政府资讯科技总监办公室

信息安全

安全风险评估及审计

实务指南

[ISPG-SM01]

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	G51 安全风险评估及审计指南第 5.0 版已转换成安全风险评估及审计实务指南。修改报告可于政府内部网络「信息技术情报网」查阅：(http://itginfo.ccgo.hksarg/content/itsecure/review2016/amendments.shtml)	整份文件	1.0	2016 年 12 月
2	增加关于信息技术安全管理的新章节、修定安全风险评估与安全审计的描述，及与其他实务指南保持参考上的一致。	整份文件	1.1	2017 年 11 月
3	根据最新版本的《基准信息技术安全政策》[S17] 第 7.0 版和《信息技术安全指南》[G3] 第 9.0 版的更改加入相关更新	整份文件	1.2	2021 年 6 月

目录

1. 简介

信息技术安全风险评估和安全审计是信息安全管理的重要组成部分。本文件提供了参考模式，以便独立安全顾问或审计师所提供的服务，在范围、方法及成品各方面互相配合。透过这模式，可提高管理层用户、信息技术管理人员、系统管理员及其他技术和操作人员对安全风险评估和审计的认识，让他们了解进行安全审计所需的准备工作、应注意的各个方面及安全审计可能得出的结果。

1.1 目的

本文件阐述信息技术安全风险评估和安全审计的一般架构。本文件应按需要与其他安全文件如《基准信息技术安全政策》[S17]、《信息技术安全指南》[G3]及相关程序等一同使用。

本实务指南旨为政府所有需要处理安全风险评估或安全审计的人员，以及为政府进行安全风险评估或安全审计的安全顾问或审计师而设。

1.2 参考标准

以下的参考文件为本文件在应用上的参考：

- 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 – Overview and vocabulary (fourth edition), ISO/IEC 27000:2016
- 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 - Information security risk management (second edition), ISO/IEC 27005:2011

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	
安全风险评估	是识别、分析和评估安全风险的过程，并决定缓解措施以降低风险至可接受水平。
安全审计	是以信息技术安全政策或标准为基础的遵行状况审计，以确定现有保护的整体情况，并验证现有的保护措施是否已经妥善地实行。

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，来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；和
- 态势认知和信息共享。

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；和
- 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引致服务中断的事件，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。

态势认知和信息共享

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. 安全风险评估与审计简介

3.1 安全风险评估与审计

安全风险评估和审计是一个持续的信息安全实践过程，以发现和纠正安全事务。如图 3.1 所示，它们涉及一系列活动。它们可以被描述为需要持续监察和控制的迭代过程的循环。 每个过程由不同的活动组成，以下为一些例子。

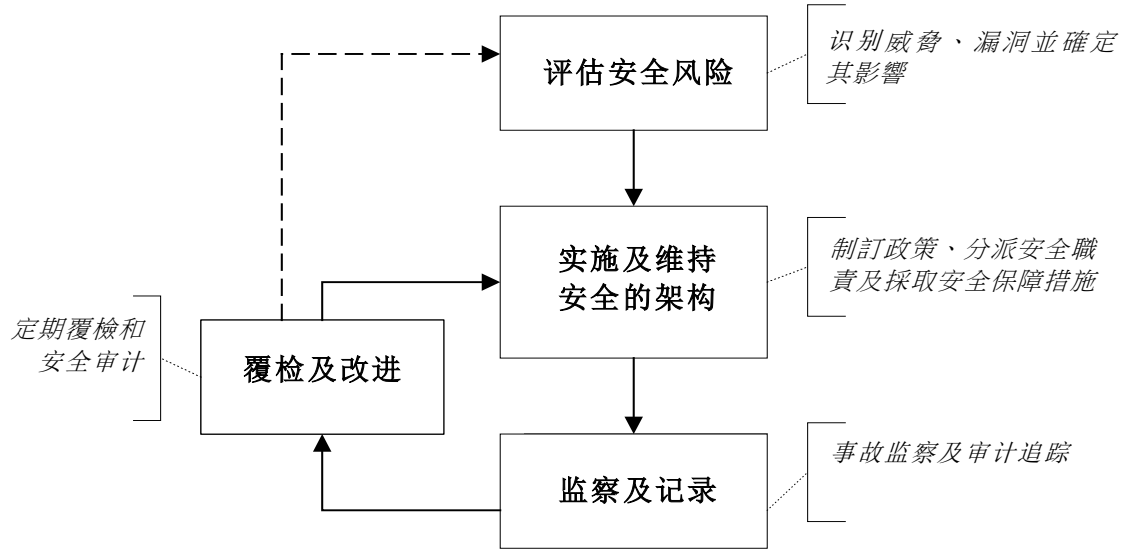

图 3.1 安全风险评估与审计的循环程序

评估安全风险是评估和识别与安全漏洞相关风险及后果的第一步，同时可为管理层提供基础，以制订具成本效益的安全计划。

根据评估结果，应采取适当的安全保护和保障措施，以维持安全的保护架构，其中包括制订新的安全要求、修订现时的安全政策和指南、分派安全职责和采取安全技术保护措施。

通过实施安全架构，还需要持续的监察及记录，以便妥善安排处理安全事故。此外，日常操作如需使用资源或信息以作用户访问的尝试和活动，应进行适当的监察、审核和记录。

评估后要对措施的遵守情况，进行周期性覆检和重新评估，以确保安全控制措施获切实执行，达到用户的安全要求，并紧贴急速发展的科技和不继转变的环境。此模型有赖持续反馈和监察。覆检可透过定期安全审计进行，以找出需要改进之处。

3.2 安全风险评估与安全审计

安全风险评估和安全审计都是持续的过程，但在性质和功能方面是有所不同。

安全风险评估是识别、分析和评估安全风险的过程，并决定缓解措施以降低风险至可接受水平。安全风险评估是风险管理流程的一部分，旨在为信息系统提供适当的安全级别。它有助识别安全漏洞所造成的风险和后果，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。

对于新的信息系统，安全风险评估通常在系统开发生命周期开始时进行。对于现有的系统，评估须在整个系统开发生命周期中定期进行，或在信息技术环境有重大改变时进行。

信息安全审计是以信息技术安全政策或标准为基础的遵行状况审计，以确定现有保护的整体情况，并验证现有的保护措施是否已经妥善地实行。安全审计是持续的过程，以确保现时的安全措施符合部门的信息技术安全政策、标准和其他协议上或法律要求。

虽然安全风险评估与安全审计在某些功能上有相似之处，但两者之间有以下主要分别。

安全风险评估	**安全审计**
识别威胁和漏洞、评估所涉及的风险水平、确定可接受的风险水平和相应的风险缓解策略	确定在部门信息技术安全政策、标准和其他协议上或法律要求的安全措施有效地实行的过程
从风险角度出发，评估范围不一定与安全政策和标准相关	从遵守规定角度出发，评估根据安全政策、标准或其他预定的准则
对于新的信息系统，在系统开发生命周期的早期和系统投入生产之前进行 对于现有的信息系统，至少每两年一次或有重大变更时进行	定期审查，持续进行
可自行评估或由独立第三方完成	必须由独立第三方完成
主要成品：风险登记和风险缓解措施	主要成品：遵行要求清单

第 4 节和第 5 节会分别介绍实行安全风险评估和安全审计流程的细节。

4. 安全风险评估

安全风险评估是识别、分析和评估安全风险的过程，并决定缓解措施以降低风险至可接受水平。

系统评估程序包括识别和分析：

- 系统的所有资产和相关程序
- 可影响系统机密性、完整性或可用性的威胁
- 系统漏洞和相联的威胁
- 威胁活动带来的潜在影响和风险
- 减低风险所需的保护要求
- 适当安全措施的选择和风险关系的分析

应就系统编制完整列表及安全要求，以作为识别和分析活动的资料，使分析的结果更为有用和准确。与管理员、计算机 / 网络操作员或用户等有关各方进行访谈，亦可提供更多分析数据。视乎评估的范围、要求和方法，亦可利用自动化安全评估工具进行分析。评估所收集的资料后，呈报已发现的安全风险清单，并就各项风险而决定、推行及采用适当的安全措施。

负责分析所收集的资料及权衡安全措施工作的人员需具备深厚的专业知识和丰富的经验，应委任合资格的安全专家进行安全风险评估。

4.1 安全风险评估的好处

- 可全面和有条理地向管理层反映现有的信息技术安全风险和所需的安全保障措施
- 以合理客观的方式制订信息技术安全开支和成本预算
- 为决策和政策考虑提供不同的解决方案，使信息安全管理能够从策略性的层面推行
- 为日后比较信息技术安全措施的变化提供依据

4.2 安全风险评估频率和类别

4.2.1 安全风险评估频率

安全风险评估是一项持续进行的工作。对于一个新的信息系统，评估工作应在系统开发生命周期之初进行，以便及早识别安全风险和选择适当的安全控制。对于使用中的信息系统，必须至少每两年或于系统有重大改动时作评估，以了解信息系统存在的风险。该两年期的定义为获得批准拨款后连续两次评估工作的开始日期，或两次评估报告的发布尔日期之间的期间。这两年的间距不包括推行安全保障措施的时间。安全风险评估只能概括地揭露在某特定时间信息系统所存在的风险。对于关键业务信息系统或具高风险访问的系统，应更频密地（最好每年一次）进行安全风险评估。

4.2.2 安全风险评估类别

视乎评估的目的和范围，安全风险评估可分为不同类别，而进行的时间则视乎系统要求和资源而定。

- 高层次评估：此类评估注重以较具策略的角度和有系统的步骤，分析部门的安全状况及系统的整体基础结构或设计。在此类评估中，拥有众多信息系统的决策局 / 部门倾向于就其信息系统进行高层次的风险分析，而并非详细的技术控制覆检。此类评估亦可应用于尚处于规划阶段的系统，以便在开发系统前识别风险或覆检一般安全控制措施。

- 全面评估：一般会定期对决策局 / 部门的信息系统进行此类评估，以确保系统的安全性。全面评估可用以评估决策局 / 部门内某个特定的信息系统所存在的风险，并提供改进建议。在数据收集阶段，将会进行一般控制覆检、系统覆检及安全漏洞识别。随后应通过一个验证过程，以确保所有建议的补救措施得到切实的跟进。

- 投入运作前评估：与「全面评估」所进行的工作类似，通常会在新的信息系统推出前或原有系统出现重大功能变动后进行此类评估。对于新的信息系统，决策局 / 部门应在设计时间进行安全覆检，确保已识别所需的安全要求，并适当地引入于系统设计时间或其他阶段。应在生产前的安全风险评估中核实安全覆检的跟进行动，以确保系统在正式推出前已推行所需的安全措施及控制措施。

