府计算机安全事故协调中心发布的现时安全漏洞讯息、威胁警报和重要通知。应将即将或已经发生具威胁的安全警报传达及分享给决策局 / 部门内的负责同事，以便采取及时的应对措施来缓解风险。

决策局 / 部门可以利用网络风险信息共享平台接收和分享安全事务、安全漏洞和网络威胁情报的讯息。

3. 云端运算安全的介绍

3.1 云端运算

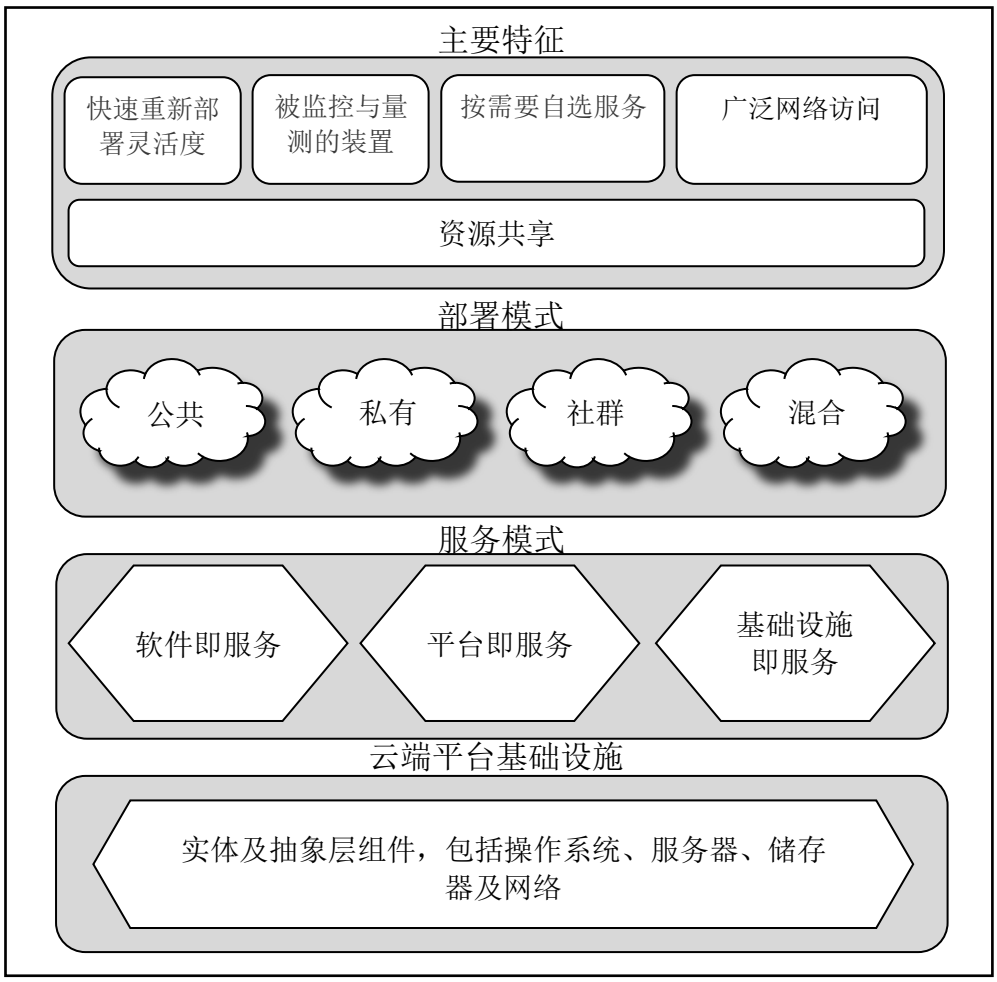

图 3.1 云端模式

云端运算模式能让用户随时随地、便捷地、按需要地透过网络访问一系列可配置的计算机运算资源（例如网络、服务器、储存器、应用系统及服务），这些资源只需透过少量的管理工作或与服务供应商少量的互动，便能迅速地准备妥当及发布。如上图3.1 所示，云端平台基础设施下的云端运算大致上可以分为三个服务模式及四个部署模式[1]。

[1] "The NIST Definition of Cloud Computing", SP 800-145, 美国国家标准技术研究所(NIST).

3.2 云端平台的基础设施

云端平台的基础设施由软件及硬件所组成，用以提供云端计算的重要特性，包括资源共享、快速重新部署的灵活度、可监控与量测的服务、按需要的自助服务，以及宽带网络访问。云端平台的基础设施可被视为同时包含物理层及抽象层。物理层由支持云端服务的硬件资源组成，一般包括服务器、储存器及网络组件；抽象层由软件所组成，部署在物理层上，这也是云端平台的重要特征。在概念上，可以理解为抽象层设于物理层之上。

3.3 云端服务的模式

云端服务有以下三种典型的模式：

- 基础设施即服务：云端服务供应商向决策局 / 部门提供一项包括基本运算资源 / 设备（储存器、硬件、服务器及网络组件）的服务，决策局 / 部门仍控制所安装的操作系统及应用系统；
- 平台即服务：云端服务供应商向决策局 / 部门提供一项包括基本运算资源 / 设备，及虚拟环境的服务，然后由决策局 / 部门于供应商提供的环境或云端平台的基础设施上，部署本身的应用系统；以及
- 软件即服务：云端服务供应商向决策局 / 部门提供一项包括基础设施、平台（或虚拟环境），以及软件的服务。决策局 / 部门的用户连接到这个环境，并经定制后运行信息技术应用系统。

3.4 云端平台部署的模式

云端的部署有以下四种典型的模式：

- 公共云端平台：云端平台基础设施开放予公众使用。基础设施支持多租户特性，并可以由第三方拥有、管理及运作（或这三种方式的任何组合）。云端部署于云端服务供应商处所；
- 私有云端平台：云端平台基础设施只供由数个决策局 / 部门组成的单一机构独立使用。基础设施可以由该机构（即内部私有云端平台）或第三方（即外包私有云端平台）拥有、管理及运作（或这三种方式的任何组合）。云端部署于机构自己的处所或供应商处所；
- 社群云端平台：云端平台基础设施只供来自有共同目标、兴趣及 / 或关注的机构的特定用户羣组专用。基础设施可以由用户羣组内的一个或多个组织拥有、管理及运作（或这三种方式的任何组合）。云端部署于机构自己的处所或供应商处所；以及
- 混合云端平台：云端平台基础设施由两个或多个不同云端平台基础设施（私有、社群或公共）组成，并可由不同云端服务供应商提供。这种模式令数据及应用系统具有可移植性。

3.5 四种部署模式的比较

四种部署模式在信息安全不同层面的比较如下：

层面	公共云端平台	私有云端平台	社群云端平台	混合云端平台
服务提供	透过互联网提供服务	透过（虚拟）私有网络提供服务	透过（虚拟）私有网络提供服务	混合使用互联网及私有网络
服务水平协议	由云端服务供应商订立服务水平协议	由机构订立服务水平协议	由参与机构共同订立服务水平协议	混合不同服务水平协议
可使用情况	生产力、业务及社交媒体应用系统，及其他云端信息技术服务	寄存于专为政府使用而设的基础设施内的政府内部服务	向政府与拥有相同业务需要的非政府组织所形成的社群提供的服务	因为私有云端平台不能满足容量需要，而连接到公共云端服务的私有云端应用系统

是否采用云端运算是一个业务上的决定，除安全因素外，决定过程亦应考虑如转移成本、生命周期成本及应用系统的准备程度等有关因素。除此以外，决策局／部门应评估数据的敏感程度，选择适当的部署模式处理及储存数据。决策局／部门须确保无论用何种部署模式，保密数据都须得到保护，并符合所有政府的安全要求及满足业务的需要。决策局／部门亦应透过对可能采用的云端平台作全面安全评核，识别云端服务供应商在信息安全的差距，并采取有效的方法以减低对数据造成的风险。

4. 云端平台安全概览

一如任何新的运算模型或技术，云端运算亦可能构成新的安全风险。在考虑采用云端运算时，应使用风险为本的方法。重要的是，决策局／部门必须考虑各种安全范畴，例如数据保密性、完整性、额外设置、复原能力、管辖权等。另外，亦需要知道何种数据会被考虑转移至云端平台、这些数据对风险的承受力，以及选择的服务和部署模式。云端服务用户或其潜在用户必须明白云端运算当中的挑战及风险，让自己能为缓解或控制这些挑战及风险而作出更好准备。应就评估得出的风险水平及数据价值，部署适当的安全控制及措施。

4.1 云端服务模式及信息安全

作为一般原则，在从软件即服务移至平台即服务，再移至基础设施即服务的过程中，客户机构可以对更多资源有更大的安全控制。图4.1展示在云端平台上，不同负责方的控制范围：

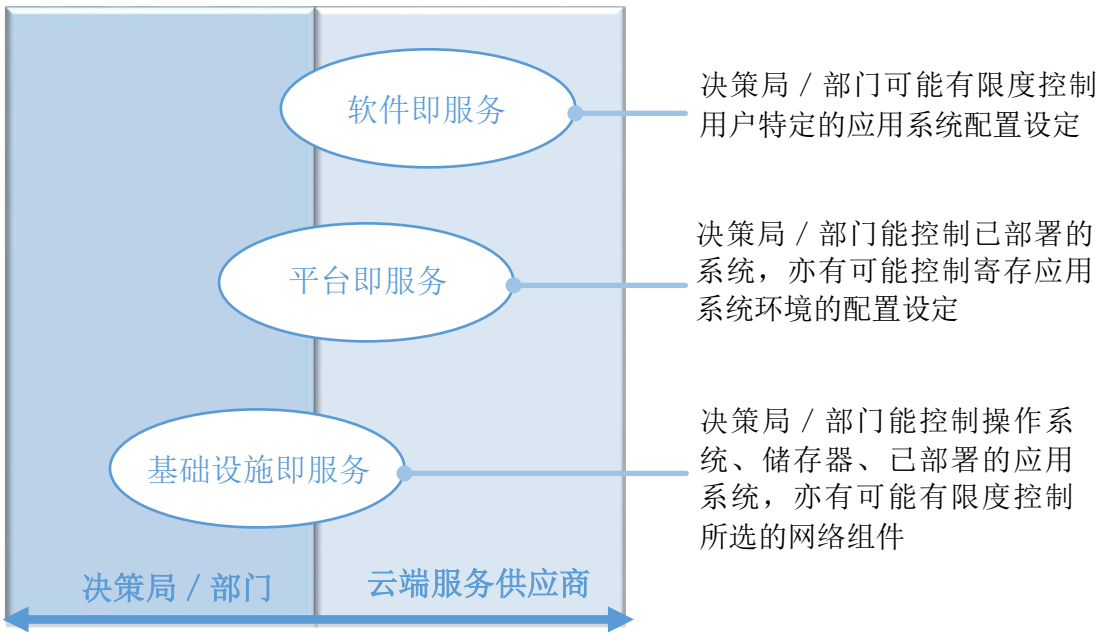

图 4.1 决策局／部门及云端服务供应商在不同云端服务模式下的控制程度／责任

软件即服务一般由客户端使用浏览器经互联网访问，而客户不会管理或控制下层的云端平台及基础设施。于软件即服务模式下，客户机构通常对关键安全能力（例如数据加密或遵行审计）持有甚少的直接控制权。

平台即服务于中层提供云端设施。透过减少一些给予客户的现成功能，平台即服务一般比软件即服务有更大的扩充能力。客户机构通常对平台有一定的控制权，并有更大的弹性来为上层的资源施行附加的安全措施。