4.3 安全风险评估步骤

安全风险评估包括图 4.1 所示的几项主要工作：规划、数据收集、风险分析、安全保障措施识别及选择，和监察及推行。

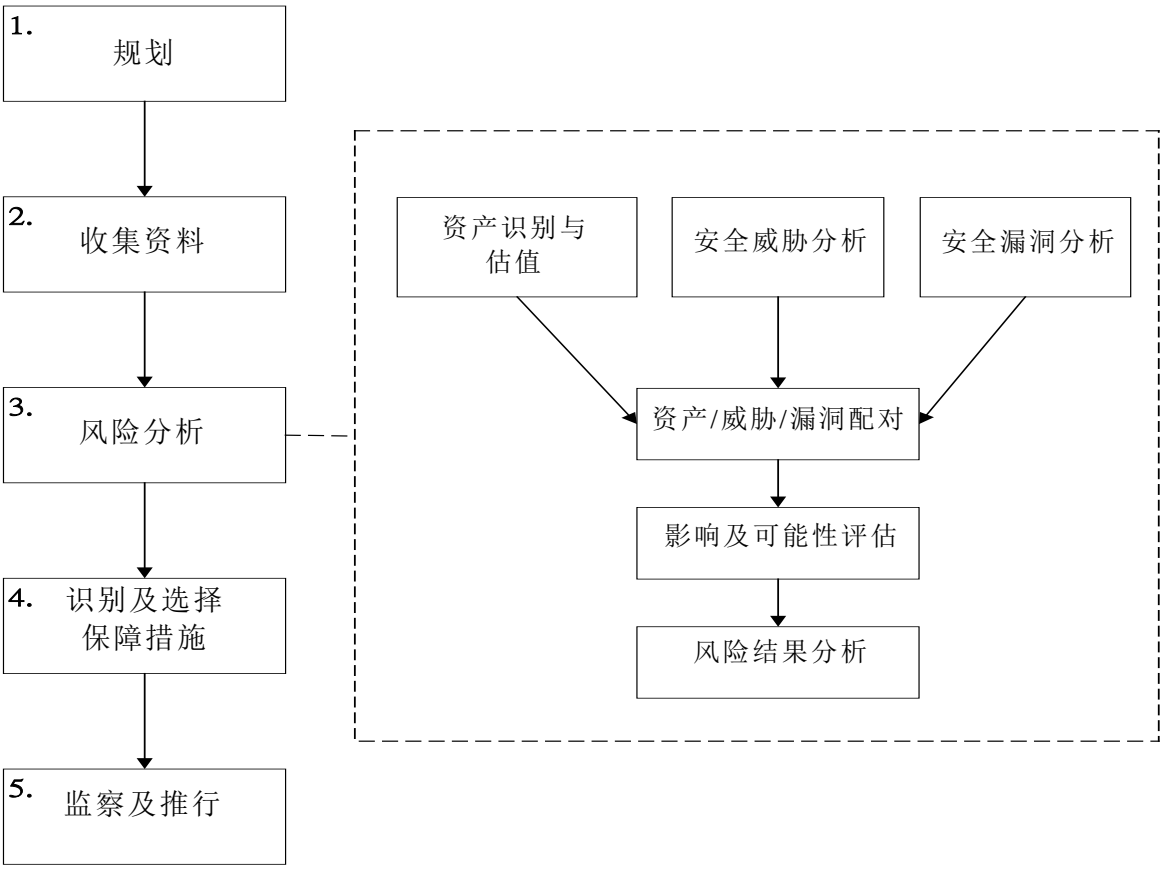

图 4.1 一般安全风险评估步骤

4.3.1 规划

在评估安全风险前，须就筹备、监察和控制等工作进行规划。其中一个建议是假如风险评估活动牵涉渗透测试或漏洞扫描，应事前通知持份者如网络小组、应用系统小组及安全事故处理小组，以避免产生过多错误警报，影响日常运作。下列为应事先界定的主要事项。

- 计划范围和目标
- 背景资料
- 限制
- 相关人士的职务和职责
- 方式和方法
- 计划规模和时间表
- 保护数据和工具

4.3.1.1 计划范围和目标

计划范围和目标可影响分析方法和安全风险评估所得的成品种类。安全风险评估的范围可涵盖内部网络与互联网的连接、计算机中心的安全保护措施，以至整个部门的信息技术安全状况。因此，相应目标可能需要识别安全要求，如内部网络与互联网连接时的保护措施、识别计算机室内潜在风险的地方，或评估部门的整体信息技术安全水平。安全要求应根据业务需要而制订（一般由高级管理层决定），以识别决策局 / 部门所需采取的安全措施。

4.3.1.2 背景资料

背景数据是指可就评估供顾问作初步参考的有关数据，例如正受评估系统的过去和现况数据、有关联的各方、上次评估的撮要数据，或即将发生并可能影响评估的改变。

4.3.1.3 限制

各种限制包括时间、财政预算、成本和科技等均应加以考虑。建议决策局／部门及早提交拨款申请，以确保安全风险评估与审计工作获得所需款项。这些限制可能影响计划的时间表和支持评估的可用资源。举例来说，评估宜需在非繁忙办公时间，甚至非办公时间进行。

4.3.1.4 相关人士的职务和职责

应小心界定参与计划各方的职务和职责。为使评估达到最佳效果，宜分派代表各个工作领域的团队或小组，分别负责指定的工作。视乎工作安排和要求，部分或全部下列人士均可参与计划：

- 系统或数据拥有人
- 信息技术安全管理员或主任
- 计算机操作人员
- 系统或网络管理员
- 应用程序或系统开发人员
- 数据库管理员
- 用户或高级用户
- 高级管理层
- 外聘承包商

4.3.1.5 方式和方法

评估方式和方法是指分析资产、威胁、漏洞和其他因素之间的关系。分析方法有许多，大致上可分为两大类：定量和定性分析。

为发挥更大效用，为评估所选的方法应能够就风险的影响和安全问题的后果作出定量报告，同时作出一些定性分析，以描述对风险减到最低的适当安全措施及其影响。下文将阐述这两种分析方法的详情。

4.3.1.6 计划规模和时间表

编定计划的时间表是评估的重要步骤之一。时间表须列明评估计划中将要进行的所有重要工作。预计的计划规模（例如计划成本和参与计划的人数）可直接影响计划时间表。计划时间表可用来控制进度和监察计划。

4.3.1.7 保护数据和工具

在安全风险评估的各个阶段，将收集大量数据和系统配置，而其中可能包含敏感数据。

因此，评估小组应确安全全地储存所收集的所有数据。在规划阶段应准备档案加密工具和锁柜 / 可上锁的工作室，以防止未获授权人士取阅敏感数据。

此外，应妥善存置、控制及监管评估工具以免遭滥用。只有评估小组内的有关专家方可运作有关工具，以防对系统造成损害。除非采取适当控制措施以防止未获授权访问上述工具，否则亦应在使用后实时将该等工具和其产生的数据删除。

完成评估程序后，将会编撰安全风险评估报告以记录发现的所有风险。如遭未获授权访问有关数据(尤其是在修正系统前)，可能会对有关决策局 / 部门构成直接威胁。因此，评估小组在编撰安全风险评估报告中及完成报告后，必须采取适当的措施保护有关报告。高级管理层亦应严格保密安全风险评估报告。最后，评估小组须将所有要求提供的数据和文件归还有关决策局 / 部门。

4.3.2 资料收集

数据收集的目的在于了解现有系统和状况，并透过分析所收集的数据 / 数据，以确认风险所在。

一般来说，不论相关数据以何种格式储存，都应予以收集。下列是一般收集的资料：

- 安全要求和目标
- 系统或网络的结构和基本设施，例如显示信息系统资产配置和互连情况的网络图
- 证据或证明文件，显示计算机室的实体环境符合根据所存放数据的保密类别而订定的实体安全要求，例如建筑署发出的认证／通知或上次安全风险评估与审计报告的相关结果
- 向公众公开或网页上发布的资料
- 硬件设备等实体资产
- 操作系统、网络管理系统及其他系统
- 数据库、档案等信息内容
- 应用系统和服务器数据
- 网络支持的协议和提供的服务等数据
- 访问控制措施
- 业务流程、计算机操作程序、网络操作程序、应用系统操作程序等程序
- 识别及认证机制
- 相关的法定，规管及合约要求以符合有关最低安全控制的要求
- 政策和指南

常见的数据收集方法一般有两种：

- 一般控制覆检
- 系统覆检

4.3.2.1 一般控制覆检

一般控制覆检是透过人手，以访谈、实地走访、文件覆检、观察等方法，以识别在现时环境推行中一般控制的潜在风险和威胁。这些控制和程序包括但不限于：

- 部门信息技术安全组织，特别是人员的职务与职责
- 管理职责
- 信息技术安全政策

- 人力资源安全，包括安全意识培训
- 资产管理
- 访问控制，例如密码政策、访问权限
- 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连续性管理
- 遵行要求

在收集数据时可采用以下方法：

- 实地走访：应安排走访数据中心、计算机室和办公室，以找出实体安全风险。此外，安全小组应在实地观察时记录有关系统操作和终端用户的行为（例如使用设置密码的屏幕保护），以复核有关安全政策是否被严格遵从。

- 小组讨论：评估小组可举办小组讨论或研讨会，以搜集有关决策局 / 部门或信息系统现时安全情况(控制或风险)的数据。视乎所欲取得的目标数据，可以任何形式及话题进行讨论。

- 与各级人员进行访谈：此外，与不同级别的重要人员或代表进行实地访谈也宜验证之前收集到的资料，从而提高所收集资料的准确度和完整性。

- 问卷调查：问卷调查或清单是有效的简单工具用来识别潜在风险。问卷调查可由安全顾问按环境的个别情况设计。

举例来说，与各级人员进行访谈的对象可包括以下人员级别：

- 高级管理层：负责作出策略性决策（例如评估范围和目标）

- 业务管理层：须了解受策略性安全更改影响的主要业务流程和程序

- 人事部人员：须识别就系统安全和使用权对人员招聘、终止雇用及转调推行的具体控制措施

- 操作和技术人员：提供技术和操作数据

就高层次评估或设计时间的评估而言，采用实地走访及问卷调查的方法未必适合或可行。因此，安全评估小组应着重透过小组讨论和与各级人员进行访谈等活动收集资料。

附件 A 所载为安全风险评估的一般提问清单。

4.3.2.2 系统覆检

系统覆检是从内部访问点，识别网络或系统的任何安全漏洞和薄弱环节。系统覆检着重不同平台的操作系统、管理和安全监察工具。

系统覆检的内容包括：

- 系统档案或记录
- 操作中的程序
- 访问控制档案
- 用户列表
- 配置设定
- 安全修补程序级别
- 加密或认证工具
- 网络管理工具
- 记录或入侵检测工具

评估小组也应找出是否存在企图入侵等异常活动。

为了更有效及全面地收集上述数据，可在目标主机上采用因应个别需求而设计的自动化脚本及／或工具，藉以取得有关系统的具体数据。这些资料将会用于稍后阶段的风险分析。

在覆检后，应适当地记录和在设计时间或其他阶段处理所识别的风险和建议。

当有需要时，应进行技术性漏洞测试如漏洞扫描、渗透测试和应用程序原始码检测，以识别网络或系统的漏洞和弱点。在进行漏洞扫描及／或渗透测试前，评估小组应就范围、可能的影响、及回退／复原程序得到决策局／部门的同意。如果涉及关键业务系统，则应以业务连续性计划及运作复原计划为基础。

在适当情况下，应进行网络、主机及系统的漏洞扫描以覆盖至少以下内容：

- 网络层面试探 / 扫描和发现
- 主机漏洞测试和发现
- 系统 / 应用程序（包括网上系统／应用程序）扫描

评估小组应覆检是否已对所有适用及已知的漏洞，包括但不限于由政府计算机安全事故协调中心所发出的所有相关安全警报，安装修补程序或采用替补的措施。

对于面向互联网并处理保密数据的网上应用系统、设有输入字段的网站或关键业务系统，亦应进行网页渗透测试。

有关漏洞扫描及 / 或渗透测试的详情，请参考第 4.3.3.3 节 – 安全漏洞分析。

投产前的安全风险评估应核实开发小组已完成应用程序原始码检测，以确保所需的安全措施和控制措施均已在系统内妥善推行。

对于高层次评估或设计时间的评估，实地走访和问卷调查方法有时可能不适用或不可行。在这种情况下，安全评估小组应集中从各项活动（如小组讨论和多层次访谈）收集资料作补充。

附件 A 列出一般安全风险评估的提问清单。

4.3.3 风险分析

风险分析有助厘定资产价值及其相关风险。应进行各方面的风险分析，包括但不限于以下范畴：

- 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
- 信息技术安全方面的业务连续性管理

风险分析程序一般可分为上文图 4.1 所示的子程序：

- 资产识别与估值
- 安全威胁分析
- 安全漏洞分析
- 资产 / 威胁 / 漏洞配对
- 影响及可能性评估
- 风险结果分析

下文将概括阐述风险分析子程序。

此外，决策局 / 部门在分析与电子服务(包括政府与市民(G2C)和政府与雇员(G2E)应用系统)登记和认证程序有关的风险时可参考《电子认证风险评估参考架构》中的保证模式。

4.3.3.1 资产识别与估值

安全风险评估范围内的所有资产必须予以识别，包括数据、服务、声誉、硬件和软件、通讯、界面、实体资产、支持设施、人员和访问控制措施等有形和无形资产。

数据分类是评估程序的关键步骤，而各项资产可归入不同的类别，例如资产可归类为程序、应用程序、实体资产、网络或某类数据。归类的目的是反映这些资产对评估对象系统或领域的重要性。

值得注意的是，资产估值法将会因应采纳的分析方法不同而各不相同。风险分析法将在第 4.3.3.6 节 – 风险结果分析中阐述。

资产价值可以下列方式表达：

- 有形价值，例如信息技术设施的重置成本、硬件、软件、系统数据、媒体、供应器、档案，以及支持系统的信息技术人员
- 无形价值，例如商誉和服务质量的改善
- 信息价值，例如机密性、完整性及可用性
- 资产所储存、处理或传输数据的数据分类