基础设施即服务要求客户机构推行本身的应用系统，以及在基础设施即服务云端服务供应商所提供的基础设施之上设立自己的操作平台。客户机构对操作系统、已部署的应用系统，以及对储存器、网络和运算资源的定制的设定，仍保留安全管理及控制的弹性。

无论服务属于何种云端服务模式，云端服务供应商仍要负责控制及保护下层的基础设施组件，如处理、储存器、网络及其他基本运算资源，以确保基本服务的可用性及安全。

4.2 云端平台推行情景及信息安全

客户机构的安全控制程度在公共云端平台与私有云端平台有所不同。公共云端平台是提供给一般公众，并且由多个租户共同使用，而私有云端平台是由单一机构专用的。私有云端平台可以让机构有更严谨的访问控制，从而更好地控制网络基础架构和安全策略。因此，公共云端平台有可能面临更多安全风险，而私有云端平台更能抵御安全威胁。云端服务具有不同的推行情景，它可由内部提供或是外包，可部署于机构处所或非机构处所。这些推行情景对云端环境的安全尤关重要。

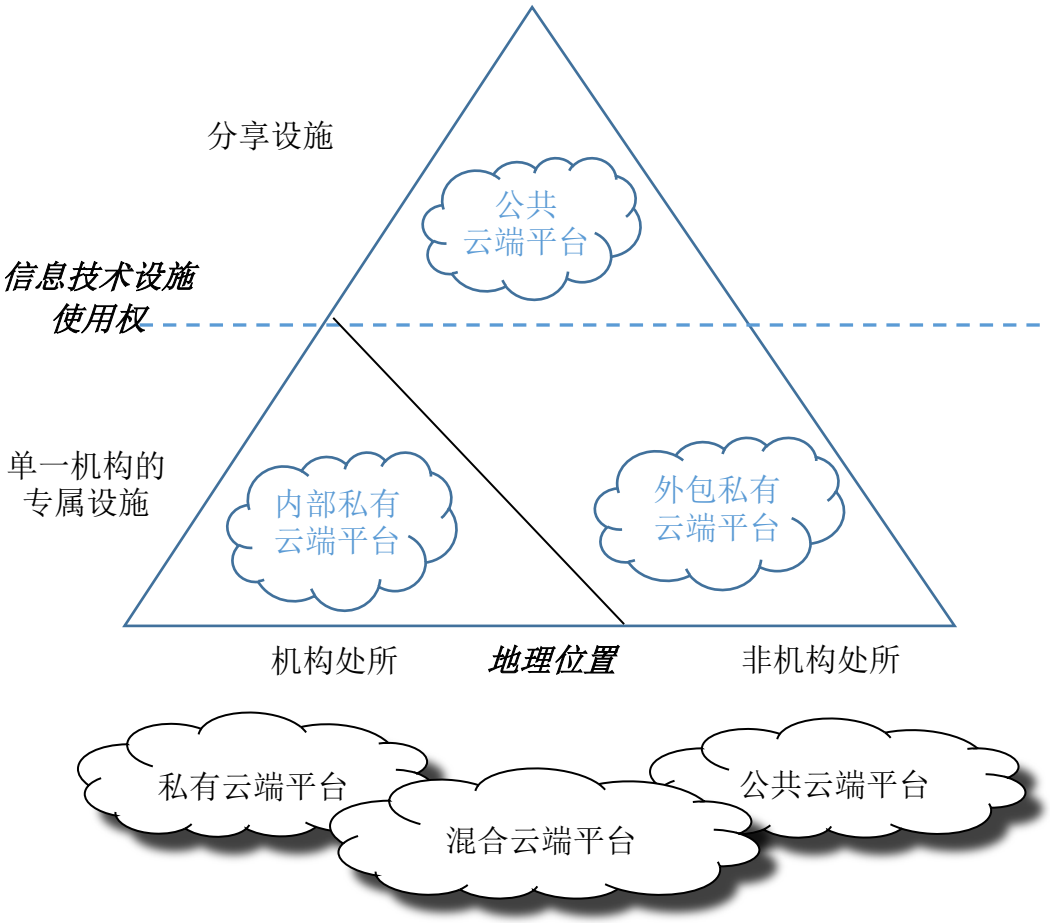

图 4.2 云端平台推行情景

为更深入讨论在政府内推行云端平台的安全考虑事项及控制，本文将会参考图4.2中的四种情景：

- 「内部私有云端平台情景」由政府拥有及在政府处所的数据中心运作。
- 「外包私有云端平台情景」包括给政府专用的设施，并由外聘云端服务供应商于非机构处所的数据中心运作，例如政府云端平台（ GovCloud）。
- 「公共云端平台情景」 由外聘云端服务供应商提供服务给公众使用。
- 「混合云端平台情景」由两个或以上的云端平台情景（公共或私有）组成。

4.2.1 内部私有云端平台情景

内部私有云端平台寄存于机构处所内，并由机构内部员工管理。由于无须或极少依赖外聘云端服务供应商提供云端服务，部分非技术性安全问题，如外包要求、数据位置及服务终止（将在下一节讨论），未必适用于该推行情景。因此，内部私有云端平台的推行者应参照传统安全环境的安全政策及指南，因为相关的安全要求依然适用。

4.2.2 外包私有云端平台情景

外包私有云端平台的寄存服务、基础设施、运算资产如数据及应用系统，以及运作和管理均外包予云端服务供应商，以达至较高的成本效益或运作效率。相比公共云端平台，外包私有云端平台有额外的好处，包括能从云端服务供应商处得到专属的资源及较好的响应。

客户机构应要求云端服务供应商告知确实操作云端服务的人员资料，并于人事变动时，向客户机构证明取代的操作人员拥有同样或较高资历。客户组识亦应要求云端服务供应商执行合适的安全控制，以确保云端服务的人员及管理质素。由于数据中心处于非机构处所，实体访问控制将由云端服务供应商直接管辖。服务买家经常误解在外包时，云端服务供应商会负起所有持续的管理责任，但事实是服务买家仍有责任监察云端服务供应商，否则欠缺管制，会削弱信息技术安全的安排。

4.2.3 公共云端平台情景

公共云端平台的基础设施及其所包括的运算资源都透过互联网开放予一般公众。由于平台是由出售云端服务的云端服务供应商所拥有，所以顾名思义，它不属于客户机构。云端服务和数据的安全不是由客户机构完全管理。因此，有必要明白云端服务供应商提供的公共云端运算环境，以确保机构的安全及私隐要求得以满足。

由云端服务供应商提出的标准服务水平协议记录双方对服务、优先次序、责任、保证及保用的共同理解。服务水平协议可能只有有限或甚至没有任何商议空间。客户组识应留意在违反服务水平协议时，对安全的影响及相关罚则。

4.2.4 混合云端平台情景

混合云端平台情景是在上述三种推行情景之上尚存的另一种可行推行情景。在第3.4节所提及，混合云端基础设施由两个或以上不同的云端基础设施（例如私有及公共）组成。因此，混合云端平台推行情景是由其他三种推行情景（内部私有云端平台、外包私有云端平台及公共云端平台情景）组成。

云端服务供应商所提供，从云端环境连接到客户机构网络的连接不应削弱现有的安全水平。客户机构应在取得云端服务时评估当中的安全风险，并应用「若双方安全水平不同，则双方都要采用较强的安全」的原则。

图 4.3 描述理论化混合云端平台推行情景。

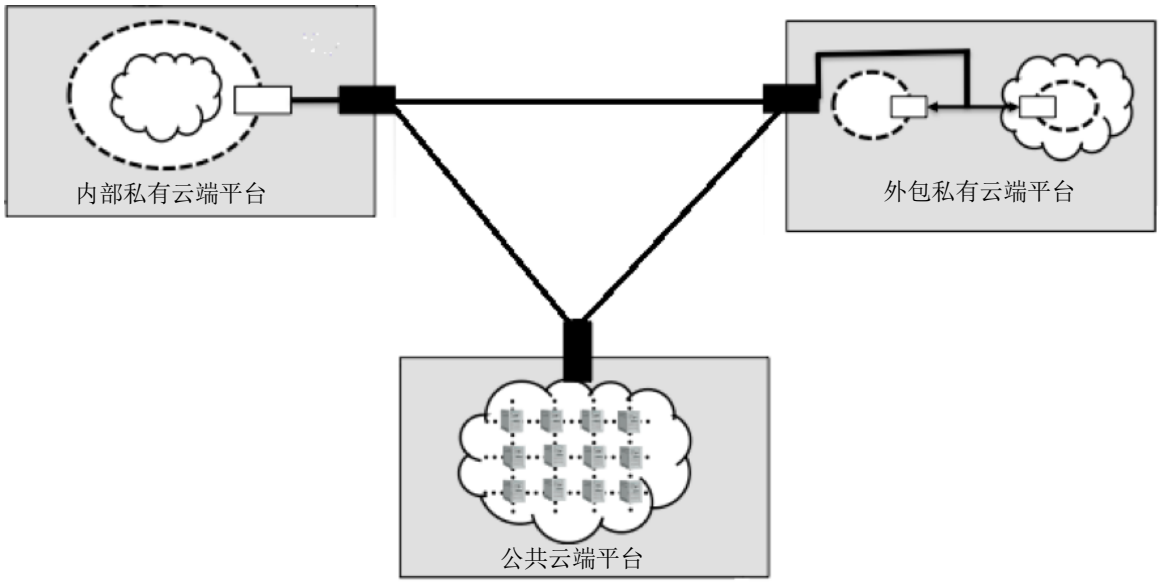

图 4.3 混合云端平台情景

「云爆发」是混合云端平台情景经常采用的方式。「云爆发」是指企业利用内部私有云端平台进行基本操作，但在平台需求高峰时期，则可选择访问一个或多个的外包私有云端平台，以平衡平台的负载量。

5. 云端服务的安全考虑及控制

在明白云端运算及云端安全的基本概念后，本节将探讨安全控制。云端运算可视为向企业提供以信息技术为本的服务新方法，而非一种独立的新科技。当然，部分技术，如虚拟化，在云端运算上具有显着的重要性。由于云端运算大部分采用与传统信息技术环境相类似的管理工具、操作系统、数据库、服务器平台、网络基建、网络规约及储存器组等，云端平台的安全控制亦因此与传统信息技术环境大致相似。故此，在政府的安全文件包括《基准信息技术安全政策》[S17]及《信息技术安全指南》[G3]内的安全控制仍然适用。可是，根据所采用云端服务及部署模式的特征，以及部署云端服务所使用的技术，云端环境的某些风险将变得更为显着，而在传统信息技术环境未遇过的新风险亦可能随之出现。以下的部分将会集中在安全范畴，描述云端安全的挑战及提供处理这些风险的安全作业实务。

- 管理职责
- 信息技术安全政策
- 人力资源安全
- 资产管理
- 访问控制
- 加密方法
- 实体及环境安全
- 操作安全
- 通讯安全
- 系统购置、发展及维护
- 外包信息系统的安全
- 安全事故管理
- 信息技术安全方面的业务持续运作管理
- 遵行要求

在每个安全考虑事项及控制的说明旁边，都附有一个标签，标示该控制最适合应用于哪种部署情景。对于混合云端平台，应根据当中的组合考虑其安全控制。若平台包括公共及内部私有云端平台，则应保留该两种部署情景的安全考虑事项及控制。标签只标示一般关联，欠缺某种部署情景标签并不代表该控制与这些部署情景完全无关。

决策局／部门在考虑选用云端服务时，应采取风险为本的方法、评估业务需要及数据的保密类别，并确保云端服务供应商的安全措施、服务水平及管理要求符合政府的数据保密类别及业务要求，并遵行政府的安全要求。由于不同的云端服务供应商的安全等级有所不同，各决策局／部门应全面审视和仔细考虑云端服务供应商处理数据的方式。以下有关云端的安全作业模式适用于一般的云端部署方案。随着云端技术的发展，云端服务供应商会在市场提供新的云端解决方案和服务。决策局／部门应进行内部研究及评估，识别潜在的风险，并采取相应的良好作业模式和合适的部署模式。由于每种安装都可能有各自指定的部署情景，推行者应自行判断并选出最适合的安全控制。

决策局 / 部门应确保云端服务供应商在基础设施的设计、开发、部署和配置过程中，对政府数据（尤其是涉及敏感数据）提供适当保护，以便把政府的敏感或保密数据与其他客户环境适当隔离。

各标签的意思如下：

「安全考虑事项及控制名称」[I] [O] [P]

[I] - 「内部私有云端平台」
[O] - 「外包私有云端平台」
[P] - 「公共云端平台」

附件A概括在不同范畴内，云端平台推行的安全控制，以方便决策局 / 部门参考。

根据《基准信息技术安全政策》第17.3节公共云端服务，机密或以上保密类别的资料不得利用公共云端服务储存或处理，而限阅类别的资料必须遵照相关的公共云端安全架构或政府资讯科技总监办公室所发布的指南在公共云端服务储存或处理。

5.1 管理职责

机构所属之数据的安全管理和控制最终须由该机构的用户负责。应采用风险为本方法，于机构的信息系统策略计划及 / 或机构信息技术计划中加入云端运算策略，并应采用及严格推行合适的安全管理作业实务及控制。要操作和维持一个安全的云端运算方案需要严谨的管理作业实务，而良好的作业实务牵涉监管机构信息系统资产，以及推行为建立和保存信息系统资源机密性、完整性及可用性而制订的政策、指南及程序。

因为在云端环境内，数据会在分布式云端储存器之间转移，这对维持可审计的数据位置记录及确定数据在不同管辖范围内可得到足够的保护并不容易。此外，云端服务供应商的服务牵涉很多崭新科技，而服务运作亦有赖庞大的硬件基建及复杂的管理工作。若云端服务供应商未能正确配置及处理其中任何部分，系统将可能出现故障或者导致安全事故。对于外包私有或公共云端平台，「云锁定」是另一个挑战。「云锁定」是指由于转用另一云端服务供应商将要牵涉到的复杂性，导致客户机构只可依靠现有的云端服务供应商。这情况可能令业务难以转移到新的云端服务供应商。

- 依照不同管辖范围分析对安全程序的影响 [O] [P]

  数据在云端平台上，可以在不同实体位置及管辖范围之间转移及储存。所有合约应明确说明规管法律和司法管辖权条款。决策局 / 部门应注意保存在另一个司法管辖区的数据受该司法管辖区的法律约束。此外，不论数据储存在甚么地方，某些云端服务供应商可能受其注册所在的司法管辖区的法律约束。即使合约或服务水平协议规定了数据访问的限制，但仍不能凌

驾该司法管辖区的法律。因此，决策局／部门应考虑到自身的权利可能在云端服务供应商的管辖范围内受影响。而由于不同的法律和监管遵行要求，将数据及应用系统移至云端服务亦可能对安全程序带来影响。决策局／部门须根据储存或处理数据的性质评估相关安排的风险。应详细分析凡此的潜在影响，并制订相关程序。如有必要，应就合约安排寻求法律意见，以确保敏感数据得到充分保护，免遭不自主披露。亦应考虑加强安全措施，以弥补决策局／部门未能直接控制的范围。受影响的程序可能包括事故报告、活动记录、数据保存及应用系统测试。

- 核实对业界安全标准的遵行 [O] [P]

  安全认证是对外聘云端服务供应商安全管理、成熟程度及质素保证的证明。应检查从而明了云端服务对国际认可业界安全标准的遵从程度，例如ISO 27001（信息安全管理）及ISO 27017（云端服务之信息安全控制实务守则），并确保既满足业务需要，又遵从政府的安全要求。由云安全联盟制订的共识评估倡议问卷提供了一系列评核云端服务供应商的参考问题。应要求外部云端服务供应商出示有关合格证明书及报告以作核实。

5.2 信息技术安全政策

- 覆检部门安全政策 [I] [O] [P]

  应覆检部门安全政策，并作出所需调整，以保障业务应用系统在云端环境中，在部署安全控制以保护数据时仍然有效。调整范围可以包括全新或经修订而又针对云端相关范畴（如多租户特性、数据位置、虚拟化，以及云端服务的安全使用等）的安全要求及控制。

5.3 人力资源安全

- 界定资源控制及信息安全中的职务及责任 [I] [O] [P]

  应清晰界定及记录（例如服务水平协议）支持云端服务运作及负责云端服务信息安全人员（包括但不仅限于决策局／部门和云端服务供应商）的职务及责任，特别是外包的多租户云端环境数据中心。决策局／部门须要求云端服务供应商确保负责处理包含政府敏感或保密数据的外包信息系统的员工和承包商，适合担任该职务。应要求云端服务供应商清楚分隔工作职责，例如同一人不应同时担当系统及安全管理工作。须严格执行「有需要知道」原则，而且应备存负责监管机构的最新联络资料。

- 要求不可披露协议及确保适当人力资源管理 [O] [P]

  在合适情况下，云端服务供应商的人员及其分判商应同意及签署不可披露协议。决策局／部门亦可透过合约形式（如云服务合约）以确保云端服务供应商的人员及其分判商履行保密责任。除非获得授权，否则云端服务供应商须承诺不会向任何第三方传送或披露敏感或保密数据。如第三方要求提供有关数据，而该等要求不能直接拒绝，则云端服务供应商须立即通知决策局／部门，并将有关要求转交他们处理。甄选云端服务供应商时，应考虑供应商向所属而又拥有高访问权限的人员所作的背景审查程序，以及清晰的终止雇用过程和程序。背景审查宜按需要地包括相关人士过往的教育履历、工作及犯罪纪录。终止雇用程序宜要求相关人员归还所有资产，尤其是与其工作有关的保密数据、钥匙及权标，亦必须删除所有有关的访问权限。

- 发出指南或通知以提醒用户 [I] [O] [P]

  应定期发出针对个别云端应用系统的指南或通知，以确保云端服务终端用户全面留意数据的敏感程度，并对潜在的安全威胁保持警觉，使用户能于数据生命周期中采取适当行动，例如在云端系统删除不再使用的数据。

- 确保给予有关人员适当的安全训练 [I] [O] [P]

  应定期为内部及外部人员，包括云端服务供应商的分判商的员工，提供信息安全意识培训，以确保他们对安全保持警觉及理解安全要求（例如现行政府信息技术安全要求），注意信息安全风险和事故应急处理程序，以及明白不遵守云端服务供应商制定的信息技术安全规定时须承担的责任和后果。负责安全管理及操作的人员宜持有国际、本地或业界认可的知名专业资历，例如 CCSK[2]、CCSP[3]、 CISM[4]、CISP[5]、CISSP[6]、ITIL[7]或同等程度。

5.4 资产管理

非机构处所、外包数据中心、多租户特性、互联网的使用及其他许多云端平台特性，再加上透过实体或网络连接以未获授权的方式来访问敏感数据，都造成安全风险。数据的机密性可能因为云端网络供应商对保护客户的数据缺乏承担而蒙受风险，进而令客户应用系统及数据曝露于各种来自互联网的威胁中。此外，在预期以外的服务中止情况下，例如公司合并、云端服务供应商破产、服

[2] CCSK －国际云端安全证书
[3] CCSP －云端资安专家认证
[4] CISM － 国际信息安全经理人认证
[5] CISP － 注册信息安全专业人员
[6] CISSP －信息安全系统专家认证
[7] ITIL － 信息技术基础架构库

务关闭及任何预期以外的事件，用户机构可能难以或甚至不可能从外聘云端服务供应商取回数据。

- 透过加密保护数据 [I] [O] [P] [8]

  数据加密能增强数据的机密性。决策局／部门应确认云端服务所提供的加密功能能够符合加密控制使用的加密政策。保密数据无论在静止或传递中，都必须根据政府安全要求和业务需要采用严谨的加密方式以作保护。为避免受专有算法所捆绑，应使用开放和可靠的加密算法。而加密匙亦应得到适当的保护和管理（参考第 5.6 节加密方法）。

- 遵守有关外包数据中心的数据保护及私隐法例 [O] [P]

  须遵守数据保护和私隐法规。为保障个人私隐而又位于香港境内的个人资料，须遵守《个人资料（私隐）条例》（第 486 章），特别是保障资料第四原则（个人资料的安全）。

  为追求更高成本效益，有些外包数据中心是设置于海外。跨境储存于海外数据中心，或与海外数据中心作转移的数据，因跨境的原因，此类数据中心可能受到当地法例规管，因此需要小心考虑采用海外外包服务。

  《个人资料（私隐）条例》（第 486 章）第 33 条虽然尚未颁布，但应在合适情况下参考该章节。第 33 条规管个人资料从香港转移至其他缺乏保护调制解调器制的地方，除非符合条例列明的例外情况。个人资料私隐专员公署已发表《将个人资料移转至香港以外地方数据概览》，提供相关参考数据。决策局／部门须确保云端服务供应商会在转移数据离开香港边境前得到决策局／部门的批准。

- 个人资料去识别化 [I] [O] [P]

  考虑将信息系统的数据（包括收集、处理、存储、归档及披露数据当事人的数据）去识别化，藉此加强数据保护。数据去识别化是指用于替换原始数据集的算法和过程，可在不影响业务目的的情况下，防止经处理的结果泄露数据当事人的身份。

  除为了保护数据外，另一个实施个人资料去识别化的原因是政策合规。显而易见，法规和私隐框架均着重对个人私隐的保护，并要求实施不同程度的数据去识别化 [9,10]，以便更妥善保护个人数据。

[8] 虽然没有针对非保密数据加密的规定，但为更好地保障数据私隐，决策局／部门宜在使用公共云端服务时，使用加密保护非保密数据。

[9] CT.DP-P2, NIST Privacy Framework v1.0 规定「对数据进行处理以限制个人身份的识别（例如去识别化的私隐技术、标记化）。」

[10]《通用数据保障条例》Recital 28 规定「对个人数据应用假匿名可以降低有关资料当事人的风险，并帮助管制者和处理者履行其数据保护的责任。」

去识别化并没有一个划一的做法可遵从。视乎获取个人数据的数量、应用程序的敏感度，以及涉及个人私隐的事故对政府声誉的影响等因素而定，保护措施可从「假匿名」[11]开始扩展到「匿名化」[12]，以作全面保护。技术措施可考虑使用一般化 [13]、随机化 [14]、标记化 [15]及合成数据 [16]等。

风险为本的方法有助确定所需的去识别化程度。私隐影响评估等评估工具如有助确保遵行并找出未处理的残留风险。在设计系统时，须尽可能纳入「贯彻私隐设计」的概念。

- 追踪数据位置 [O] [P]

  大多云端平台用户选择私有云端方案而非公共云端方案的其中一个原因是数据位置。云端服务供应商亦应提供数据地图以记录提供数据在数据中心间之流动，让客户明白数据在静止、传递时，以及备份的位置。亦应要求云端服务供应商作出承诺，以确保当涉及敏感数据（特别是个人资料）时，数据不会转移到其它地区。