资产识别与估值是制备资产清单的先决工序。资产列表以有形价值和无形价值反映资产的相应价值(如有)，或以机密性、完整性及可用性等显示资产的信息价值。列表所列的资产价值如越需精确，完成资产识别与估值工序所需的时间也越长。

资产清单包括但不限于：

- 信息资产的名称和种类
- 资产的实体位置
- 储存媒体和销毁储存 / 处理资料前的保留期
- 储存 / 处理数据的性质，例如是备份还是正本
- 显示资产重要性 / 价值的指针，例如敏感程度、操作需要或关键性
- 传入 / 发出的信息流通，例如经互联网、电邮、拨号调解器或其他电讯媒介连接的传输信息模式
- 已安装的操作系统和软件
- 开发和维修费用
- 各项已识别的资产价值
- 资产所储存、处理或传递数据的数据分类

4.3.3.2 安全威胁分析

安全威胁是指可能会为信息资产、系统及网络的机密性、完整性及可用性带来负面影响的潜在事件或任何情况。安全威胁分析宜不时修订，以反映信息资产所面对的任何新潜在威胁。

安全威胁源自：

- 人为错误
- 心怀不满的雇员
- 恶意或粗心大意的人员
- 滥用系统及计算机资源
- 计算机诈骗
- 盗窃
- 商业间谍
- 自然灾害

安全威胁分析的目的是找出安全威胁，并厘定发生安全威胁的可能性及其破坏系统或资产的潜力。系统误差或控制记录可转化为安全威胁数据和统计数字，所以是有用的数据源。

安全威胁可分为三大类：

- ***社群威胁***：与人为因素直接相关的蓄意或无意安全威胁，例如人为错误、遗漏或疏忽造成的结果、盗窃、诈骗、滥用、损害、破坏、泄漏及窜改数据
- ***技术威胁***：因技术问题导致的安全威胁，例如程序错误、设计瑕疵、通讯线路（例如电缆）的破损
- ***环境威胁***：因环境灾害导致的安全威胁，例如火灾、水浸、停电、及地震

4.3.3.3 安全漏洞分析

安全漏洞是指于操作、技术和其他安全控制措施和程序中能够令安全威胁有机可乘，以致资产因而受损的薄弱环节，例如第三方拦截传输中的数据，未获授权访问数据等。

安全漏洞分析是指找出和分析系统及环境中的安全漏洞。安全漏洞分析强调系统化地衡量这些漏洞。

各个漏洞均可评定为不同级别或程度（例如高、中、低）以反映其重要性。而重要和关键资产必须先行确认。

识别安全漏洞是在自动化工具或程序的辅助下，采用以下一种方法找出网络的安全漏洞：

(i) 安全漏洞扫描

评估小组可使用自动化安全漏洞扫描工具进行安全漏洞扫描，从而快速找出目标主机或网络设备存在的安全漏洞。与抗恶意软件方案相类似，扫描工具安装在评估小组的计算机上，并需在使用前定期更新漏洞标识符档案。根据用户要求，会对单个或一组主机 / 网络进行已知安全漏洞扫描服务（例如系统容许匿名档案传送规约、电邮转递）扫描，以确定是否存在任何安全漏洞。

在安全漏洞扫描过程中，由于自动化漏洞扫描工具可产生大量系统要求，故接受扫描的各目标组群的系统和网络的性能可能受到影响。评估小组应与系统和网络管理员合作制订计划，以使安全漏洞扫描过程中发生服务中断的可能性降至最低。

此外，值得注意的是，自动化扫描工具找出的安全漏洞，在该系统环境中未必是真的安全漏洞。举例来说，由于可能已采取辅助控制措施，故自动化扫描软件标记的某些「安全漏洞」实际上未必会成为安全隐患。因此，此测试方法可能会发出虚假警报，故评估小组须作出专业判断以确定所发现的安全漏洞是否对系统有所影响。

网络安全漏洞扫描是在短时间内收集漏洞数据的有效方法。与渗透测试不同，网络安全漏洞扫描并无渗透入网络内部，亦无尝试利用发现的安全漏洞测试网络。因此，倘需要进行更为深入的安全分析，可采用渗透测试。

应用程序如网上应用程序或流动应用程序，在安全漏洞被利用前，应该先进行应用程序安全漏洞扫描，以找出安全漏洞。

(ii) 渗透测试

渗透测试可在内部或从外部进行。渗透测试以人手程序，并辅助以可安装在便携式计算机的自动化工具，来扫描网络或系统，以得出连接工作站和服务器的网络图，同时尝试渗透被测试的网络和系统，在网络和系统内部或从外部找出安全漏洞。

渗透测试也可能包括与用户进行访谈和运用不同的黑客入侵技巧测试系统或网络。在进行入侵测试前，必须全面地计划和商定具体的入侵程度和种类。入侵测试宜在访问某系统后，或在进一步深入分析被渗透的系统后停止。在决定进行入侵测试前，应寻求服务供货商或安全评估小组的建议。若要进行外来的道德黑客入侵，应事先解决法律上的问题。

渗透测试的目的包括但不限于：

- 测试系统抵御蓄意攻击的能力，以找出安全薄弱环节
- 测试及验证安全防护及控制的效率
- 测试侦测及应对攻击的防御能力

有关描述渗透测试的一般步骤见下图 4.2：

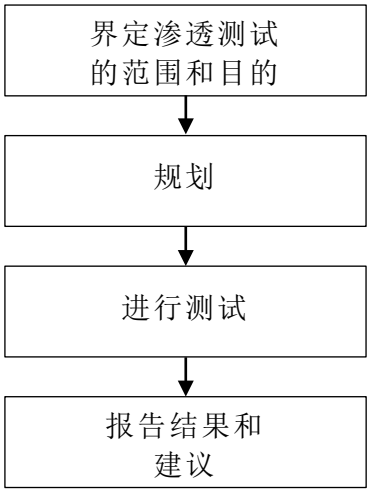

图 4.2 渗透测试的一般步骤

决策局 / 部门在进行渗透测试时应特别小心，因为该测试可能会给系统造成与真实攻击类似的影响，例如服务中断、未获授权访问或未获授权修改数据等。因此，在进行渗透测试之前，决策局 / 部门应考虑以下安全问题：

- 必须清晰界定测试的范围和目标；不得对界定范围以外的机器 / 系统进行测试。
- 进行渗透测试的服务供货商应与系统拥有人讨论及得到其准许，决定进行入侵攻击、暴力攻击及拒绝服务攻击是否适当及其影响。
- 服务供货商须签署不可向外披露数据协议，以保障系统内数据的保密或机密性。
- 只委聘信誉卓著而且纪录良好的服务供货商，并考虑对服务供货商进行背景和资格审查，以确保有关供货商具备所需的经验和专业知识。
- 由于渗透测试可能会影响目标系统中数据的完整性，所以必须为目标系统制作最新的完整系统备份。
- 清楚界定「达成任务」的条件，例如将档案放入指定目录、取得某些测试帐户的密码、访问到拥有妥当访问控制保护的指定网页等。不得修改或删除生产数据。
- 向服务供货商提供联络人名单（例如系统拥有人、信息技术管理员），在突发事件发生时作联络之用。如在测试过程中出现任何突发事件，服务供货商应联络有关人员，汇报情况。
- 取得服务供货商的联络人名单，以在必要时实时停止所有测试。
- 在进行渗透测试之前，知会并警示安全监控供货商，除非测试旨在评估安全监控供货商监控的效能。
- 事先取得将进行测试的机器的源互联网协议地址，以便透过检查和比较入侵检测 / 防御系统记录以判断是否遭受真实攻击。
- 考虑安排渗透测试在非繁忙工作时间进行。
- 确保服务供货商即使可成功访问用户数据，亦不会修改任何数据。

渗透测试示例如下：

- 远程互联网防火墙渗透测试：互联网协议地址试探、传输控制协议或用户数据报协议试探、基于协议的拒绝服务攻击，例如互联网控制讯息协议瘫痪、域名称服务伪冒，和基于服务的渗透测试，例如电邮服务器的渗透测试、暴力密码攻击和电邮轰炸
- 实地防火墙渗透测试：小包嗅探、互联网协议地址伪冒、源路由小包及劫持通讯对话
- 拨号网络渗透测试：暴力密码攻击和拨号式扫描
- 应用系统渗透测试：包括但不限于配置及使用管理测试、认证测试、

身分管理测试、对话管理测试、错误处理等

须对这些自动化工具推行严格的访问控制，以限制任何未获授权访问和使用。由于利用这些工具能够对系统、网络或网上应用程序发动拒绝服务攻击等模拟攻击，在使用自动化工具时，安全评估小组和系统管理员应密切监视这些工具。

有关渗透测试的详情，请参阅《渗透测试实务指南》。

4.3.3.4 资产 / 威胁 / 漏洞配对

将威胁与资产和漏洞配对有助确认资产、威胁和漏洞可能形成的各种组合。各个威胁均能够与一个特定漏洞，甚至多个漏洞配对。除非漏洞令威胁有机可乘，否则威胁并不能对资产构成风险。

在进行风险结果分析前，应减少各种可能形成的组合。部分组合可能毫无意义或根本不能形成。资产、威胁及漏洞三者之间的关系对分析安全风险至关重要。计划范围、财政预算和其他限制等因素，也可能影响配对的深度和广度。

4.3.3.5 影响及可能性评估

为资产、威胁和漏洞配对后，便能够确定影响和可能性。

(i) 影响评估

影响评估（或称影响分析或后果评估）即估计可能发生的整体破坏或损失的程度。评估的影响包括收入、利润、成本、服务水平和政府声誉、对相关系统机密性、完整性及可用性的损害。此外还须考虑能够承受的风险水平，以及哪些资产会如何和何时受到这些风险影响。安全威胁的影响越严重，风险也越高。

(ii) 可能性评估

可能性评估是对安全威胁发生频率的估计，即发生的或然率。可能性评估须观察影响风险发生可能性的环境。一般而言，一个系统的漏洞令某一威胁有机可乘的可能性可根据不同情况衡量，如系统可供访问的程度和获授权用户的人数。可访问系统的程度可能受实体访问控制、系统配置、网络种类、网络布局和网络界面等多种因素影响。与互联网连接的系统比内部系统的漏洞更容易令威胁有机可乘。前者的获授权用户（即公众）人数亦可能远多于后者，内部系统的用户人数通常有限。与用户人数成千上百的系统相比，只有一名用户的系统受到威胁的机会显然较

小。能够访问系统的人数越多，确保个别用户只进行获准操作的难度便越大。正常来说，当获授权用户的人数愈多，漏洞被利用的可能性便愈高。

可能性的高低可视乎发生次数的多寡（例如每天一次、每月一次及每年一次）而定。安全威胁的可能性越高，风险也越高。举例来说，如应用软件有一个众所周知的安全漏洞，乘此漏洞发生蓄意社群威胁的可能性就很高。如果受影响的系统为关键系统，则影响也很严重。由此得出的结果是该威胁具有高风险。

厘定已确认的各个风险的影响和可能性，便能够估计整体的风险水平。在估计风险水平时应订明假设。

4.3.3.6 风险结果分析

风险结果可利用不同的方式和方法分析：定性、定量和矩阵法。

(i) 定性和定量法

定性法是根据经验和判断，以描述性、文字等级或排序反映重要 / 严重程度的方法，例如过去的经验、市场调查、行业实务及标准、调查、访谈和专业人士 / 专家的判断。定性法须主观地为风险评级，例如按高、中、低评级；由 1 至 5 按序排列；或从重要程度最低向最高排列等。定性法较为主观。

举例来说，资产的价值可以重要程度表达，例如不重要、重要和非常重要。

定量法是利用数字数据得出百分比或数值的方法，例如成本 / 效益分析。定量法所需的时间和资源均多于定性法，因为定量法需要考虑并为每个可能的因素（即资产、威胁或漏洞）评级。

举例来说，资产的价值可以购入价或维修费用等金钱价值表达。安全威胁的频率可以发生率表达，例如每月一次或每年一次。

定性法一般在初步筛选时使用，而定量法则用来对一些关键因素进行更详尽和具体的分析，以及进一步对高风险领域进行分析。

(ii) 矩阵法

矩阵法以三种不同的严重程度（高、中、低），记录和估计安全保护措施的三个关键要求：机密性、完整性及可用性。风险水平可根据各风险因

素的严重程度排列次序。风险诠释应局限于最重要的风险，以节省整体人力物力和减低复杂程度。

表 4.1 所示为某个特定安全威胁对某功能或某资产的风险分级矩阵示例。影响和可能性栏内的数字显示了风险级别（3——高、2——中、1——低）。由于风险水平是影响值乘可能性值的积，所以风险水平值可介乎 1 至 9 不等（9——高、4 及 6——中、1 至 3——低），不包括 5、7、8（因为影响值乘可能性值的积不可能等于 5、7、8）。利用风险分级矩阵便能够将各个安全威胁归入某个整体风险水平级别。