- 侦侧及防止数据迁移至云端平台 [O] [P]

  除了传统的数据安全控制（如访问控制或加密方法）外，决策局 / 部门应避免政府数据，尤其保密数据，在未得到许可前移到云端平台。决策局 / 部门可使用数据库活动监察工具与档案活动监察工具以监察有否大量的内部数据遭迁移；或使用网址过滤方法与数据遗失保护工具以监察数据有否移至云端平台。

- 备存最新的资产清单 [I] [O] [P]

  资产包括所有在云端环境内的软件及硬件元素，而决策局 / 部门的资产种类则因云端服务模式而有所不同。决策局 / 部门须订立及备存一份云端环境内的最新资产清单。资产应包括以下：

  (i) 业务信息
  (ii) 法律 / 合约文件（例如公共域名注册和相关互联网规约地址、数据储存的实体位置等）
  (iii) 虚拟设备

[11]数据假匿名是以一个或多个人工标识符（即假名）取代数据记录中的可识别个人资料的方法。假名令个人资料不易从数据记录中识别，但亦可用作数据分析和数据处理。
[12]数据匿名化是将数据转化成不能识别个人身份的一种方法。
[13]数据一般化降低数据的精确度，同时在记录层面保留数据真实性。通过减少数据集的所选属性或一组相关属性内包含的数据粒度以完成操作。
[14]数据随机化增加归档数据的噪音。它不能在记录层面保留数据真实性，但会降低单选标识属性的风险。一般来说，数值会被修改，以使它们的新数值以随机方式与其真实数值有差别。
[15]数据标记化以非敏感的数据元素取代敏感的数据元素。这种没有外在意思的非敏感数据元素通常被称为标记。该标记能随后找出敏感数据。
[16]合成数据生成具有某些统计特征的人工数据以作为目标数据。合成数据集不包含从现有数据主体收集或与之相关的任何数据，但对于预期目的而言看起来是真实的。

(iv) 虚拟储存器
(v) 软件

- 确保计算机设备的弃置或重用控制是合适及得到妥善推行 [I] [O] [P]

  因为有些多租户环境（如公共云端服务）难以支持安全销毁数据，所以应加倍留意弃置或重用计算机设备（如硬盘及备份媒体）前定位数据及安全删除调制解调器制的完整性及效用。在甄选外聘云端服务供应商时，在对存有保密数据的计算机设备于有关服务期满或终止时或政府提出要求时弃置或重用的要求中，应加入安全销毁数据作为其中一个甄选的准则。云端服务供应商须订立在其所有平台上安全删除政府数据的程序，并在数据删除后以书面确认。亦应定期从云端服务供应商取得相关的安全审计报告作分析，以确保符合所需的安全要求。

5.5 访问控制

不同于私人云端平台般，可由客户控制网络及授权人士使用该网络，公共云端平台的客户机构欠缺这一道防线。公共云端平台的客户机构未必能够知道本身的数据曾否遭他人访问，包括管理数据的人士及在系统上的其他用户。在采购和部署云端服务之前，应该充分理解用以监控和防范的未授权访问（特别是云端服务供应商所提供的特权账户）的安全控制。并应该建立机制，在特权用户被拒绝访问的情况下，容许恢复特权用户的访问。

由于云端平台多租户的环境，存在第三方可透过云端平台网络访问共同信息储存服务的可能，导致数据外泄的风险。如果欠缺更细致的数据访问控制，由未授权人士泄露敏感数据的相关风险将会提高。

例如，预期以外的软件错误或人为过失混淆了用户权限，可能导致其他同平台的不明租户有意或无意地访问客户数据。另外，若云端应用系统存有与企业不同的一套用户身分，用户权限被解除时，由企业用户目录更新到云端应用系统之间将会出现时间差。这时间差可能让未授权人士在修改生效前访问敏感数据。

在私有云端环境内，用户机构能对安全措施，例如数据加密、密码匙管理及数据访问控制等，有更佳控制及保证；亦能严格限制机构以外人士访问资料。

决策局 / 部门应推行密码匙管理程序，以便涉及敏感或保密数据时，密码匙不会与云端服务供应商共享。简而言之，在包含敏感或保密数据的公共云端环境进行数据储存加密时，决策局 / 部门应采用自己的密码匙管理或单独及独特的密码匙管理服务。

- 清晰订立逻辑控制 [I] [O] [P]

  云端环境的运作可能牵涉不同的单位，包括操作小组、应用系统支持小组、基本设施支持小组及数据中心维修小组，而授权人士亦可能是内部或由云端服务供应商或其分判商聘用。由于未获授权访问数据的风险随着获准处理信息资产人士数目的增加而提升，所以需要清晰确立逻辑访问控制内的认证及授权机制，例如谁应获准访问数据、他们又有哪些访问权限，以及在甚么情况下给予什么访问权限。对于人员访问云端平台数据，应采用「默认全部拒绝」政策及须遵循最小权限原则。

- 建立身分及访问管理架构 [I] [O] [P]

  应考虑使用身分及访问管理架构。身分及访问管理架构容许透过使用公开标准如 OpenID，扩展身分及访问管理实务，藉此于云端平台管理用户帐户的设置、认证及授权。成熟及业界认可的认证及授权标准如安全断言标记语言、可扩展访问控制标记语言都可以更进一步改善安全状况，应适当应用这些标准的安全功能，例如安全断言标记语言的可扩充标示语言签署及可扩充标示语言加密。于身分及访问管理中采用联合身分，能够有助不同身分储存库互相联结，容许用户透过单一登录访问不同的应用系统。

- 采用访问控制标准 [I] [O] [P]

  一旦采用云端服务，用户身分将可能因为身分储存库或目录管理服务连接至云端服务供应商而延伸至云端平台。在选择云端服务时，宜考虑到服务应利用业界标准（例如安全断言标记语言），推行安全单一登录方案，以传递用户身分及属性，以及执行授权政策。

- 要求严谨的认证选项 [I] [O] [P]

  云端服务可以透过不同装置及渠道访问，因此简单的用户登入名称及密码的认证未必足够保障账户免受入侵。在选择云端服务时，应考虑支持双重认证（2FA）的云端服务，并应尽可能为众多用户，特别是特权帐户启用双重认证。常用的双重认证有一次性密码、生物特征和数码证书等。

  为了进一步提供保护，用户访问（尤其是特权账户）应限制于指定的计算机、网络或位置。政府资讯科技总监办公室发表的电子认证架构 [17]为评估风险、决定安全要求，以及推行适当认证方法提供基础。应跟从该架构，决定及推行云端服务上电子交易的电子认证要求。

- 管制及控制高权限实用程序 [I] [O] [P]

  于云端环境内执行未授权的高权限实用程序，可能会令系统及应用系统的控制失效。决策局 / 部门应向云端服务供应商要求提供高权限实用程序的功能规格，以确定在使用这些程序访问云端服务时，安全控制仍然生效。

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

5.6 加密方法

- 管理及保护密码匙 [I] [O] [P] [18]

  密码匙应根据安全规定及政策得到妥善管理及保护。应切实执行密码匙储存管理，密码匙应由决策局 / 部门保管。须界定密码匙生命周期的管理流程：密码匙如何产生、使用、储存、备份、复原、流转及删除。加密操作及密码匙管理宜限制于身份及访问管理系统之下以加强保护。决策局 / 部门不应在不同的云端平台重复使用同一个密码匙，以避免当密码匙被破解后，所有云端平台（特别是混合云端的情况下）亦因此遭到入侵。

5.7 实体及环境安全

一如外包私有云端平台，公共云端平台的数据中心位于客户机构处所以外，云端平台亦可能跨越数个位处不同地理位置的数据中心。当数据移到非客户管理的云端平台数据中心，数据的实体控制将交到云端服务供应商。由于公共云端平台的多租户特性，其中一项主要的安全关注便是数据受同平台不明租户或第三方未授权的实体访问的风险。

于云端数据中心推行充足的实体安全措施，能防范于物理层面运算资源遭入侵的活动。有些云端服务供应商只提供没有上锁的计算机机架。这显然不足以应付多租户环境，因为任何能出入数据中心的人士都有机会接触到存有租户数据的计算机装置。处于非机构处所的云端平台数据中心的环境及设备安全，以及实体访问控制都是实体安全范畴上主要关注的地方。

由公共云端服务供应商提供的服务通常不是针对单一租户环境。随着服务的不断更新，这些云端服务供应商可提供新的解决方案和服务给云端平台用户，例如单一租户解决方案，以迎合市场的需求。建议决策局 / 部门在选择适当的部署模式时仔细研究整个云端解决方案，包括基础设施的构建。例如，如果决策局 / 部门考虑使用私有云端平台来满足业务需求和安全要求，那么单一租户方案只是其中一个考虑因素。决策局 / 部门亦应评估云端基础设施需否专用，以满足私人云端解决方案的要求。据此，决策局 / 部门应根据业务需要和政府安全要求，评估在整体架构上推行何种安全控制措施。

- 选择场地位置及设施的风险分析 [O] [P]

  处于非机构处所的数据中心的设计和管理在实际上未必将安全放在最优先次序。事实上大部分云端服务供应商都将焦点放在成本效益上。因此，在合适的情况下，应实地考察有关设施，例如不间断电源供应器、空气调节及通风系统、灭火系统、水灾损害及水浸控制系统。应根据地方的自然灾害、地区（例如当地管辖权）、网络依赖程度（例如互联网网络枢纽）

[18] 虽然现时的规定没有涵盖非保密数据需要加密，但作为保障数据私隐的良好作业实务，决策局 / 部门宜在使用公共云端服务时，对非保密数据，采用加密技术，并同时对密码匙作管理及保护。

等，评核数据中心、运作复原中心的选址及运作。在不能进行实地考察的情况下，云端服务供应商应向决策局 / 部门提交有关认证或审计报告作参考。

- 为外包数据中心的所有信息技术设备及数据储存媒体采取适当实体保护 [O] [P]

  由于外包云端平台的多租户特性，可能会于外包云端平台数据中心发生未授权访问，所以应对共享数据中心内，所有信息技术设备及数据储存媒体，并所有场外备份媒体订立安全要求，以给予合适的实体保护。云端服务供应商所推行的安全措施应合乎这些安全要求。

- 有需要时划出独立区域作专门用途 [I] [O]

  若因为数据的敏感程度或其他安全要求，而有特别需要不与其他租户共享设备或载有其他租户应用系统的设备架，可考虑设立独立区域，将应用系统拥有人的数据及资源，通常包括服务器、网络设备、储存器、电源及讯号电线，与其他租户分隔。应清楚界定应用系统拥有人在数据中心内的独立区域范围，并应只容许获授权人士访问该区域。另外，数据中心亦不应向公众开放，令公众可以容易进出。为减少未授权或无可避免的访问，独立区域不宜设于公用区域如走廊及主要出口附近。所有数据中心的实体访问都应得到数据中心经理批准并记录在案。

- 限制独立区域的出入 [I] [O]

  应使用电子控制访问系统或其他同级的访问控制措施严格控制独立区域的出入。即使在有人的情况下，独立区域应长期保持上锁。应使用双重控制于授权及审批独立区域的出入，包括授权及批准增减长期出入人员名单。长期出入人员名单应由应用系统拥有人或其他获授权人士审批。所有有需要到达独立区域或设备架的出入人士都应先得到批准并记录在案。应定期（如每季度）覆检区域出入人士的记录，确保记录完整准确，亦应定期覆检长期出入人士名单。

- 考虑为受控制区域订立不同的安全级别 [I] [O]

  对于包含敏感或保密数据的外包信息系统，决策局 / 部门须确保服务供应商已采用适当的控制措施，以管理对设有信息系统的实体区域的访问，以及限制未经授权的其他客户或外人的访问，并仅允许政府批准的人员或访客进入。

  为提高安全水平，值得考虑为数据中心不同区域推行不同程度的控制。一般而言，可以根据寄存于区域内应用系统的重要性及数据的敏感程度，决定该区的出入控制程度。应清楚记录及标记受控制区域的实体及管理控制。

- 确保为共享相同设备架的多个应用系统采取合适访问控制 [I] [O]

  在不同应用系统共享设备架的情况下，应于设备层面，而非设备架层面，订定实体访问审批。此外，为减低共享设备架的风险，亦应推行其他访问控制，例如独立钥匙锁、帐户锁定政策及定期覆检系统记录。

5.8 操作安全

5.8.1 信息备份

- 定期为数据备份 [I] [O] [P]

  因为数据存于云端服务供应商的备份媒体时，可能会和其他云端平台租户数据混在一起，云端服务供应商未必能提供备份媒体予个别云端平台租户。对业务有重要影响的系统，应最少保留一份定期营运数据的脱机备份，以便可以复原至最新状态。在此情况下，须定期进行备份测试，确定复原程序合乎现况。应稳妥储存备份，以及日志、访问记录及任何因法律和规管原因而需要的相关信息的副本，并应只容许获授权人士访问。

5.8.2 记录

- 为审计及分析保存及保护记录 [I] [O] [P]

  对于无论公共或私有云端平台，取得关键记录数据对清晰了解操作及安全事件尤其重要。部分类型的记录数据有助减低操作及安全风险。决策局 / 部门应界定记录种类及内容，如网络、系统、应用程序、管理和变更管理活动的审核记录。记录信息应全面，而且能够反映云端平台的动态特性，例如增减虚拟机实例。应妥善订明记录的保存期，记录亦应能防范干扰。对于公共云端服务，决策局 / 部门应要了解云端服务供应商会否容许用户修改记录设定及会否提交所需记录数据，而且应有与系统关键程度相称的记录覆检程序。可以使用事件关联工具加强记录分析功能。

5.8.3 配置管理及控制

- 确保妥善执行安全程序 [I] [O] [P]

  应建立程序收集及储存审计记录、活动报告、系统配置副本、修改管理报告及其他测试程序结果。视乎云端服务模式，云端服务供应商应在有需要时应提供这些信息。

5.8.4 修补程序管理

- 确保修补程序管理过程有足够控制 [I] [O] [P]

  修补程序赋予程序新功能，并解决程序内的错误或安全漏洞，但由于修补程序是额外／经修改的编码，它亦可能为程序带来不可预计的不良副作用，造成重大风险及严重影响数据的机密性、完整性及可用性。因此，决策局／部门应了解云端服务供应商如何处理以减少不明朗因素，例如云端服务供应商如何厘定修补优先次序，以及执行修补程序的时间表。另外，修补程序管理应得到决策局／部门及云端服务供应商双方同意。

5.9 通讯安全

于云端平台数据中心，实体服务器及网络组件都被虚拟化，并可能由数个租户共享。传统网络的安全措施未必能有效防范云端环境内，同一服务器上虚拟机的攻击。由于部分安全威胁只针对某些虚拟化基本设施，例如通讯盲点、虚拟机间攻击，及虚拟机混合信任水平，加上虚拟机变化不定的特性，都会令维持安全水平及确保记录可被审计的工作变得困难。复制服务器影像并发布到其他实体伺务器的过程十分方便，但亦导致配置错误及其他漏洞借此传播。当采用及推行云端平台基础建设时，需要处理这些由虚拟化带出的安全威胁及问题。

此外，由于数据在分布式云端平台部署中会被共享，数据在云端服务中可能会于不可信网络（例如互联网、公共网络）及／或政府网络间传递，所以应妥善保护传递中的数据。网络及通讯的安全作业对云端服务非常重要。

5.9.1 一般网络保护

- 于传递时保护数据 [I] [O] [P]

  决策局／部门应于多租户或外包数据中心环境内，加强对在服务器及网络组件之间传递的保密数据的网络安全水平。为避免窃听，应为在数据中心内的通讯网络上进行的数据传输进行加密，例如传输层安全性规约（TLS）。建议在连接到云端服务时采用安全措施（如虚拟私有网络、传输层安全性规约）保护在公共网络（如互联网）或政府网络上以保障传递数据的机密性及完整性。在适用的情况下，亦可考虑使用数据层面的加密方法，令数据在传递前可被加密。

- 保护网络上的运算资源 [I] [O] [P]

  很多装置，例如服务器、桌上及手提电脑、智能手机及平板计算机都能利用互联网连接云端服务器。外来入侵者可能透过系统漏洞对云端环境的网络组件及服务器发动攻击。另外，亦不容忽视在多租户环境内，借着云端间通讯进行的内部入侵。应推行适当的网络安全措施，令运算资源在有关

的措施下得到保护，例如网络防火场、应用系统防火墙、入侵检测系统／入侵防御系统及记录监察。应留意要成功抵御攻击，就需要保护云端运算的客户端及服务器端双方。

5.9.2 虚拟化的安全

虚拟化技术是让云端平台实现多租户或多应用系统环境灵活部署及提供按需要服务的主要机制。虚拟化能让云端服务供应商从实体服务器的剩余能力取得更多运算资源，但亦同时带来安全风险。云端运算的特性令决定如何处理安全事故、数据外泄或其他需要调查的安全问题变得困难。

正如第5.7节所述，由公共云端服务供应商提供的服务通常不是针对单一租户环境或单一应用环境。随着科技和市场发展，一些云端服务供应商可能在行业中提供新的服务和方案。有些公共云端服务供应商也可能扩展他们的方案，容许租户对云端服务资源有更多的控制，因此有些原本对私有云端适用的虚拟化的安全考虑也扩展至适用于公共云端。

同样，建议决策局／部门在选择适当的部署模式时，应当仔细研究整个云端基础设施。例如，如果决策局／部门考虑使用私有云来满足业务需求，那么在评估其是否为专用云端基础架构时，无论是否使用虚拟化，单一租户环境只是其中一个考虑因素。因此，决策局／部门应根据业务需要和政府的安全要求，对整体基础设施应该推行何种安全控制措施进行评估。关于虚拟化的安全实践，请参考以下要点：

- 保持主机操作系统精简及坚固 [I] [O] [P]

  为减少受攻击风险及修补次数，主机操作系统应配置最少所需功能。应强化及尽量精简已安装的主机操作系统，例如停用不必要的服务和通讯端口，务求减低加载任意组件、软件库和软件的能力。

- 部署高可用性技术 [I] [O] [P]

  为应付单点故障，应考虑复原能力如主机上的虚拟机集群。例如当一个主机失去供电时可能会影响数个虚拟机。在硬件故障的情况下，受影响的虚拟机可以利用剩余能力于集群节点中自动重启，令服务影响减至最低。

- 为虚拟化中的每个独立组件订立安全要求及巩固组件 [I] [O] [P]

  整体虚拟化方案的安全非常依赖当中每个组件的个别安全。从虚拟机管理程序和主机操作系统，到客户操作系统、应用系统及储存服务，所有这些组件都应根据相关的安全政策及标准而强化。应使用涵盖所采用虚拟化技术的漏洞扫瞄工具定期扫瞄主机及客户操作系统，并应制订及推行配置管理程序，将虚拟环境内，实体及虚拟机的所有安全设定纳入管理。

- 启用虚拟机专属的网络安全功能 [I] [O] [P]

  虚拟机可以于硬件底板上作通讯，而非透过联机网络。底板上的通讯并不能够被监察，或在有可疑通讯时线内拦截。应采用虚拟机专属的安全机制，例如虚拟网络及虚拟机管理程序层的虚拟防火墙，对虚拟机底板上的通讯进行更仔细监察。应只容许获授权人士远程访问虚拟机的管理控制台。

- 执行最小权限原则及工作分隔 [I] [O] [P]

  在分散及虚拟化环境内，如何界定细分计算机用户（包括不同的管理员）的角色和职责颇具挑战。云端、虚拟机架构、储存器、网络和系统的管理员应能执行他们的职务而无法访问到他们所管理的系统中的敏感数据。决策局 / 部门应严格执行职务分工，并定期检讨以防范不同的攻击，包括外部攻击（例如：进阶持续性渗透攻击）或内部攻击。此外，应将安全管理工作的账户、职务及人士与其他行政活动分开，防范未授权修改，进一步保护计算机资源及审计追踪。

- 建立安全区域分隔不同信任水平的虚拟机 [I] [O] [P]

  应在发展虚拟机环境初期，探讨分隔虚拟机的效用及可行性。建议依据发展阶段（如设计、测试及投入运作）、数据类型（保密及非保密数据）、架构层（例如网络、应用程序、数据库和档案）或系统关键性（关键系统及非关键系统），于不同的实体服务器上建立安全区域。若不能避免于同一实体服务器上分享不同类型的数据 / 系统，则可同时利用虚拟局部区域网络、防火墙及入侵检测系统 / 入侵防御系统，分隔虚拟机作为对策。连接虚拟化环境到内部网络不应削弱现有安全水平。

- 于较关键系统考虑使用裸机（类型 I）虚拟机管理程序 [I] [O]

  一般而言，有两类虚拟机管理程序 —裸机（类型 I）及寄存式（类型 II）。裸机虚拟机管理程序于硬件产品上运行，而寄存式虚拟机管理程序则安装在主机操作系统（例如 Linux）之上。寄存式虚拟机管理程序有可能会继承主机操作系统的漏洞，以及在相对复杂环境内面对更多安全威胁。相对地，裸机虚拟机管理程序一般提供更精简及安全的硬件操作系统，而且这类虚拟机管理程序直接与硬件作沟通，减少安全问题。一般而言，公共云端平台比私有云端平台有更多的安全风险考虑，因其云端平台基础设施被用户共享。因此，即使公共云端服务供应商提供裸机虚拟机管理程序时，公共云端平台仍可能不适用于关键系统，特别是当涉及保密数据时。因此，这项安全考虑和控制不应用于公共云端平台情景。

- 分析相关安全风险 [I] [O] [P]

  在推行虚拟化前，应先与没有虚拟化的选项比较，分析当中安全风险。这应成为选出云端服务供应商或产品前的风险管理程序的一部分。

- 覆检虚拟机及应用系统的资源要求 [I] [O] [P]

  为避免资源冲突，应妥善计划及检讨资源的运作，例如中央处理器、内存、输入／输出流量、磁盘空间，以及网络容量。

- 防范两个虚拟机之间的未授权访问 [I] [O] [P]

  应对虚拟机间的沟通采取最小权限原则。例如虚拟机应适当配置，收紧主机防火墙规则及关掉不必要的网络规约，以防范未获授权访问。

- 备存资产记录 [I] [O] [P]

  已部署的虚拟化环境需要记录在案。由于在虚拟化环境内，有些网络组件（如虚拟交接器／防火墙）未必能容易地利用在线工具辨认，因此需要准备一份可供审计的完整虚拟机及基本设施组件详细列表，并应保持更新。

- 确保软件使用证有效及足够 [I] [O] [P]

  虚拟化正改变软件授权方式。不同软件供应商可能采用不同授权方法，例如按个体（实体或虚拟）、硬件（实体或虚拟）、用途，或客户（例如人数或同时连接数目）等。在很多情况，决策局／部门需要评估、商议及优化与主要供应商订制在虚拟化环境内的使用协议。