风险类别	**影响** **（高、中、低）**	**可能性** **（高、中、低）**	**风险水平=** **影响 X 可能性** **（高、中、低）**
机密性	3	2	***6***
完整性	3	1	***3***
可用性	2	1	***2***
整体	***3***	***2***	***6***

表 4.1 风险分级矩阵示例

表 4.1 备注：

- 影响（高）：非常重要：可对机构造成重大损失和严重破坏；造成极大的、灾难性或严重的长期破坏 / 干扰

  例如拒绝服务，未获授权访问系统

- 影响（中）：重要：对机构不利的中度损失；造成严重的短期破坏 / 干扰或有限的长期破坏 / 干扰

  例如入侵者可收集系统的关键数据，以便在未获授权的情况下访问，或展开进一步攻击

- 影响（低）：不重要：对机构损害轻微，或不构成损害的轻微损失；造成有限的短期破坏 / 干扰

  例如入侵者可能取得非关键数据

- 可能性（高）：在大部分情况下预期会发生
- 可能性（中）：偶尔会发生
- 可能性（低）：在某特定时间或在特殊的情况下发生
- 风险水平（高）：对风险的承受能力低，即需要最高级别的安全保护措施
- 风险水平（中）：对风险的承受能力一般

- 风险水平（低）： 对风险的承受能力较强
- 整体结果 在各级风险类别中，最高安全风险水平

将风险类别再细分为子类别，再附上更多风险水平的加权数值，便能够进一步扩充上列矩阵。

确定风险水平后，便能够为已确认的各项资产编制技术、操作和管理要求清单。由于不可能完全杜绝风险，有关清单(如表 4.2 所示)可成为承受、减低、避免或转介风险决策的依据。

评估结果	可选方案	描述
• 后果轻微 / 可能性低 • 可用性或其他因素比安全因素重要	承受风险	承担责任
• 不可承受的高风险	减低风险	减轻后果或减低可能性，或一并减低
• 风险过高，或费用过高，因而无法减低，也无法管理	避免风险	采用其他方法，或不再进行可能引发风险的工作
• 另一方愿意承受风险 • 另一方控制风险的能力更强	转介风险	将部分或全部风险责任转移给另一方

表 4.2 风险方案表

对于选定的任何方案，必须向管理层提出如何实施所选方案的建议。此外，如果选择减低风险，还须建议保障和安全措施。

然后按风险的重要性和潜在影响，为各个风险排列先后次序。一般而言，安全风险水平越高，排列先后次序时便有较大的优先权。换言之，有较大优先权的风险一般是无法承受，以及需要管理层高度关注的风险。

4.3.4 识别及选择安全保障措施

在覆检安全风险评估的结果后，便能够识别及评估安全保障措施的效用。安全评估小组会建议采取可行的安全保障措施，将已找出的威胁和漏洞的可能性及其影响减至可接受的水平。

4.3.4.1 常见安全保障措施类别

安全保障措施可以是快速修复在现行系统配置所发现的问题程序，也可以是系统升级计划。安全保障措施可以是技术性或程序性的控制措施。

安全保障措施一般可分为三个常见类别：

- 杜绝入侵途径：完全杜绝未获授权者访问关键资源
- 巩固防御能力：使未获授权者难以访问关键资源
- 系统监察：协助实时、准确地侦测和应付攻击

安全保障措施包括：

- 制订／改善部门信息技术安全政策、指南或程序，以确保达到安全成效
- 因应在安全风险评估所发现的薄弱环节重新配置操作系统、网络构件和设备
- 运用密码控制程序或认证机制，确保采用强化密码
- 运用加密或认证技术保护数据传输
- 改进实体安全保护
- 制订安全事故处理及报告程序
- 提高人员的安全意识，并为他们提供培训，确保人员遵守安全要求

4.3.4.2 确定和选择安全保障措施的主要步骤

选择适当的安全保障措施，有赖负责选择的人员精通系统知识和专业技术，所以并不简单。管理风险的成本须与风险水平相称，即为某特定资产减低风险的成本，不应超过有关资产的总值。

下列为确定和选择安全保障措施的主要步骤：

- 为各目标漏洞选择适当的安全保障措施
- 确定各安全保障措施的相关成本，例如开发、推行和维修成本
- 将安全保障措施／漏洞组合与所有安全威胁配对，即在保障措施与威胁之间建立关系
- 厘定及量化安全保障措施的影响，即采取选定的安全保障措施后得以减低的风险幅度

安全保障措施可能涉及实体、管理、程序、操作和技术安全保障措施等的不同组合。进行分析能够为不同的情况选定最适当的组合。

一项安全保障措施可能减低多项威胁带来的风险，但有时采取多项安全保障措施却只能够减低一项威胁带来的风险。因此，将所有安全保障措施整合，能够显示减低全部风险的整体效益。

在采取安全保障措施前，应测试采用不同措施的影响，为此，选择程序可能要进行数次才能掌握建议的更改对风险结果的影响。

除安全风险评估找出的因素外，选择安全保障措施时还须考虑其他因素。

例如：

- 组织因素，例如部门的目标和目的
- 相关的法定、规管及合约要求
- 文化因素，例如社会习俗、信仰、工作风格
- 质量要求，例如安全程度、可靠程度、系统性能
- 时间限制
- 支持服务和功能
- 技术、程序和操作要求和控制措施
- 市面上现有的技术

4.3.5 监察与推行

应妥善地以文件记载风险评估结果。这些文件可供审计安全风险评估程序之用，并有助持续监察和覆检。

必要时应重新进行评估。另一项重要工作是追踪环境转变和已发现风险及其影响之优先次序的变化。安全审计是覆检安全措施推行情况的方法之一。

应明确界定、覆检和分派操作员、系统开发人员、网络管理员、数据拥有人、信息技术安全主任和用户等相关人士的职务和职责，以配合推行安全保障措施。管理层应拨出专用资源，并支持对推行安全保障措施的监察和控制。

4.4 常见的安全风险评估工作

下列是安全风险评估的部分常见工作，以供参考，实际工作将视乎评估范围和用户要求而定。

- 识别可能影响信息技术和安全整体方向的业务需要及修订要求。
- 就每个信息系统的操作，定出及记录所有适用的相关法定、规管及合约要求。
- 分析资产、威胁、漏洞、其影响和可能性。
- 评估计算机设备和其他网络构件的实体保护措施。
- 对网络结构、协议和构件进行技术和程序覆检与分析。
- 覆检及检查远程访问系统、服务器、防火墙和外部网络连接（包括客户互联网连接）的配置、实施和使用情况。
- 覆检密码和其他认证机制。
- 覆检机构内部人员目前的安全意识和投入感。
- 覆检有关供货商和承包商所提供服务或产品的协议。
- 提出切实的技术建议，以处理所发现的漏洞，并减低安全风险的水平。
- 执行自动应用程序原始码扫描，以加强各决策局／部门所开发应用程序的安全保障措施。

4.5 成品

安全风险评估在进行的各个阶段，可能提交不同的评估成品。下表（表 4.3）所示为不同成品的清单。**附件 B** 载列了不同成品内容的示例，以供参考。

	工作	成品	简介
1	确定安全要求	安全要求报告	就已确定的资产、威胁、漏洞及其影响和可能性，阐述用户安全要求的报告
2	安全风险评估	安全风险评估报告	就已确定的资产、威胁、漏洞、其影响及改进建议或补救措施，阐述安全风险评估结果的报告
3	覆检现行的安全政策、指南和程序	崭新／经修订的安全政策、指南和程序	一份或一套安全相关内容文件，以控制安全保护措施在评估领域的推行

表 4.3 成品列表

5. 安全审计

安全审计是以信息技术安全政策或标准为基础的遵行状况审计，以确定现有保护的整体情况，并验证现有的保护措施是否已经妥善地实行。它的目标是确定当前环境是否按照预定的安全政策要求受到适当的保护。安全审计应定期执行，以确定符合安全政策和有效地实行安全措施。

安全审计需要安全政策和标准、审核列表和物品列表，并可能涉及不同领域，如网上应用系统、网络架构、无线通讯等。附件 C 列出不同的审计领域。附件 D 提供不同安全范畴的审计检查列表样本。附件 E 提供作为遵行证据的已记录数据样本列表。安全审计可能涉及使用不同的审计工具和不同的审查技术，以揭示安全不合规处和漏洞。在审计过程后会准备一份审计报告，用以指出当前的保护措施与安全政策和指南所规定的要求之间的符合情况和差距。

在拣选审计师和进行审计工作时，必须确保审计过程客观而公正。作为一般原则，审计师不得审核本身有份参与的工作。安全审计师可以覆检与系统相关的文件，以了解是否存在不足或不合规之处。

安全审计的主要目的在于：

- 检查安全措施是否符合现行的安全政策、标准、指南和程序
- 识别不足之处，并检验现行政策、标准、指南和程序的成效
- 识别及覆检相关法定、规管及合约要求
- 识别、分析并了解现存的漏洞
- 覆检现行的操作、行政和管理事项的安全控制措施，并确保在操作、行政和管理等方面贯彻落实有效安全措施并符合最低安全标准
- 为改进提供建议和纠正措施

5.1 审计频率及时机

5.1.1 审计频率

安全审计是持续进行的活动，而非一次性的事件。安全审计应定期进行，以确保符合安全政策、指南和程序，并确定将风险减至可接受水平所需的最低要求控制措施。值得注意的是安全审计只能概括地揭露在某特定时间所发现的安全漏洞。

5.1.2 审计时机

安全审计应在不同情况下进行，而进行的确切时机则视乎系统要求和资源而定。

- 安装 / 升级后审计：在启用崭新或经过重大升级的系统前，为确保符合现行政策、指南及配置标准的审计
- 定期审计：定期（例如每年一次）以人手或使用安全相关的工具自动进行审计，确保已采取最低限度的控制措施以侦测及处理安全漏洞
- 抽样审计：随机检查，以反映实际作业情况
- 晚间或非办公时间审计：在非办公时间或晚间进行审计以减低相关风险

5.2 审计工具

审计工具中有不少自动化工具可帮助找出安全漏洞。选择采用何种审计工具则视乎安全需要和监察工作负荷的影响而定。

举例来说，有些安全扫描工具可透过扫描和发动仿真攻击，查出网络（基于网络的扫描工具）或特定主机（基于主机的扫描工具）目前的存在安全漏洞。检查结果会记录在审计报告中以供进一步分析。

这些市面上供应的现成工具可与安全审计师自行开发的工具一并使用。安全审计师还可能使用在黑客圈子中最新的工具，以模拟层出不穷的攻击活动。

社交工程攻击和审计列表等人力覆检技术也可用来对机构内部的整体安全意识水平进行非技术覆检。

5.3 审计步骤

一般而言，安全审计可分为以下几个步骤：

- 规划
- 收集审计资料
- 进行审计测试
- 报告审计结果
- 保护审计数据和工具
- 改进与跟进

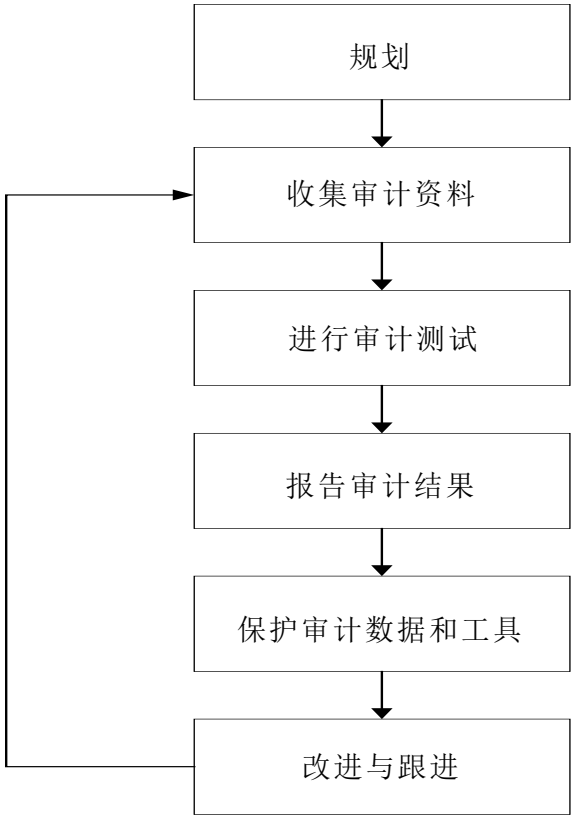

图 5.1 一般审计步骤

5.3.1 规划

规划有助厘定和挑选有效益和有效率的方法，以进行审计和收集所需的所有数据。规划所需的时间视乎审计的性质、范围和复杂性而定。

5.3.1.1 计划范围和目标

审计应有清晰的范围和明确的目标。在进行审计前，应与安全审计师确认和商定用户要求。

安全审计的范围包括：

- 互联网安全
- 内部网络的一般安全
- 关键任务系统
- 主机安全
- 网站服务器、电邮服务器等网络服务器的安全
- 防火墙、路由器等网络构件和设备
- 计算机室的一般安全
- 目录服务、邮件传递服务、远程访问服务等网络服务
- 系统文件和记录