- 为脱机虚拟机安装最新的安全修补程序及病毒标识符 [I] [O] [P]

  休眠中的虚拟机容易被安全及监察作业忽略，导致虚拟机曝露于已知的威胁中。决策局／部门应就此强制要求更新休眠虚拟机的安全修复程序及病毒标识符。在合适情况下，可以考虑使用一些先进的安全工具以应对休眠中而又有修补需要的虚拟机。

- 检验快照复原后的虚拟机安全状况 [I] [O] [P]

  大部分的虚拟机容许建立「快照」，储存不同时间的机器设定及配置状态，作备份及维修之用。若有需要从过往一段时间的快照复原虚拟机，必须查核快照的修补程度以及其安全设定及配置。应开启虚拟机的审计追踪功能，包括修补工作，以追踪不同活动。

- 保护虚拟化影像及配置档案 [I] [O] [P]

  因为虚拟机连内在的数据及应用系统能够从一个主机被复制到另一主机上，入侵者可将虚拟机副本带到另一个不安全的虚拟机管理程序，从而访问原本虚拟机内的数据及配置档案。决策局／部门应收紧具审计功能的逻辑及实体访问控制，防范未授权访问及修改资源池，例如中央处理器、内存及储存输入／输出装置。

- 关掉不必要的通讯端口、服务及虚拟硬件 [I] [O] [P]

  应关掉所有不必要的通讯端口、服务及虚拟硬件例如通用串行总线端口、虚拟机间的剪贴簿功能及虚拟网络适配器等，令各组件间互相被逻辑性隔离，防范因其中一个虚拟机受到入侵，而泄露数据至其他虚拟机。

- 按需要地为每个虚拟机或相关虚拟机集群推行基于虚拟机管理程序、基于网络及基于主机的保护方案 [I] [O] [P]

  基于网络的防火墙（或入侵检测系统）能于多租户环境有效运作。而基于主机的防火墙则提供较细致的网络控制，能在虚拟环境内运作，但在大型云端环境可能有工作量及管理问题。基于虚拟机管理程序的防火墙为动态云端环境提供安全自动化功能，监察及栏截虚拟机间的恶意通讯。应小心选择以上的防火墙，以符合业务需要，并为防火墙配置严谨的防火墙规则。防火墙亦应能在重置虚拟机时，便携到新环境上。

- 记录虚拟机管理程序和虚拟机上，高权限账户的活动 [I] [O] [P]

  为追踪安全事故的源头及事件，需要记录高权限帐户在虚拟机上的所有活动。同样地，由于虚拟机管理程序拥有管理及配置辖下虚拟机的能力，因此亦需要记录虚拟机管理程序的高权限帐户。安全记录应包括例如访问虚拟机影像及快照、变动用户访问权限，及修改档案权限等事件。应考虑使用防窜改记录工具及完整性监察工具以确保记录档案完整，亦应定期监察及覆检安全记录。

- 小心管理虚拟机影像及快照 [I] [O] [P]

  虚拟机的影像及快照可能收集了在取得影像／快照一刻，出现在系统内的保密数据。因为快照记录了拍照一刻活跃内存的内容，所以快照比影像的风险更高。若不能防范影像／快照被修改，入侵者就有可能访问，并注入漏洞或恶意软件，然后于虚拟环境内重新部署。应删除不再使用的影像副本及快照。应确实执行与虚拟机所处理数据的保密分类同级的安全措施，以保护相关的虚拟机影像和快照。

- 安全清除虚拟机数据 [I] [O] [P]

  当在实体服务器删除虚拟机，或将虚拟机移到另一实体服务器时，决策局／部门应确保磁盘上没有残留任何可作复原之用的数据。应使用安全删除方案清除虚拟机。

- 保护管理界面 [I] [O] [P]

  应在虚拟机以外执行安全控制，以免管理界面（例如网上管理界面及应用程序界面）受到未授权访问。应在启用审计追踪功能的情况下，控制和监察所有管理对话，以尽早侦测并阻截未授权或可疑的对话。

5.10 系统购置、发展及维护

随着云端运算的兴起，安全架构亦趋高度多变。云端特征，例如于一个数据中心内与多租户共享计算机资源，令配置管理及持续服务供应亦比传统信息技术环境更见复杂。云端运算影响着软件发展周期的各个方面，亦为建立及维持现行应用系统的工具和服务带来一些新挑战。

对于一些软件即服务的应用系统，云端服务供应商将多个租户数据储存至应用系统数据库，并在每个数据库表加入额外属性如「租户名称」识别租户。恶意租户可以透过软件漏洞，例如手稿程序错误或经特制结构化查询语言的查询，入侵应用系统，并访问其他租户数据。此外，安全弱点诸如过时网页浏览器和未受保护的网页对话，都可能导致应用系统的完整性和调制解调器密性受损害。所有与应用系统安全有关的安全问题在应用系统移至云端平台后仍然适用。

- 在云端应用系统上，应用安全软件开发周期[I] [O] [P]

  云端平台上建立应用系统时，应该采用安全的软件开发周期程序（或其他合适的开发方法），例如安全设计覆检及软件测试，务求减少应用系统在发布后面对的潜在威胁。通过在开发周期的积极检查，以解决整个开发过程中的安全威胁。这包括：

  (i) 在设计时间建立威胁模型，于早期识别及减少潜在安全问题；
  (ii) 依循编写程序的良好作业模式及安全编码标准（例如源始码审查、个人资料去识别化、数据输入确认及输出编码要求），防范网上应用系统漏洞；以及
  (iii) 于部署前要求使用不同工具（例如程序代码扫描和分析工具、测试工具和源始码混淆工具）作测试、验证及程序代码保护。

- 管理及保护凭证 [I] [O] [P]

  云端技术令应用系统部署变得容易，而部署工作亦一般由云端平台的开发人员专责。管理及保护进入运作环境的凭证亦变得重要。应小心保管凭

证，以协助防范未授权访问及非法窜改应用系统程序及控制档案。应订立周详的政策及程序并严格遵守，以维持应用系统环境的完整性。

5.11 外包信息系统的安全

公共及外包私有云端平台的云端服务都并非经内部人员管理或操作。就外聘云端服务供应商管理的云端服务的相关安全作业，须考虑以下方面：

- 在决定开始使用处于外包数据中心的外包云端服务前，分析安全风险[O] [P]

  应依据信息技术安全要求分析所有安全风险。分析结果将为管理层提供基础以就开展外包云端服务作出合适决定。

- 在准备外包标书时，清楚界定外包范围的安全要求 [O] [P]

  在准备外包标书时，应清楚界定业务及安全范畴内的相关要求，如实体安全、管理职责、安全事故管理及安全风险评估及审计，并列明可量度的表现指标。应在定制的服务水平协议内列明要求。亦如任何外包安排一样，应清晰厘清数据拥有权，并得到云端服务供应商同意。

- 制定服务水平协议及监察修改 [O] [P]

  应充分留意由服务水平协议条款引起的后续效应，例如数据位置、不同方面的职务和责任、遵行要求，以及数据备份及复原等。有需要时，修改服务水平协议以解决任何可能导致安全事故的安全问题。决策局 / 部门应评估及确定服务水平协议内的条款合乎自身业务及安全要求。对于公共云端服务，由于云端服务供应商可保有权利于任何时间更改一些服务水平协议内的条文，并只有限度提早作出通知，因此应定期访问云端服务供应商网站，检查通用条文有否任何改动。

- 确保外聘云端服务供应商提供符合政府安全要求的安全控制 [O] [P]

  应推行控制机制，以满足政府对所涉及调制解调器密级别及敏感程度相对应的安全要求。决策局 / 部门应在适当情况下尽职审查及监督云端服务供应商以满足业务、安全及私隐需要。对于云端服务供应商未能完全处理的风险，决策局 / 部门应提供额外的控制以减低该风险。

- 确保妥善解决外来威胁 [O] [P]

  外包云端服务供应商应利用最佳作业实务保护本身提供的主机及应用系统，以防范外来威胁及未授权访问。在可行的情况下，作业实务可包括，但不限于，强化操作系统、以最新修补程序保持更新、适当安装基于虚拟机管理程序、基于网络或基于主机的抗恶意软件程序、入侵检测系统 / 入

侵防御系统及防火墙。云端服务供应商应定期进行安全风险评估，确保系统保持所需安全水平。决策局／部门亦应定期覆检云端服务供应商提交的安全风险评估及审计报告。

- 制订退出策略 [O] [P]

  应于采用云端服务早期制订退出策略或退出计划。退出计划宜由云端服务供应商或决策局／部门提供。退出计划应包括如何将数据及虚拟环境从云端服务供应商处提取，以及如何清除数据及虚拟环境。在制订退出计划过程中，亦需处理与单一云端服务供应商捆绑的风险。通过对退出条款的再行商讨亦有助减低风险。

5.12 信息安全事故管理

即使信息系统已采取所有必需的安全措施，系统仍会偶尔发生安全事故。安全事故处理涉及安全事故发生前，发生途中及发生后的一系列连续的过程。云端运算的特性令客户机构在安全事故、数据外泄或其他需要调查的安全问题上，更难决定该如何处理。例如，客户机构可能认定一宗安全事故为危急，但云端服务供应商未必同意，并因而只投放少量工夫跟进个案。

云端运算的采用改变了事故应急的结构，尤其于公共云端平台上，由于客户机构并不拥有该网络，所以不能直接访问网络记录。一些云端服务供应商在他们的通用水平服务协议上列明供应商并无责任调查任何可能导致安全事故的安全违规及服务滥用。客户机构应留意以下事故监察及应急的安全作业实务：

5.12.1 安全事故监察

- 界定事故监察及通报责任 [O] [P]

  在服务水平协议内，应订明外聘云端服务供应商在事故监察上，能给予决策局／部门的支持。源自云端服务供应商基础设施的信息安全事故可能影响决策局／部门的资源，因此应向决策局／部门详细通报。决策局／部门亦应与云端服务供应商建立通讯计划，于发生事故时通报及升级处理。服务水平协议应记载清晰的事故分类计划、通报责任，以及云端服务供应商应达到的服务水平。

- 提供数据作事故分析 [O] [P]

  决策局／部门应得允许访问与事故侦测有关的数据来源及数据，云端服务供应商亦应为事故分析提供适当协助。备份及其他记录副本、访问记录，以及任何其他相关数据都应能被移离云端环境。对于公共云端服务，记录数据的可用性会因用户所选项而异。应根据业务需要和调制解调器密分类开启并适切配置审计追踪及记录功能。

5.12.2 安全事故应急

- 确保符合事故应急规定 [I] [O] [P]

  决策局 / 部门应留意云端服务供应商整体事故处理的理念，以及确保供应商对安全事故所采取的行动及应急时间符合部门的要求。应清楚界定云端服务供应商在事故应急中的职务。决策局 / 部门应与云端服务供应商就如何收集、储存及分享事故调查证据（例如安全记录）达成共识。

- 覆检云端服务供应商往绩 [O] [P]

  若有的话，应取得及覆检云端服务供应商的事故应急管理往绩及经验。现有用户就事故应急计划的推荐将有助参考。

- 为非机构处所云端服务订立事故应急管理及程序 [I] [O] [P]

  决策局 / 部门应就事故应急措施与云端服务供应商紧密合作，并应已建立及备存处理云端服务事故处理管理及程序。与一般系统相似，事故处理程序应包括向政府信息安全事故应急办事处汇报，以及根据《信息安全事故处理实务指南》作出的采取行动。应制订及建立有效机制来报告、通知、调查及处理信息安全事故或安全违规。云端服务供应商应于供应商及决策局 / 部门同意的时间，向决策局 / 部门指派的联络人报告所有有关安全的问题。应有一套内部升级程序处理事故，旨在能迅速应急及得出适当决议，以对决策局 / 部门运作的影响减至最低。有需要时，亦宜将以上安排所得的表现指针纳入服务水平协议内。