部分审计目标列举如下，以供参考：

- 为遵守系统安全政策和程序提供证明
- 检验和分析系统的安全保障措施，以及操作环境
- 评估安全机制设计在技术和非技术方面的实施情况
- 证实所有安全功能的欠缺、恰当或不当整合和操作

5.3.1.2 限制

应为审计预留充裕时间，以确保能依时完成所有的测试。有些时候，当进行审计时，系统或网络须脱机或暂停运作，以致可能发生服务中断的情况。在展开安全审计工作前，必须为目前的配置和数据进行备份及复原处理。

5.3.1.3 职务和职责

与进行安全风险评估类似，应小心及清楚界定各参与者的职务和职责。有关一般参与计划的成员可参阅第 4.3.1.4 节 – 相关人士的职务和职责。

尤其是，安全审计师在获委聘后，应计划进行安全审计工作前的预备事项：

- 通过翻查文件、访谈、会议和人力覆检确定和核实目前的环境
- 确定与审计相关的重要领域或操作事项
- 确定可能影响审计的一般控制措施
- 确定和估计审计所需的资源，例如审计工具和人力资源
- 确定审计所需的任何特殊或额外处理程序

安全审计必须在妥善的监控和授权下进行。决策局 / 部门与安全审计师之间必须建立沟通渠道。

另一方面，应先考虑以下两方面事项：

- 安全审计师的独立性

  应就安全审计的性质，考虑所委聘的安全审计师是否适当的人选。选择独立和可信赖的第三方作为安全审计师可确保审计观点正确、公平和客观。委聘内部或外部安全审计师的工作应慎重计划，尤其是委聘处理保密数据的安全审计师。在审计过程中，拣选审计师必须客观。审计师不得审核本身有份参与的工作。

  安全审计是持续发现和纠正安全问题的过程。应避免长期聘请同一安全审计师，以避免独立性下降，以及避免由于使用相同方法重复进行审核而导致的安全覆检盲点。

- 人手编排

  安全审计应由具备足够技术和经验的审计师，在系统管理员的陪同下进行。事先应清晰界定和分派参与审计各方的职务、职责和责任。

5.3.2 收集审计资料

对于需要收集多少数据、收集哪类数据，以及如何过滤、储存、访问和覆检审计数据和记录，都必须明确厘定。

收集数据的数量取决于审计范围、目标及数据可用性。

收集资料须慎重规划。收集数据的安排必须符合政府法例和规例，而且必须避免挑起或引发其他潜在的安全威胁和漏洞。必须收集、妥善保存和保护所有需要的数据，以防止未经授权的访问。

审计资料可以多种不同的方式储存，例如，

- 记录档案，例如系统启动及关闭的数据、用户的登入和退出、曾执行的指令、违反访问控制的事件、帐户和密码更改。
- 记录，例如审计追踪、日志、摘要、所有事项的详尽报告、统计报告或例外报告。
- 存储媒体，例如光盘。

除收集电子数据外，部分实体事件或人为工作亦应妥为记录，以供将来参考之用。

这方面的工作包括：

- 计算机设备维修保养工作，例如日期、时间、提供支持的供货商数据及工作情况
- 变更控制和管理事项，例如更改配置、安装新软件、数据转换或更新修补程序
- 安全审计师或访客等外部人士的亲身实地走访
- 政策和程序更改
- 操作记录
- 安全事故记录

一般来说，收集审计数据的步骤可能会遵从安全风险评估所采用的数据收集技术。但是，安全审计的目的并非评估操作环境所存在的风险，而是覆检操作、行政和管理方面的现有安全控制，以及确保符合既定的安全标准。收集审计数据或证据旨在证实有否采纳适当的安全控制并已妥善执行。有关数据收集技术的详情，请参考第 4.3.2 节 – 资料收集。

5.3.3 进行审计测试

经过全面的规划和数据收集后，安全审计师可进行：

- 根据既定的审计范围，对现行的安全政策、标准或指南进行的一般覆检
- 对安全配置的一般覆检
- 利用不同的自动化工具进行诊断覆检及 / 或渗透测试的技术性调查

视乎审计范围，安全审计所涉及的系统或网络也各有不同。

附件 C 所载为不同审计领域的目的和范围。

5.3.4 报告审计结果

安全审计报告须在完成审计工作后提交。安全审计师应分析审计结果并提交反映目前安全状态的报告。为了去除不适用的结果和误报，应加以分析由扫描工具产生的报表。严重程度可能要因应决策局 / 部门的个别环境情况而作出调整。

有关审计报告须可让信息技术管理人员、行政管理人员、相关系统管理员和系统拥有人、及审计组和控制组人员等不同人士看懂。

有关安全审计报告建议内容，请参阅**附件 B**。

5.3.5 保护审计数据和工具

在整个安全审计的各阶段中，妥善保障审计数据和工具是不可缺少的。

审计数据和所有与审计相关的文件须予以适当保密分类，并根据其保密级别受到保护。

审计工具应妥善备存、控制及监察以免被滥用。审计工具应只由安全审计师在受控制的环境下使用。除非已采取适当的控制措施保护审计工具以防未获授权访问，否则在使用后应立即移除审计工具。

安全审计师在完成审计工作后，必须向有关各决策局 / 部门归还所有审计资料。有关归还数据的安排必须在委聘安全审计师前，与安全审计师达成协议。

5.3.6 改进与跟进

如果需要采取纠正措施，部门应分拨资源，以确保尽快作出改进。如有任何不合规之处，应通知系统管理层。有关跟进工作的详情，请参阅较后章节。

6. 服务的先决条件和一般工作

6.1 假设和限制

在进行安全风险评估或审计时，应作若干假设：

- 时间和资源有限
- 目的在于尽可能减低及控制安全风险

6.2 用户的责任

由外聘人士进行安全风险评估或审计时，决策局 / 部门应配合并负责下列各项工作：

- 对提供服务的供货商和安全审计师进行背景和资格审查，以确保有关供货商和安全顾问 / 审计师具备所需的经验和专业知识
- 在展开任何评估或审计活动前，编制一份协议予提供服务的供货商签署。协议内包括但不限于免责声明、服务详情及不可对外披露数据声明。编制协议的工作对决定进行外部渗透测试（例如拨号式扫描或从互联网模拟黑客入侵内部网络）尤为重要
- 调派人手担任与供货商联络的第一（及第二）联络人
- 向供货商提供联络人名单，以便有需要时在办公及非办公时间联络
- 保持合作开放的态度。如确实有安全需要，应认同评估结果，并制订改善计划
- 只开放进行评估所需的系统、网络或计算机设备的实体和逻辑访问权，并保护可能受评估服务影响的所有资产
- 向供货商索取有关在测试时网络、服务或系统所受影响或损害程度的正式通知，以便在测试前准备好复原计划和适当的事故处理程序
- 在合理的时间内回复安全顾问 / 审计师的查询
- 提供足够的办公地方和办公室设备，让供货商能够提供服务；宜向供货商提供限制出入的办公地方
- 提供评估和审计特定领域需要的一切文件，包括日志记录政策或其审查程序，例如访问日志记录的检查
- 与供货商定期举行计划控制和覆检会议
- 当评估相关风险并准备好复原方案后，应尽早推行更改或采取改进措施，尤其是针对极高风险领域的措施

6.3 服务的先决条件

应符合的先决条件如下：

- 提供所需的所有正式或非正式已记录数据，例如网络图、操作手册、用户访问控制列表、安全政策、标准、指南和程序。有关已记录数据作为遵行证据示例列表，请参阅**附件 E**。
- 提供与评估领域相关的人员支持，例如互联网使用、防火墙配置、网络及系统管理、安全需要和要求等。
- 安排评估人员在陪同下参观场地，以收集更多评估和审计资料。
- 选择由独立的第三方进行安全审计。

6.4 安全顾问 / 审计师的责任

为决策局 / 部门进行安全风险评估或审计的安全顾问 / 审计师应：

- 具备必要的技术和专业知识。
- 了解各个工具的影响，并估计它们对决策局 / 部门有怎样的影响。
- 向互联网服务供货商、警方或其他有关方面索取适当的书面授权，这一点在进行黑客入侵测试时尤其重要。
- 不论测试成功与否均予以记录。
- 确保报告能反映决策局 / 部门的安全政策和运作需要。
- 运用良好的判断力，向决策局 / 部门实时报告在审计过程中发现的任何重要安全风险和不合规之处。

6.5 一般工作示例

事项	工作清单	工作详情
1	简介会	商定服务范围、目的和成品
2	计划规划	制订一份双方同意的提交成品时间表和服务期限
3	准备检查清单	准备一份检查清单，并得到决策局 / 部门的同意
4	准备技术性漏洞测试回退／复原程序 (例如漏洞扫描、渗透测试等)	在技术性漏洞测试及渗透测试前准备回退／复原程序
5	资产识别与估值	在协议的范围内识别和评估资产
6	安全风险评估	
	一般控制覆检	透过文件覆检、实地走访、与各级人员进行访谈、小组讨论、调查等进行一般控制覆检
	系统覆检	进行系统覆检以识别系统漏洞。按需要进行漏洞扫描、渗透测试和原始码扫描
	风险和影响分析	识别资产、威胁、漏洞及其风险和影响
	安全保障措施分析	识别和挑选可供选择的安全保障措施
	提交安全风险评估报告	编撰评估报告，列明评估结果和建议
	演示安全风险评估结果	向管理层演示评估结果和发现
7	安全审计	
	遵行要求检查	透过文件覆检、实地走访、与各级人员进行访谈、小组讨论、调查等，并根据 S17 及部门安全政策或在安全审计范围内相关的政策进行遵行要求检查
	提交安全审计报告	编撰安全审计报告
	演示安全审计结果	向管理层演示审计结果和发现
8	妥善保障资料和结果	完成安全风险评估和安全审计工作后，应妥善保障所有收集到的数据、测试结果和工具

事项	工作清单	工作详情
9	跟进行动	
	制订跟进计划	制订一个响应建议并有推行时间表的跟进计划
	保障措施推行的覆检	覆检推行保障措施后的安全状态
	提交验证报告	编撰验证报告，总结每项发现的最终结果
10	结束	
	提交验证结果	将结果提交管理层以结束该项目

表 6.1 一般工作示例

7. 安全风险评估及审计跟进

7.1 跟进的重要性

安全风险评估和审计的好处不在于所提出的建议，而在于有效地落实建议。在建议提出后，基本上由管理层负责落实建议。如果管理层决定不落实建议，便须承担相关的安全风险和不合规之处，并应为不落实建议的决策提出充分理由。