- 与云端服务供应商为事故应急进行演习 [I] [O] [P]

  决策局 / 部门须在可行的情况下与云端服务供应商合作进行事故应急演习。可行的演习方法包括纸上演练、电话串联演练，以及全面演习。应于新版本的事故应急计划中记录改善之处。

5.13 信息技术安全方面的业务持续运作管理

- 确保有效的数据备份及运作复原安排 [I] [O] [P]

  无论由决策局 / 部门或云端服务供应商管理运作复原安排，决策局 / 部门都应确保这些安排的效用与决策局 / 部门的要求一致；订定恢复点目标及复原时间目标、运作复原中心位置、复原小组的职务和责任、运作复原事件用的通讯渠道，以及复原优先次序，并与服务水平协议互相联系。

- 制订业务连续性计划 [I] [O] [P]

  决策局 / 部门的业务连续性计划应包括失去云端服务供应商服务及失去需要倚赖的第三方支持。应与云端服务供应商协调，测试计划的这个部分。若情况许可，应检视云端服务供应商的业务连续性计划。建议要求云端服

务供应商提供现行管理支持的证据，以及云端服务供应商业务连续性计划定期覆检的证据。

5.14 遵行要求

在规模经济的考虑下，云端服务供应商推行多租户环境及混合使用资源池。尤其在用户共享的公共云端平台、数据中心、运算装置、数据储存器及人力资源。而由于私隐问题，一般不会容许个别客户机构进行深入的评估及审计。在大部分的公共云端平台，云端服务供应商未必能够同意个别客户自定义审计责任。若云端服务供应商不允许客户直接进行安全风险评估及审计，则应要求供应商提供符合业界标准及满足决策局／部门要求的第三方审计报告。

须留意云端运算可指不同的服务模式，包括软件即服务、平台即服务及基础设施即服务的模式。每个模式的风险和安全控制不同，外包的主要考虑因素亦各异，因此安全风险评估及审计的程序亦可能不尽相同。

5.14.1 安全风险评估

- 为云端平台系统或应用系统评估风险 [I] [O] [P]

  一如传统应用系统，在云端平台系统或应用系统提供正式服务前，以及进行大规模升级和变更前，应进行安全风险评估。应评估云端平台的安全风险，并推行合适的安全控制以减低风险。亦应定期检讨安全控制的成效，以及按需要改善控制，因为随着新技术的出现，可能会对云端服务提供更好的保护（附件 B 提供了一些与云端安全相关的新兴技术）。若所需的安全控制应由云端服务供应商推行，则应获知云端服务供应商的安全推行细节。

- 定期进行安全风险评估 [I] [O] [P]

  安全风险评估是一项持续的活动。对于私有云端平台，安全风险评估的频率应该根据信息技术安全政策而订定；对于公共云端平台，决策局／部门则应确保云端服务供应商按照与决策局／部门安全政策一致，或事前共同协议的时期，定期由外聘安全审计师进行安全风险评估，例如按系统的关键性，每年一次或每两年一次重新评估安全风险及控制。

5.14.2 审计

- 达成审计共识 [O] [P]

  决策局／部门应寻求审计权。为审计及核实于服务水平协议内列明的安全控制有否推行及是否有效，决策局／部门需要提早与云端服务供应商，就决策局／部门可对云端服务供应商访问的程度达成共识。签署合约前的安全控制审计将因此成为云端平台合约生效往后的审计基准。双方应就如何收集、储存及分享遵行证明（例如审计记录、活动报告、系统配置）达成共识。

决策局／部门亦应聘用独立审计师定期进行审计，包括渗透测试和安全漏洞评估，并提供相关的理论依据和证据，以支持有关遵行安全要求的判断。若不能够对云端服务供应商进行安全审计，则应要求云端服务供应商提供第三方审计报告。

- 保持安全审计的宽度及深度一致 [O] [P]

  若可行的话，决策局／部门及云端服务供应商应共同互相披露或提早选择外聘核数师。决策局／部门与云端服务供应商的安全审核宽度及深度应保持一致。应定期收集云端服务供应商的审计报告以作分析，确保符合所需安全要求。

- 确保云端平台上的安全遵行 [I] [O] [P]

  应检查有否遵照政府安全规例及政策。在采用云端服务前，应在服务合约及服务水平协议内清晰列明加入遵照政府安全规例及政策的规定。由云端服务供应商提交，用以作遵行检查的数据宜包括信息安全政策、应急计划及测试报告、事故应急程序、安全审计报告、授权覆检报告、职务分工图、信息安全意识培训记录、系统基准配置标准文件、配置管理计划，以及定期覆检结果。

- 场内安全检查 [I] [O] [P]

  云端服务供应商应协助决策局／部门进行场内安全审计及让决策局／部门瞭解数据中心内现行的安全措施。审计小组应由不同方面人士组成，包括信息技术、信息安全、业务连续性及实体安全。决策局／部门应在检查访问前，要求云端服务供应商提交业务连续性计划、运作复原计划、相关证书（例如 ISO[19]、信息技术基础架构库标准）、审计报告及测试计划。

完

[19] ISO － 国际标准化机构

附件 A: 不同云端平台部署情景的安全控制概览

安全控制	[I]	[O]	[P]
5.1 管理职责			
• 依照不同管辖范围分析对安全程序的影响		√	√
• 核实对业界安全标准的遵行		√	√
5.2 信息技术安全政策			
• 覆检部门安全政策	√	√	√
5.3 人力资源安全			
• 界定资源控制及信息安全中的职务及责任	√	√	√
• 要求不可披露协议及确保适当人力资源管理		√	√
• 发出指南或通知提醒用户	√	√	√
• 确保给予有关人员适当的安全训练	√	√	√
5.4 资产管理			
• 透过加密保护数据	√	√	√
• 遵守有关外包数据中心的数据保护及私隐法例		√	√
• 个人资料去识别化	√	√	√
• 追踪数据位置		√	√
• 侦侧及防止数据迁移至云端平台		√	√
• 备存最新的资产清单	√	√	√
• 确保计算机设备的弃置或重用控制是合适及得到妥善推行	√	√	√
5.5 访问控制			
• 清晰订立逻辑控制	√	√	√
• 建立身分及访问管理架构	√	√	√
• 采用访问控制标准	√	√	√
• 要求严谨的认证选项	√	√	√
• 管制高权限实用程序	√	√	√
5.6 加密方法			
• 管理及保护密码匙	√	√	√
5.7 实体及环境安全			
• 为选择场地位置及设施分析风险		√	√
• 为外包数据中心的所有信息技术设备及数据储存媒体采取适当实体保护		√	√
• 有需要时划出独立区域作指定用途	√	√	
• 限制独立区域的出入	√	√	
• 考虑为受控制区域订立安全级别	√	√	
• 确保为共享相同设备架的多个应用系统采取合适访问控制	√	√	
5.8 操作安全			
5.8.1 信息备份			
• 定期为数据备份	√	√	√

5.8.2 记录			
• 为审计及分析保存及保护记录	√	√	√
5.8.3 配置管理及控制			
• 确保妥善执行安全程序	√	√	√
5.8.4 修补程序管理			
• 确保修补程序管理过程有足够控制	√	√	√
5.9 通讯安全			
5.9.1 一般网络保护			
• 于传递时保护数据	√	√	√
• 保护网络上的运算资源	√	√	√
5.9.2 虚拟化的安全			
• 保持主机操作系统精简及坚固	√	√	√
• 部署高可用性技术	√	√	√
• 为虚拟化中的每个独立组件订立安全要求及巩固组件	√	√	√
• 启用虚拟机专属的网络安全功能	√	√	√
• 执行最小权限原则及工作分隔	√	√	√
• 建立安全区域分隔不同信任水平的虚拟机	√	√	√
• 于较关键系统考虑使用裸机（类型I）虚拟机管理程序	√	√	
• 分析相关安全风险	√	√	√
• 覆检虚拟机及应用系统的资源要求	√	√	√
• 防范两个虚拟机之间的未授权访问	√	√	√
• 备存资产记录	√	√	√
• 确保软件使用证有效及足够	√	√	√
• 为脱机虚拟机安装最新的安全修补程序及病毒标识符	√	√	√
• 检验快照复原后的虚拟机安全状况	√	√	√
• 保护虚拟化影像及配置文件安	√	√	√
• 关掉不必要的通讯端口、服务及虚拟硬件	√	√	√
• 按需要地为每个虚拟机或相关虚拟机集群推行基于虚拟机管理程序、基于网络及基于主机的保护方案	√	√	√
• 记录虚拟机管理程序和虚拟机上，特权账户的活动	√	√	√
• 小心管理虚拟机影像及快照	√	√	√
• 安全清除虚拟机数据	√	√	√
• 保护管理界面	√	√	√
5.10 系统购置、发展及维护			
• 在云端应用系统上，应用安全软件开发周期	√	√	√
• 管理及保护凭证	√	√	√
5.11 外包信息系统的安全			
• 在决定开始使用处于外包数据中心的外包云端服务前，分析安全风险		√	√
• 在准备外包标书时，清楚界定外包范围的安全要求		√	√
• 制定服务水平协议及监察修改		√	√

• 确保外聘云端服务供应商提供符合政府安全要求的安全控制		√	√
• 确保妥善解决外来威胁		√	√
• 制订退出策略		√	√
5.12 信息安全事故管理			
5.12.1 安全事故监察			
• 界定事故监察及通报责任		√	√
• 提供数据作事故分析		√	√
5.12.2 安全事故应急			
• 确保符合事故应急规定	√	√	√
• 覆检云端服务供应商往绩		√	√
• 为非机构处所的云端服务订立事故应急管理及程序	√	√	√
• 与云端服务供应商为事故应急进行演习	√	√	√
5.13 信息技术安全方面的业务持续运作管理			
• 确保有效的数据备份及运作复原安排	√	√	√
• 发展业务连续性计划	√	√	√
5.14 遵行要求			
5.14.1 安全风险评估			
• 为云端平台系统或应用系统评估风险	√	√	√
• 定期进行安全风险评估	√	√	√
5.14.2 审计			
• 达成审计共识		√	√
• 保持安全审计的宽度及深度一致		√	√
• 确保云端平台上的安全遵行	√	√	√
• 场内安全检查	√	√	√

附件 B: 新兴云端安全技术

随着云端运算的广泛应用、传统安全控制可能不足以保护云端环境中机构的信息资产。正因为如此，安全服务供应商为了解决相关的安全问题，推出一些新的云端运算安全措施。下面重点介绍与云端安全相关的一些新兴技术例子。

B.1 身份管理即服务（IDaaS）

随着越来越多云端服务的部署，用户访问及访问记录的管理工作变得日具挑战。身份管理即服务（IDaaS）是一种基于云端的服务，提供一系列针对云端应用及客户处所内的旧有系统的身份及访问管理功能。身份管理即服务的功能包括：

- 身份管治与管理 —这包括身份管理的能力，例如自助服务用户配置、密码同步
- 身份访问 —这包括用户验证、单一登录，以及政策执行
- 身份分析 —这包括记录事件，以及访问报告

由于身份对平台或系统极为重要，云端平台用户在部署身份管理即服务时要注意以下事项：

- 身份管理即服务供应商的可靠性和诚信
- 身份管理即服务在云端平台和网络访问时的可用性
- 身份数据的复原能力和保护
- 对用户身份的操作和访问控制
- 凭证管理