安全风险评估和审计所提建议主要涉及以下三方面：

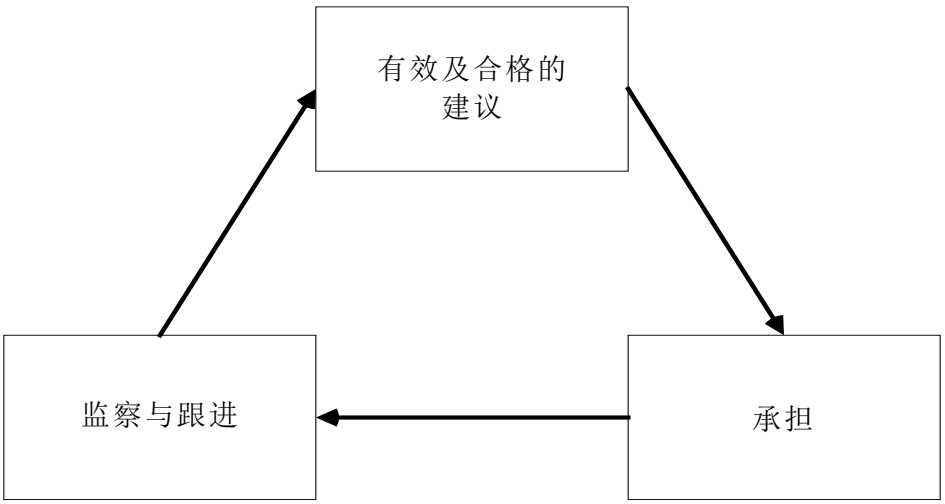

图 7.1 就建议采取的跟进行动

7.2 有效及合格的建议

安全顾问 / 审计师必须提出有效及合格的建议，这些建议应符合以下条件：

- 明确清晰、容易理解和可识别
- 具说服力、证据充分
- 具重大意义
- 切实可行

此外，安全顾问 / 审计师的建议应针对问题的真正成因，并在足够证据和充分理由的基础上提出最佳的选择方案。有关建议须全部提交管理层，而管理层则有权批准及落实建议。

7.3 承担

个人和部门的承担对落实建议至关重要。安全顾问 / 审计师、人员和管理层可能有不同的考虑和着眼点，和对落实建议的次序亦可能持不同意见。

7.3.1 安全顾问 / 审计师

安全顾问 / 审计师是首先提出改进建议的一方。他们应：

- 对自己的建议有信心，如果用户遵从其建议，应能够产生理想的改善效果；
- 了解决策局 / 部门在环境、时间、资源和文化等方面的限制；以及
- 通过适当及有效的沟通途径提出建议。

7.3.2 人员

人员在这里尤其是指直接或间接受建议影响的一方。人员可能须支持落实建议，也可能就是实际上须改变日常操作程序的用户。人员应：

- 获部门鼓励以加强与安全顾问 / 审计师合作；
- 获足够时间和资源以作出改进；以及
- 获保证他们能够从建议中得益。

7.3.3 管理层

管理层在落实改进建议的工作中扮演重要角色。管理层应：

- 在安全事务上采取积极主动而不是消极被动的态度；
- 在整个评估或审计过程中给予充分的支持；
- 调拨充足的资源以作出改进；
- 认识到跟进责任的价值和重要性；
- 鼓励在规划、控制和沟通足够的情况下立即采取改进行动；以及
- 提高人员的安全意识并加强培训。

7.4 监察与跟进

监察与跟进包含三个主要步骤：

- 建立有效的监察与跟进机制
- 确认建议并制订跟进计划
- 主动监察及报告

7.4.1 建立监察与跟进机制

管理层应就建议订立监察与跟进机制。除负责安全风险评估或审计的人员外，管理层可调派额外人手监督监察机制的整体成效。

管理层负责提供充分的支持、整体指南和方向。监察机制的范围、目的和功能可由管理层制订。此外，管理层还可制订基本规则和指南，作为安全评估监察与跟进的一般参考。

7.4.2 识别建议并制订跟进计划

为有效并及时地采取改进措施，应进行以下各项工作：

- 识别主要、重大和关键建议，以便进行额外监察，并投放最多的人力物力。
- 为所有建议，制订跟进计划。跟进计划包括落实方案、估计时间、行动列表、成果验证程序和方法。
- 汇报并强调重点建议和跟进工作。
- 根据计划，跟进所有建议。

7.4.3 主动监察及报告

在完成落实建议的工作前，必须主动监察及报告跟进行动的进度和进展情况，并就所有建议采取跟进行动。

7.4.3.1 跟进行动的进度和进展情况

跟进行动有不同的进度和进展情况：

- 尚未展开或采取的行动
- 已完成的行动
- 正采取行动而且已定下目标完成日期
- 不采取行动的理由
- 建议以外的其他行动

7.4.3.2 跟进行动

下列是一些建议采用的跟进行动：

- 覆检落实方案、文件和行动时间表。
- 找出并记录不采取行动的理由。
- 建立额外的步骤或工作项目，以解决技术、操作或管理方面的困难。
- 因应突发环境或要求转变，找出并推行其他可行的建议。
- 在证实建议已落实及测试成功、或不再有效、或已采取跟进行动但仍未凑效时，决定「终止」建议的日期。
- 评估纠正行动的成效。
- 向管理层报告成果、进展情况和进度。
- 在适当情况下提请管理层跟进，特别是在关键建议落实不足、延误、或不采用时。

完

附件 A：安全风险评估提问样本清单

在识别安全风险之前，可能须视乎安全风险评估的范围，评估很多不同的领域。在进行安全风险评估时，顾问可能会设计问卷调查，向决策局 / 部门内各级人员收集最新资料。以下为问卷可能提出涉及不同类别的问题示例。顾问会根据评估的范围和环境改进检查清单。

提问示例
规则和政策
• 是否已制订适当的安全政策、指南和程序？ • 现行的安全政策 / 程序 / 指南是否已充分列明准许及禁止的行为？ • 人员及用户在获授访问权前，是否知悉有关的法律、安全政策和程序，以及须承担的责任？ • 用户可否轻易取阅安全政策 / 指南 / 程序？ • 有否定期监察和覆检有关的安全文件？ • 系统所用的所有软件是否都符合现行的知识产权和特许协议？ • 有关人员有否确实遵从和遵守所有规则和政策？ • 有否定期覆检安全文件以应对新科技导致的威胁？
使用和支持系统服务
• 系统是否只用来履行公务上的职责，而在使用时可曾发生大规模的违反安全事件？ • 全体用户是否已接受足够的培训，懂得使用获提供的系统 / 服务？ • 是否已建立任何书面申请和授权程序，方便人员申请和管方授予服务或系统的使用权？ • 提供支持的供货商（例如互联网服务供货商）有否提供可靠及符合成本效益的支持服务？ • 互联网服务供货商代存的电邮是否已获得适当保护？ • 有否适当地监察、控制及覆检支持服务的供货商的表现？

提问示例
系统／网络的完整性
• 有否禁止用户自行连接或访问服务或系统（例如互联网连接）？ • 有否配置所有主机和工作站，防止引入活动内容或微应用程序？ • 系统记录或误差记录会否保存一段适当时间？ • 是否已采取措施保护所有记录，包括逻辑和实体控制记录免被未获授权访问及窜改？ • 系统或网络内是否已采取保护措施防止外部访问？ • 是否有任何保密资料未经加密便在网络上传递？ • 是否已采用数码证书技术？若是，请说明哪些服务或应用系统已采用该技术？
入侵检测及监察
• 是否已制订任何安全事故应急／处理程序？ • 相关的全体人员是否均了解和遵从本程序（他们是否起码了解和遵从应由他们负责或可能受影响的部分）？ • 安全事故应急／处理程序是否已列明一旦发生可疑活动应立即采取的行动？ • 如有任何可疑活动，是否会发出任何审计追踪／记录、报告或警报？ • 是否定期或有规律地覆检本程序？ • 是否会作出周详的报告，以便监察用户的活动，例如用户名称、登入／退出、连接日期／时间、所用服务、发出／收到的数据类别、获授予的访问权、使用电邮、互联网、打印机和抽取式媒体的情况、用户获分配使用的计算机设备等？ • 是否定期编制和覆检用户活动监察报告？ • 过去可曾发生任何违反安全事件？ 最近／上一次违反安全事件是什么？当时如何处理该事件？ • 是否有专人监察服务／网络？ • 是否已制订应急计划？ 是否已测试及试运行这些计划？ 是否定期覆检及测试这些计划，以顺应系统／网络的变化？ • 对不断出现的威胁，如拒绝服务攻击、分布式拒绝服务攻击、高级持续性网络攻击，及勒索软件等有否任何侦测及监视机制？ • 有否任何措施缓解当时网上威胁？

提问示例
实体安全
• 是否有任何证据或文件，显示计算机室符合根据所存放数据的保密类别而订定的实体安全要求？证据或证明文件的例子包括建筑署发出的认证／通知或上次安全风险评估与审计报告的相关结果。 • 网络的所有关键构件，例如防火墙、服务器、路由器和交换器是否已放置在限制出入或安全的地方？ • 对放置网络构件的地方是否已采取环境控制措施，以免构件受火灾、停电或供电不稳定、水浸影响？ • 是否已适当地将所有备份保存在安全的地方？ • 对网络构件有否推行任何访问控制，例如进出计算机室时必须在记录簿签字登记、对计算机室门匙的使用加以控制？
变更控制管理
• 是否已明确界定及指配系统管理员、用户及操作员于访问系统／网络的职务和职责？ • 在更改配置前，所有行动是否均已正式获批准、经过彻底测试并已作文字记录？ • 对配置文件是否已采取保护及访问控制措施，以防止未获授权访问？ • 操作系统及软件是否已采用所有最新的修补程序？ • 对管理工作（如有）是否已采取任何内部和远程逻辑访问控制？ • 是否有专人负责每天的监察、管理和配置工作？ • 是否已向人员提供有关操作系统／网络必要配置功能的培训？ • 是否在内部及远程均全面为所有配置备份？是否已妥善保存所有备份媒体？
安全风险评估及审计
• 是否曾进行任何安全风险评估和安全审计？ • 每次安全风险评估和安全审计的时间和内容是什么？ • 曾找到什么主要的安全风险？ • 是否已制订任何跟进计划以落实建议？ • 是否已妥善地解决所有安全风险？ 如果没有，原因为何？ • 是否已将未解决的跟进计划通知管理层？ • 是否已适当地保存及储存评估和审计结果？

提问示例
防范恶意软件
• 是否已采用标准的恶意软件侦测及修复措施或工具？ 所有主机和服务器是否均已安装这些软件或工具？ • 是否已就如何使用这些恶意软件侦测及修复措施或工具，制订标准或指南？ • 所有工作站和主机是否均已安装最新版本的恶意软件定义，及相应的侦测及修复引擎？ • 是否已确保使用最新的恶意软件定义档案？ 一般相隔多久会更新或向用户派发定义档案？ • 是否已定期通知用户可供使用的最新版本恶意软件定义？ • 这些工具是否能够侦测任何电邮宏指令病毒、压缩文件案、电邮附件、常驻内存数据等？ • 是否有任何支持人员负责处理恶意软件攻击事件？ • 如果侦测到恶意软件，是否会进行调查及采取跟进行动？
教导及培训
• 是否提供任何关于信息技术安全的培训或讲座？ • 是否定期向用户宣布或介绍信息技术安全技术、政策的变动或相关的新闻？ • 提供支持的全体人员是否均获得足够的培训，确保适当地配置、管理和监察网络 / 系统？

附件 B：成品内容示例

B.1 安全要求报告

该报告载录对评估领域的最低安全要求。这些安全要求可根据决策局 / 部门本身的需要划分为高层次或低层次要求。一般而言，这些要求根据资产、威胁和漏洞及其影响划分。

以下是供参考的安全要求示例清单：

- 提高安全意识及加强培训
- 确保有足够的访问控制
- 编制一套完整的信息系统和操作文件
- 制订安全事故处理及应急程序
- 制订正式的书面应急计划
- 定期进行安全审计
- 备存足够和适当的记录
- 制订授权访问和控制程序
- 确保数据传输的安全，包括为保密数据加密

B.2 安全风险评估报告

该安全风险评估报告应包括但不限于下列各项：

- 引言 / 背景资料
- 摘要
- 评估范围、目的、方法、时间表和假设，评估所包括及不包括的范围
- 当前环境或系统的描述，并附上网络图（如有）
- 安全要求
- 风险评估小组
- 评估结果及建议的摘要
- 就已确认的资产、威胁、漏洞及其影响和可能性，提供风险分析结果，界定风险水平并提出适当的理由
- 建议安全保障措施，如果提出多个建议供选择，便须附连成本 / 效益分析，例如安装防御机制或加强现行的安全政策和程序等
- 结论
- 附件包括已完成的一般控制检查列表、漏洞扫描报告、渗透测试报告、资产识别与估值结果等。

B.3 安全政策、指南和程序

除报告外，安全顾问 / 审计师可协助决策局 / 部门制订和提出某些政策和指南。

例如：

- 部门安全政策
- 变更管理控制程序
- 密码管理指南
- 信息安全事故应急及处理指南
- 一般主机安全指南
- 具体的信息系统安全政策
- 目录服务安全政策

B.4 安全审计报告

审计报告应包括但不限于下列资料：

- 引言 / 背景资料
- 撮要
- 审计范围、目的、方法、时间表，以及假设和局限
- 当前环境的描述
- 安全要求
- 审计小组
- 安全审计师的独立性声明 1
- 审计结果摘要
- 测试及测试结果详情
- 根据所发现的问题领域提出建议和纠正行动，例如违反安全政策、配置不当、已知的漏洞和潜在的漏洞、泄露数据、不使用的服务（特别是默认服务）和不使用的账户等。
- 结论
- 附件包括审计检查列表、漏洞扫描报告、渗透测试报告等。

[1]倘若由于参与审计以外的事宜而可能有损审计师的独立性，有关非审计职务的资料须予披露。

附件 C：各种审计领域

C.1 防火墙

这项审计领域的目的是确保适当配置防火墙及相关系统，以最少和最有效的安全保护措施推行安全政策。对防火墙的审计不限于配置，还涵盖防火墙的实体访问控制。

这审计领域可包括下列各项：

- 对防火墙主机实体访问控制
- 防火墙操作系统的版本和修补程序
- 防火墙配置及对互联网通讯的控制，例如规则库和开启端口
- 容许或禁止通过防火墙的服务
- 互联网连接目前的结构，例如与路由器、代理服务器、电邮服务器及网络服务器的连接
- 为获得额外服务与其他第三方产品的连接，例如恶意软件侦测及修复措施
- 远程连接支持和配置
- 管理和变更控制程序
- 访问控制清单（如有）

安全审计报告应概述对防火墙的评估，并就防火墙结构、配置、管理和操作提出建议。

C.2 内部网络

这项审计领域的目的是找出可能被获授权内部用户利用的任何安全漏洞，并确定内部系统及网络控制措施的强弱之处。另外还可覆检内部网络基础设施的布局。

审计测试一般包括内部网络扫描，从而在指定时间或预定时段内检查任何安全漏洞。测试可包括对关键主机或工作站的扫描。

此审计领域可能包括：

- 对内部工作站、服务器或网络的扫描，以确认主机、服务和网络配置
- 找出操作系统、内部防火墙、路由器、网络构件和基础设施的安全漏洞、协议和配置误差
- 尝试入侵内部网络和系统
- 评估与访问控制及监察、管理及变更控制程序和作业模式相关的内部安全措施
- 就加强网络安全提出建议

C.3 外部网络

这项审计领域的目的是从外部（例如互联网）找出系统和网络的安全薄弱环节。外部网络审计通过扫描，并在指定和预定时间及地点，从互联网向内部网络发起攻击（即黑客入侵），预测可能引发违反安全事件的外来攻击。

这项审计领域可包括：

- 扫描内部服务器，以找出容易受攻击的端口和服务
- 扫描外部网络网关，以确定可使用的端口、服务和网络布局
- 尝试从外部收集内部配置数据
- 从外部向内部系统发起入侵攻击

审计师和用户双方必须制订协议，明确地界定审计范围和测试程度详情，例如受攻击的网络部分 / 构件或可接受的攻击严重程度。安全审计师必须承诺将干扰减到最低程度，并避免对系统和网络造成破坏。

C.4 主机安全

这项审计领域的目的是评估不同计算机平台的操作系统层面安全。操作系统配置不当可产生不为系统管理员所知的安全漏洞。

在考虑操作系统安全时，帐户及密码管理、文件系统、连网工作组、访问权限和审计 / 日志记录均为不可遗漏的常见组件。详情列述如下：

帐户及密码管理

- 密码控制政策，例如密码的最短和最长的长度
- 用户配置档案和权限
- 默认用户或管理帐户
- 共享账户
- 账户政策，例如帐户锁定、账户有效期

文件系统

- 系统文件保护措施及访问权限
- 档案访问控制清单
- 网络文件系统的使用

连网工作组

- 领域及信赖关系
- 工作组
- 共享的文件夹
- 复制的文件夹
- 远程访问控制

访问权限

- 默认文件夹权限
- 共享工作站权限
- 共享打印机权限
- 登记权限
- 共享档案权限

审计 / 日志记录

- 事件记录 / 系统记录 / 误差记录审计
- 档案及文件夹审计
- 登录审计
- 打印机 / 抽取式媒体记录审计
- 警报
- 账户处理和审计追踪保护措施

C.5 互联网安全

这项审计领域的目的是找出系统和网络中与互联网应用相关的安全薄弱环节。此类审计内部网络与外部网络结合的审计领域，重点在于互联网通讯闸。

审计领域包括但不限于下列各项：

- 防火墙和路由器配置。
- 网站服务器、邮件服务器、认证服务器等主机服务器的安全控制。
- 主机、系统和网络安全管理，以及控制政策与程序。
- 互联网网关网络构件及服务器的实体安全。
- 互联网网关部分，以及与内部网络连接界面的网络安全。
- 从外部向内部互联网网关发起拒绝服务攻击或分布式拒绝服务攻击的防御能力。
- 破解内部网络构件。

C.6 远程访问

这项审计领域的目的是解决与透过拨号连接和宽带连接（例如虚拟私有网络、传输层安全协议虚拟私有网络）等通讯链路提供远程访问服务的相关的安全漏洞。此类审计领域可包括下列各项工作：

- 利用自动拨号 / 联机软件识别远程访问用户。
- 覆检远程访问服务器的安全和配置，以及这些服务器所在的网络。
- 进行实地走访，以覆检调解器或远程连接设备的实体控制和位置。
- 制订远程访问控制政策或程序。

没有采取任何控制措施的远程访问可能会成为外来入侵者的方便之门。问题在于如何建立安全的连接。

这项审计领域可能会识别和覆检下列项目：

- 需要远程访问的应用系统 / 服务及其安全要求。
- 有关远程访问的现行政策和程序。
- 现有远程访问连接，例如采用调解器、远程访问服务器、调解器群的连接或宽带连接。
- 现行的远程访问控制方法。
- 目前存在的问题和改善情况的建议。

C.7 无线通信

这项审计领域的目的是解决与无线通信相关的安全漏洞。此类审计领域应包括（但不限于）以下各项工作：

- 评估服务设定标识符（SSID）命名和命名约定及其他安全配置。
- 评估现有无线网络加密协议和加密密码钥和密码算法的强度，例如 Wi-Fi 保护存取 3（WPA3），支持强大的加密。
- 评估采用虚拟专用网络。
- 取得接驳点清单并了解其覆盖范围。
- 识别任何未获授权或非法无线接驳点。
- 尝试与无线通信连接。
- 尝试透过无线通信收集内部系统数据。
- 评估有否进行实地调查及有关场地的无线通信的覆盖范围。
- 评估客户装置上的密码匙是否获妥善保护。

C.8 电话线

这项审计领域的目的是找出将内部计算机直接与电话网络连接的没有记载或不受控制的调解器。此类审计有助杜绝任何未获授权或不当的调解器连接和内部网络及系统配置。

这项审计领域可包括：

- 评估已连接的各个调解器进入点
- 找出任何没有记载的拨号进入点
- 尝试与内部网络连接
- 尝试透过连接收集内部系统数据

C.9 网上 / 流动应用系统

这项审计领域的目的是解决与网上 / 流动应用系统相关的安全漏洞。这项审计领域应包括以下测试：

- 验证安全要求是否已在早期界定。
- 验证所推行的安全控制是否符合功能规格文件内订明的安全要求。
- 验证是否处理或过滤不正常的用户输入。
- 为网上应用系统评估因错误讯息及超文本传输协议标头上的元数据所造成的数据泄漏。
- 重演系统验收测试文件内编制的安全测试个案，以确保维持适当的安全控制。
- 评估网上 / 流动应用系统的网络及应用系统结构。
- 评估有否采取适当的访问控制措施。
- 评估加密机制与协议。
- 评估网上 / 流动应用系统程序的权限。

有关网上应用程序安全的良好作业模式，请参阅《网页及网上应用程序安全实务指南》。

C.10 安全政策、指南和程序

此章节的目的是覆检现行的安全政策、指南及程序。覆检的对象可以是高层次 / 整体 / 整个机构的安全政策，或是集中关注的特定系统、网络或安全组件。

下列是一些集中关注的安全组件示例：

- 远程访问控制
- 互联网访问控制、使用和监察
- 互联网电邮系统
- 操作系统管理
- 密码控制政策
- 用户帐户管理
- 网络、系统或网关管理
- 变更管理作业模式
- 网络安全作业模式

附件 D：审计检查清单样本

以下所列是从遵行及良好作业模式方面，安全审计可能检查的部分事项举例。本检查清单仅供初步参考，不能涵盖所有范围。审计师会根据审计的范围和环境来改进检查清单，并可能要求决策局／部门提供相关记录或文件。

审计事项
管理职责
□ 已界定部门信息技术安全组织框架及相关的职务和责任。 □ 已推行足够职务分工，避免单一个体管理信息系统的所有安全功能。 □ 部门预算包括提供必需的安全防护及资源。
信息技术安全政策
□ 安全政策以文字方式清楚载明，而且容易理解。 □ 安全政策便于有关各方取阅。 □ 定期覆检及更新安全政策并获批准，以反映最新情况。 □ 用户均知悉并承担推行安全政策的责任。 □ 安全政策所列的所有规则已落实推行。 □ 安全政策由决策局局长／部门主管及管理层核准、发布和执行。
人力资源安全
□ 所有人员在委任新职位及于整个雇用期间，都获悉本身的信息技术安全责任。 □ 明确界定所有职务和职责。 □ 向有关各方提供足够的安全培训。 □ 只限曾接受公务员事务局局长所规定适当操守审查的人员才可访问限阅类别以上的保密数据。 □ 已订明终止或职位变动后的信息安全责任及工作，并已与人员就此进行沟通。

审计事项
资产管理
□ 妥善管有、保存及维护信息系统、硬件资产、软件资产、有效保用证、服务协议书和法律 / 合约文件的清单。 □ 当人员被调职或不能为政府提供服务时，向政府归还计算机资源及数据。 □ 数据获妥善保密分类，其储存媒体亦已按政府安全要求附上标签及处理。 □ 已对存有保密数据的储存媒体执行适当的安全措施，以防范非授权访问、滥用或实体损伤。 □ 所有保密数据都在弃置或重用储存媒体前彻底清除或销毁。
访问控制
□ 处理个人资料时已遵守《个人资料（私隐）条例》（第 486 章）。 □ 记录和覆检各类用户在访问系统上所获授的权限，并确保职务分工恰当。 □ 订有明确的程序，可定期重新确认用户在访问系统和应用系统上的权限。 □ 已清晰界定及定期覆检用户权限及数据访问权限（例如至少每年一次，最好每年两次）。 □ 已备存访问权限审批及覆检记录。 □ 用户名称只代表一名用户。 □ 所有用户只获得仅足以履行其职责的最小权限。 □ 用户知悉其权限和访问权。 □ 依据所访问的数据类别，制订适当和安全的程序以分派用户帐户和密码。 □ 妥善备存用户活动记录，例如登入 / 退出时间、连接的时间、连接点、所进行的操作等。 □ 系统 / 网络没有不再使用的账户。 □ 向管理员另外提供用户帐户。 □ 管理员账户只用来进行管理工作。 □ 用户分为不同的类别，各个类别的权限明确。 □ 具有为系统 / 网络而编制完善的密码政策文件。 □ 关键信息系统采用严谨密码政策。

审计事项
□ 严谨密码政策： ■ 当密码更新时，不可重复使用 8 个先前使用过的密码。 ■ 密码须设定失效期（3-6 个月）。 ■ 输入错误密码的次数以 5 次为限。 □ 不应选用可在字典内查到的词汇、用户名称或容易猜出的短语作为密码。 □ 用户须定期更换密码，或在收到新帐户时立即更换密码。 □ 用户不得将密码写在卷标或容易被他人窥看的地方。 □ 订有适当的政策与程序，阐明有关流动信息处理及远程访问的安全要求。 □ 订有远程访问计算机、应用系统和数据的控制措施。 □ 高风险访问采用双重认证。 □ 在通过虚拟专用网络连接远程访问决策局 / 部门内部网络，或经互联网远程访问决策局 / 部门内部电邮系统方面，实施双重认证。 □ 通过虚拟专用网络传输数据时，使用严格的加密功能及 / 或双重认证（只适用于机密数据），并启动闲置对话逾时注销功能。 □ 设有正式的使用政策和程序，并须采取适当的安全措施以防范物联网装置的风险。
加密方法
□ 密码匙在整个生命周期，包括密码匙的产生、储存、存档、收回、分发、退役及销毁，都会得到妥善管理。
实体及环境安全
□ 备有证据或证明文件，显示计算机室 / 服务器室 / 计算机操作区的实体安全要求，符合部门信息技术安全政策、政府安全要求和其他相关标准订明的要求。例子包括上次安全风险评估与审计报告或建筑署发出的认证 / 通知。 □ 所有电缆保持整洁，并适当地贴上标签，以便维修和侦测故障。 □ 妥善清洁所有地板下的空间（如有）。 □ 定期清洁天花，以免积聚尘埃和污垢。 □ 水浸探测器（如有）装入地板下空间，以自动探测水浸情况。 □ 将电缆妥善安装在天花空隙。 □ 为有需要的设备安装不间断电源供应器。 □ 不间断电源供应器能够在预定的一段时间内提供足够的电力。