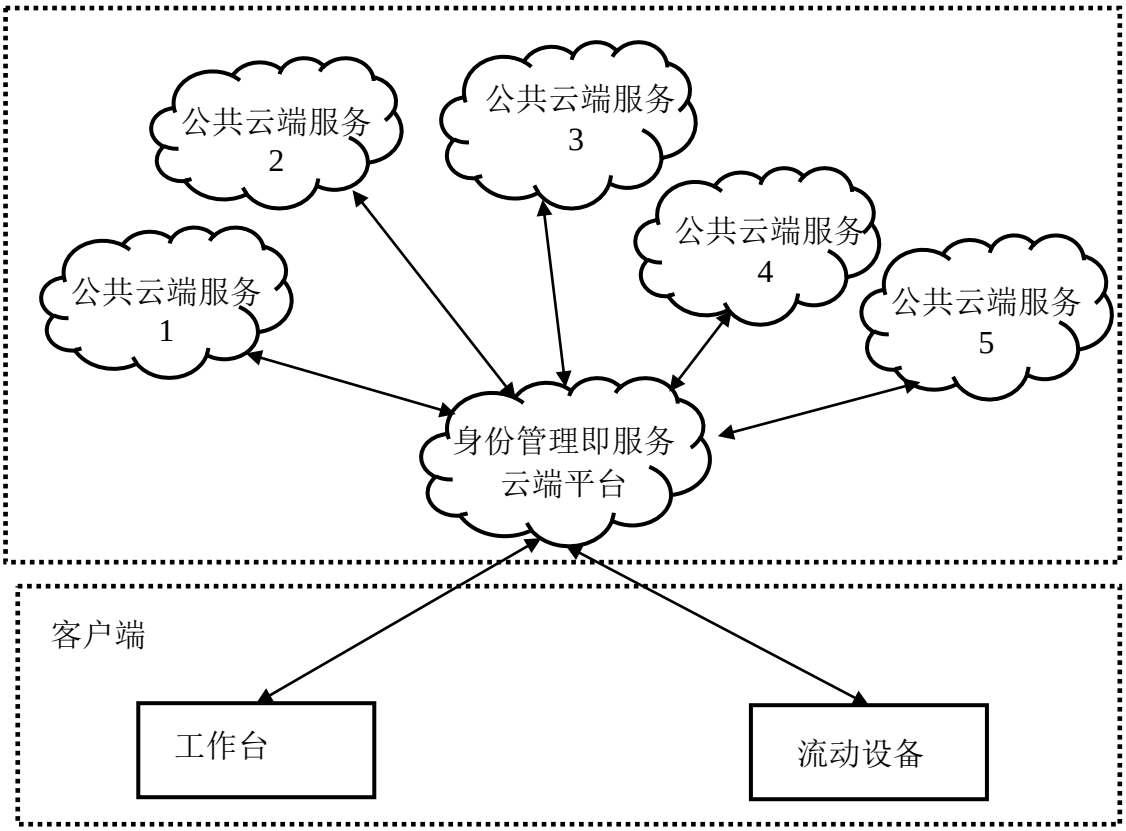

图 B.1 身份管理即服务的使用情景

在使用这些云端服务之前，应该进行关键风险分析和详细的遵行覆检。决策局／部门应确保在处理云端平台的保密资料时，特别是在考虑使用身份管理即服务时，符合政府的安全要求。 为了降低跨云端平台被入侵的风险，应避免在不同云平台之间重复使用身份。 第5节 - 云端服务的安全考虑和控制的良好作业模式也适用于身份管理即服务的云端服务。

B.2 云端访问安全代理（CASB）

云端访问安全代理（CASB）作为一个控制点，可在多个云端应用程序中确保安全政策、遵行和管治的执行。云端访问安全代理具有以下功能：

- 云端访问监控－提供机构的云端服务使用情况和用户访问的统一视图，包括使用的设备和用户位置
- 安全政策的落实执行－基于数据的保密类别实施限制访问的安全政策，及监察保密数据访问或特权升级的用户活动
- 云端服务保护数据－提供档案或字段加密
- 威胁防护－防止那些尚未获准访问的设备、用户和应用系统版本的访问

当安装于网络周边，云端访问安全代理可用于监视云端服务的使用情况，并可被视为额外的安全控制（参见图B.2）。该软件可以在机构处所、云端平台或两者混合。服务访问可以采取不同的方式，例如反向代理、转发代理、API模式或混合／多模式。云端访问安全代理可以包括在「安全访问服务前端」框架中，该框架可根据实体身份确保云端为本网络的安全访问，增强网络安全，从而容许扩充安全基础架构。由于云端访问安全代理相对较新且仍在不断发展，决策局／部门应在选择合适的部署解决方案之前，根据业务需求、特性、支持、价格、与运作和基础设施的整合等各种准则进行适当的市场研究和产品评估。

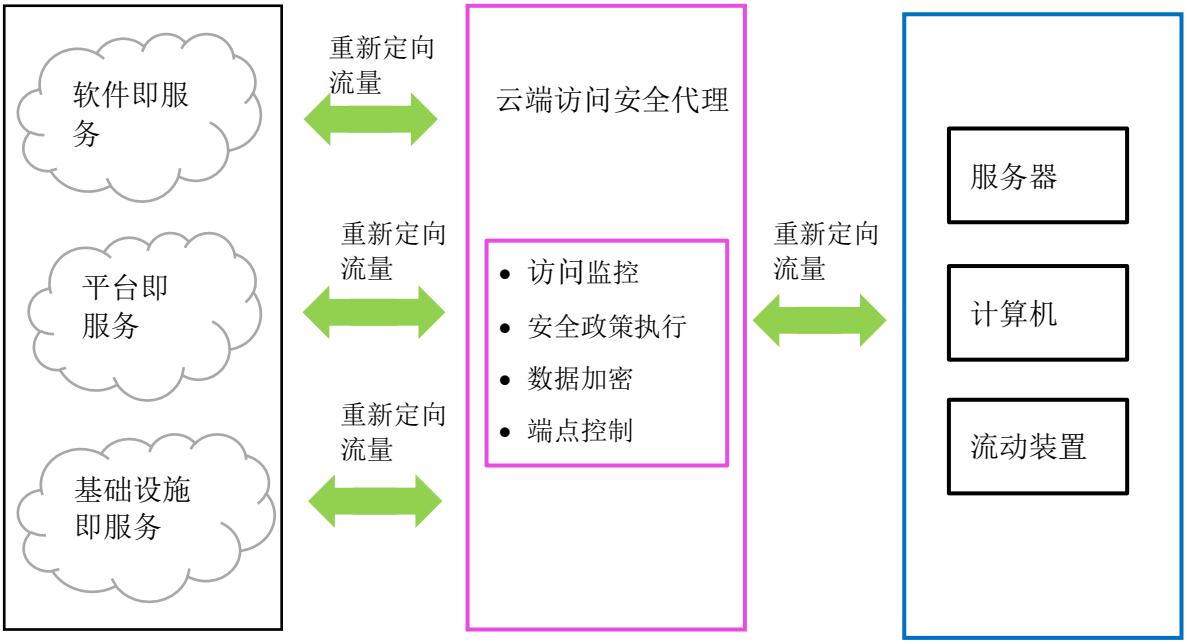

图 B.2 透过云端访问安全代理访问云端服务

B.3 云端工作负载保护平台（CWPP）

工作负载是一个通用术语，用于描述在实体服务器、虚拟服务器或容器[20]中执行的程序。随着采用不同平台的云端服务越来越多，各种工作负载也随之被建立。 因此，要保持在不同云端平台之间各工作负载的安全水平一致，这令系统管理员的工作量和难度增加，特别是当涉及公共云端服务时。

在公共云端服务部署中，云端平台用户可能不可以像机构处所内部部署那样实施安全控制，并且可能缺少对云端服务的安全控制的监视。为了迎合这一需求，云端工作负载保护平台包含一系列的软件，用于简化在各种云端平台（包括机构处所内部、私有云端平台和公共云端平台）上部署工作负载保护的管理工作。云端工作负载保护平台可以通过中央管理来监控混合云端基础设施中的安全政策，以确保执行一致的安全政策（图B.3）。

[20]虚拟机拥有操作系统的完整映像，而云端容器只包含运行某个应用程序所需的相关程序、设置和存储

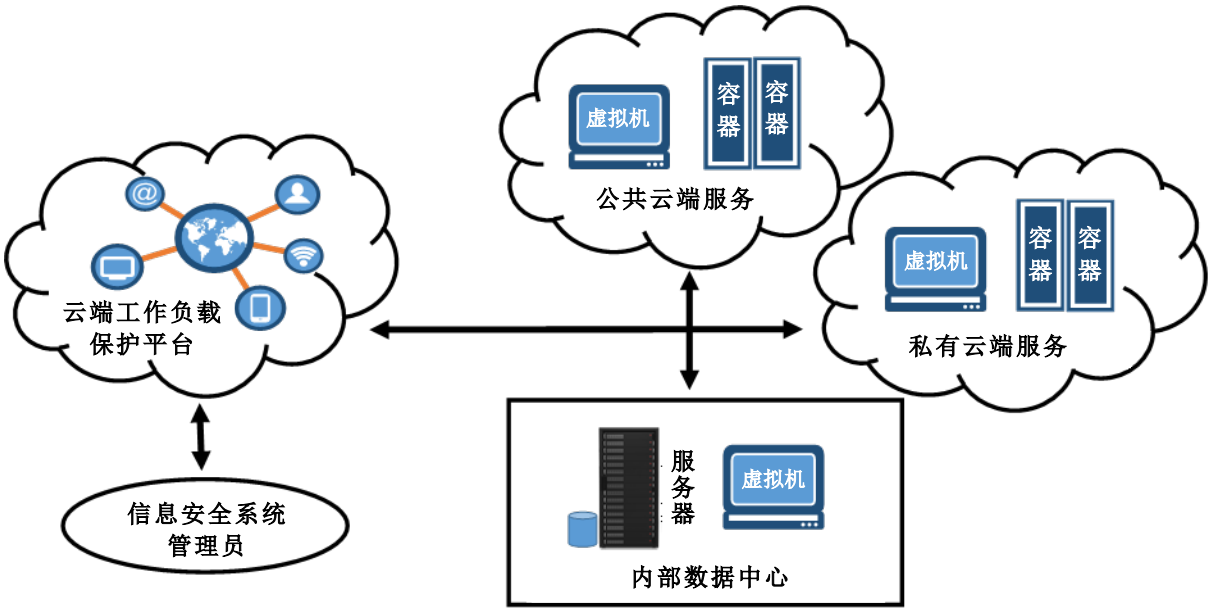

图 B.3云端工作负载保护平台

云端工作负载保护平台在混合云端环境中提供以下工作负载的管理功能：

- 系统监视和管理
- 网络防火墙和分隔
- 应用程控
- 配置和漏洞管理
- 内存记忆保护

一些云端工作负载保护平台供应商会提供额外的保护功能，例如：

- 数据加密
- 主机入侵防御系统 (HIPS)
- 端点保护，例如抗恶意软件等

与云端访问安全代理类似，云端工作负载保护平台相对较新并且仍在不断发展，决策局 / 部门应在部署前进行适当的市场研究和产品评估。尤其应该考虑不同环境中解决方案的兼容性（如服务器和操作系统的支持、虚拟化、容器、API等）以及使用集中软件管理各种云端服务的风险。