审计事项
□ 定期测试不间断电源供应器。
□ 不间断电源供应器放置在安全的地方。
□ 已适当地教导计算机室操作员有关电源供应控制和应付停电情况的知识。
□ 计算机室内没有存放任何易燃设备或物料。
□ 所有自动火警探测系统均处于正常的操作状态，并定期进行测试和检查。
□ 定期测试所有自动灭火系统，确保有关系统处于良好状态。
□ 穿过计算机室或地板下的所有水管（如有）均处于良好状态。
□ 计算机室温度和湿度受到监控，并已调校至适合计算机设备在良好状态运作的水平。
□ 妥善分发、保管及记录计算机室的所有门匙。
□ 制订明确清晰的锁匙处理及分发程序。
□ 全体人员均已受训并知悉如何使用灭火器和其他实体保护机件。
□ 计算机室内禁止吸烟、饮食。
□ 带入计算机室内的便携式计算机、流动装置和其他计算机设备应受管制。
□ 指定专人负责安排清洁计算机室的工作。
□ 定期检查设备及设施。
□ 所有访客取得授权并确认身份后才能进入计算机室。
□ 在任何时间所有访客都有授权人员陪同。
□ 所有访客在进入计算机室时领取访客标贴。
□ 记录所有访客的到访。
□ 计算机室推行适当的出入管制。
□ 所有计算机室入口已上锁，以管制出入。
□ 只准获授权人员进入计算机室，而获授权人员进出计算机室都必须签字登记。
□ 所有手册和文件不得随意摆放，而应该经存盘处理后放上书架，并推行查阅管制。
□ 计算机室内的计算机文具足够操作所需便可。避免存放过量的文具以防引起火灾。
□ 妥善保存及管制所有计算机文具。
□ 制订分发、授权及记录计算机文具的程序。

审计事项
□ 为所有计算机设备备存及检查适当的清单并加以检查。 □ 抽样实地核对计算机设备和列表记录，确保列表记录准确无误。 □ 确保流动装置或抽取式媒体于无人看管时有措施保护。 □ 被带离场地的信息技术设备得到适当管制。 □ 已使用及开启所有计算机的自动重新认证功能。 □ 在物联网装置方面，须根据物联网装置储存、处理和传递资料的保密类别来实施安全控制措施，以防装置遗失、被盗和遭受破坏。
操作安全
□ 所有从互联网下载的软件及档案都经抗恶意软件筛选及验证。 □ 具有为备份和复原工作而制订和编写的程序。 □ 为已进行的所有备份和复原工作备存记录，包括日期 / 时间、所用备份媒体、负责人等。 □ 备份不少于两份，其中一份存置于场外。 □ 备份媒体有明确的保留期及弃置程序。 □ 妥善地为所有备份媒体卷标并锁入安全的地方。 □ 在任何时间均锁好存放备份媒体的地方或储物柜。 □ 为场外存放的媒体采取适当的运送控制措施。 □ 妥善控制及记录访问媒体的情况。 □ 为所有储存媒体备存列表。 □ 妥善备存、覆检和分析每日记录，如系统记录、误差记录或用户活动记录等。 □ 由政府资讯科技总监办公室或决策局 / 部门中央提供的核准电邮系统和互联网访问服务记录须予记录。 □ 只限获授权人士访问操作系统设施。 □ 操作系统帐户没有执行不使用 / 可疑的服务。 □ 操作系统没有保留不使用的用户帐户。 □ 每天或定期妥善编制及覆检系统记录。 □ 信息系统的时钟已与可信赖的时间源保持同步。 □ 对更改信息系统采取控制措施。已备存更改记录。 □ 定期安装操作系统的修补程序，以修补操作系统内已知的安全漏洞。

审计事项
□ 建立和备存决策局 / 部门常用的硬件设备、套装软件（包括修补程序管理系统本身）和其版本号码的详细记录。 □ 决策局 / 部门须评估使用有关已终止支持软件的安全风险，以及采取适当安全措施保护信息系统和相关数据。
通讯安全
□ 与互联网连接的网络受到防火墙保护。 □ 推行入侵检测策略，在网络关键节点安装网络入侵检测系统或网络入侵防御系统，以侦测网络异常活动。 □ 采用网络分段／隔离，并以此作为所有新推行的系统或现有系统进行大规模升级和变更时须遵守的标准。 □ 接入内部网络的所有远程访问，均以认证和记录作妥善控制。 □ 只限获授权人员进行网络构件的管理工作。 □ 对共享档案、打印机等网络资源的使用，采取控制措施，只准已获授权及认证的用户使用。 □ 只限获授权人士更新网络所安装的软件。 □ 制订政策以控制网络及其资源，使其得以适当使用。 □ 为容许经网络传输和传递的数据采取安全保护措施，例如加密。 □ 指定专人负责监察网络性能和每日操作情况。 □ 妥善保管所有网络用户配置档案，以防止未获授权访问。 □ 以文件记载网络配置，并将文件存放在安全的地方。 □ 将所有网络构件存放在安全的地方。 □ 已制订并推行适当安全措施确保由另一决策局 / 部门或外聘机构控制的信息系统与本部门信息系统连接时，被连接的信息系统的安全级别不会降级。 □ 决策局 / 部门与外聘机构已就各方之间安全传递保密数据达成协议，该协议亦已被记录。 □ 定期覆检 Wi-Fi 基础设施，以评估在 Wi-Fi 通讯标准和协议所发现之安全漏洞的影响。 □ 政府互联网网域的资源记录须受现行的安全控制措施（即域名系统安全扩展）所保护。 □ 所有互联网服务（包括信息网站）推行加密传递，例如超文本传输安全协议。
系统购置、发展及维护
□ 具有为变更控制程序而编撰完善的文件。

审计事项
□ 对更改要求的影响作评估或估计。
□ 在更改前妥善核准、记录及测试所有更改。
□ 在更改前后进行充分备份。
□ 在每次更改前订明复原程序。
□ 采取控制措施，确保测试数据 / 程序不会残留在生产环境内。
□ 在变更应用在生产环境后进行检验（例如人手覆检），以确保所有变更均按要求和计划推行。
□ 只向专责人员或管理员授予适当的访问权，以修正系统 / 网络的配置。
□ 如有需要，修订备份和复原程序以反映更改。
□ 为涵盖整个系统发展周期的系统发展及整合工作，建立安全的发展环境。
□ 应建立版本控制机制，记录程序源码在应用系统发展过程中的变更。
外包信息系统的安全
□ 已识别及评估使用外聘服务或设备的风险。
□ 妥善管理已签署的机密及不可向外披露数据协议文件。
□ 在服务到期或终止时，或应政府要求，所有在外聘服务或设施的政府数据都会按政府安全要求被清除或销毁。
安全事故管理
□ 已根据各系统的特定操作需要而建立事故监察及应急机制。
□ 已预先设定记录的保留期限，以便在需要时追踪安全事故。
□ 定期覆检安全事故应急 / 处理程序并进行演习（至少每两年一次，最好每年一次）。
□ 发生安全事故时，有关人员根据既定的通报渠道妥善处理及提请管理层跟进。
□ 向终端用户提供最新版本的事故监察 / 应急程序。
信息技术安全方面的业务连续性管理
□ 根据所定次数，覆检和更新运作复原和紧急应急计划并进行演习。
□ 详细编写及定期测试关键业务信息系统的运作复原和紧急应急计划，并将计划与业务连续性计划紧扣一起。
□ 有适当复原能力以符合信息技术服务及设施的可用性要求。

审计事项
遵行要求
□ 安全政策应要求定期进行安全风险评估及审计。 □ 已跟进上一次安全风险评估及审计所作的建议。 □ 已就系统的操作，定出及记录所有适用的相关法定、规管及合约要求。 □ 保存安全要求的遵行证明记录及支持相关安全措施获有效推行的审计记录。 □ 拣选审计师和进行审计的工作客观持平。 □ 限制及控制使用软件和程序来进行安全风险评估或审计。 □ 对于涉及个人资料的信息系统，在整个数据生命周期内推行适当的安全措施。

附件 E：作为遵行证据的已记录数据样本列表

编号	已记录数据
1	信息技术组织结构表（连人员姓名及照片）
2	信息安全组织架构
3	信息安全组织会议的会议记录
4	对部门信息技术安全政策、标准、指南及程序的近期覆检或审批记录
5	近期派发部门信息技术安全政策连接收人士记录
6	信息技术服务及设备的许可使用政策
7	近期派发信息技术服务及设备的许可使用政策记录及接收人士记录
8	安全意识培训的出席名单
9	安全意识培训教材
10	外聘服务供货商所签署的不披露协议书
11	已通知外聘服务供货商其安全责任的证明
12	数据中心或服务器室设备及通讯设施的检查记录
13	用作进入数据中心或服务器室的访问钥匙、咭、密码的申请及分发程序
14	用作进入数据中心或服务器室的访问钥匙、咭、密码的申请和分发审批记录
15	获授权访问数据中心或服务器室人士的清单
16	获授权访问数据中心或服务器室人士列表的覆检记录
17	数据中心或服务器室的访客记录
18	信息系统（关键信息系统须加上标记）、硬件资产（包括手提电脑、流动装置和 USB 盘）、软件资产（包括桌面应用程序、流动应用程序）、有效保用证、服务协议书和法律 / 合约文件的清单
19	列表检查记录
20	要求信息技术设备的记录
21	用户帐户维护程序
22	新增 / 修改用户帐户以访问内部网络的审批记录
23	部门信息技术安全主任对新增共享用户帐户以访问内部网络的审批记录

编号	已记录数据
24	由部门信息技术安全主任批准的共享用户帐户列表
25	停用访问内部网络的用户帐户的记录
26	在员工辞职 / 终止雇用 / 调职时，计算机资源的移交及归还记录
27	访问内部网络的非活跃用户帐户的覆检记录
28	用户帐户的数据访问权限覆检记录
29	密码政策或标准
30	关于使用流动运算及远程访问时安全要求的使用政策及程序
31	用户对使用流动装置及远程访问时的自身安全责任的接受声明
32	可作远程访问的用户帐户列表
33	显示远程访问点的网络图
34	决策局 / 部门主管对经私人拥有计算机资源或物联网装置连接内部网络的审批记录（如有）
35	决策局 / 部门主管对使用私人拥有计算机或流动装置处理机密 / 限阅数据的审批记录（如有）
36	外聘服务供货商就弃置硬磁盘前消磁的证书
37	备份及复原政策或程序
38	备份活动的覆检记录
39	储存媒体的复原测试记录
40	备份媒体的运送记录
41	关键操作记录的覆检记录
42	信息系统的强化指南和推行记录
43	系统文件的覆检记录
44	部门信息技术安全主任对外部连接 / 或系统界面的审批记录（如有）
45	对使用独立计算机作宽带连接的审批记录（如有）
46	安全修补程序的评核及测试记录
47	不采用安全修补程序的咨询记录
48	安装安全修补程序的要求及审批记录

编号	已记录数据
49	计算机设备及软件安装记录
50	获批准用户安装的软件列表和其覆检记录
51	对端点用户工作站或流动装置内已安装软件的监察记录
52	安装不在获批软件清单上的软件的要求及审批记录
53	无线安全政策
54	无线网络的网络图
55	信息系统活动记录政策
56	服务器、网络设备、打印机和抽取式媒体审计记录的覆检记录
57	最新的安全风险评估报告及跟进行动计划
58	记录适用于信息系统运作的有关法列、监管及合约规定的文件，例如合约、服务水平协议、运作水平协议等
59	安全审计报告及跟进行动计划
60	于安全风险评估及／或安全审计中执行软件及程序（例如扫描工具）的审批记录
61	安全事故应急／处理程序
62	安全事故应急／处理演习报告
63	近期派发安全事处理／报告程序连接收人士记录
64	最新的安全事故报告
65	双重认证标准或政策