数字政策办公室

信息安全

设计层面安全实务指南

第 1.1 版

2024 年 7 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	将「政府资讯科技总监办公室」修改为「数字政策办公室」		1.1	2024 年 7 月

目录

1 简介

随着数码格局的快速发展，安全威胁日益凸显，对政府的信息系统和资产构成重大风险。仅仅依靠事后处理或采取被动措施已无法充分解决安全问题。相反，决策局／部门应采取积极主动的方法，将安全因素纳入核心业务要求，而非仅作为一项技术功能。本实务指南旨在为决策局／部门的系统发展计划提供参考指引。

1.1 目的

本文件提供了设计层面安全的总体框架，且应与其他安全文件结合使用，如《基准信息技术安全政策》[S17]、《信息技术安全指南》[G3]以及相关程序（如适用）。

本实务指南旨为决策局／部门内参与系统发展周期所有阶段的各级员工而设。另外，本文件亦供为政府提供信息技术服务的供货商、承包商及顾问使用。

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：

- 《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]，香港特别行政区政府
- 《安全风险评估及审计实务指南》[ISPG-SM01]，数字政策办公室
- 《敏捷软件开发执行指引》[G62]，数字政策办公室
- Information technology - Security techniques - Information security management systems - Requirements (second edition), ISO/IEC 27001:2022
- Information technology - Security techniques – Code of practice for information security controls (second edition), ISO/IEC 27002:2022
- Security-by-Design Framework, Cyber Security Agency of Singapore
- "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default", Cybersecurity and Infrastructure Security Agency
- "What Is Shift Left Security?", Fortinet

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	
SDLC	系统发展周期
IRS	初始化请求声明
SA&D	系统分析及设计
SBD	设计层面的安全
DMZ	非军事区
RBAC	基于角色的访问控制

1.4 联络方法

本文件由数字政策办公室编制及备存。如有任何意见或建议，请寄往：

电邮： it_security@digitalpolicy.gov.hk

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

CMMP 电邮： IT Security Team/DPO

2 信息安全管理

信息安全是关于安全控制和措施的规划、推行和持续提升，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 / 部门亦须制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。

管制、风险管理与遵行要求

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推行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推行全面的安全措施，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。

安全事件与事故管理

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。

安全意识培训与能力建立

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。

态势认知与信息共享

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信息、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 / 部门可以利用威胁情报平台接收和分享安全事务、安全漏洞和网络威胁情报的信息。

人员亦可以通过参与安全演习和参加研讨会、展示会或浏览载有安全情报资讯和一般安全资讯（例如网络安全资讯站、资讯安全网）的专页来提高安全意识

3 设计层面的安全

必须掌握系统发展周期本身的基础知识，才能真正理解设计层面安全的重要性及其与系统发展周期的协同作用。

3.1 系统发展周期

系统发展周期是一个结构化框架，涵盖系统发展的各个阶段，包括规划、分析、设计、推行、测试、部署和维护。这一周期为管理系统建立到退役的整个生命周期提供了框架。《信息技术安全指南》[G3]中所示的系统发展周期概括如下：

- ***计划开展：***用户应提交初步请求声明以申请信息技术解决方案。初步请求声明将被评估，并决定计划是否应进入下一阶段。

- ***可行性研究：***评估信息技术解决方案的可行性，并量化拟议解决方案的要求、范围、成本、好处和其他影响。

- ***系统分析及设计：***调查现有系统，指定新系统，并执行系统分析和逻辑系统设计，详细说明计划推行要求。

- ***计划推行：***推行实体系统设计、程序发展、各种测试、安装和计划评估覆检，以推行系统分析及设计的发现。

- ***计划推行后的覆检：***评估已推行系统的成本效益，并评估系统是否已及时实现其商定目标以及预期好处。

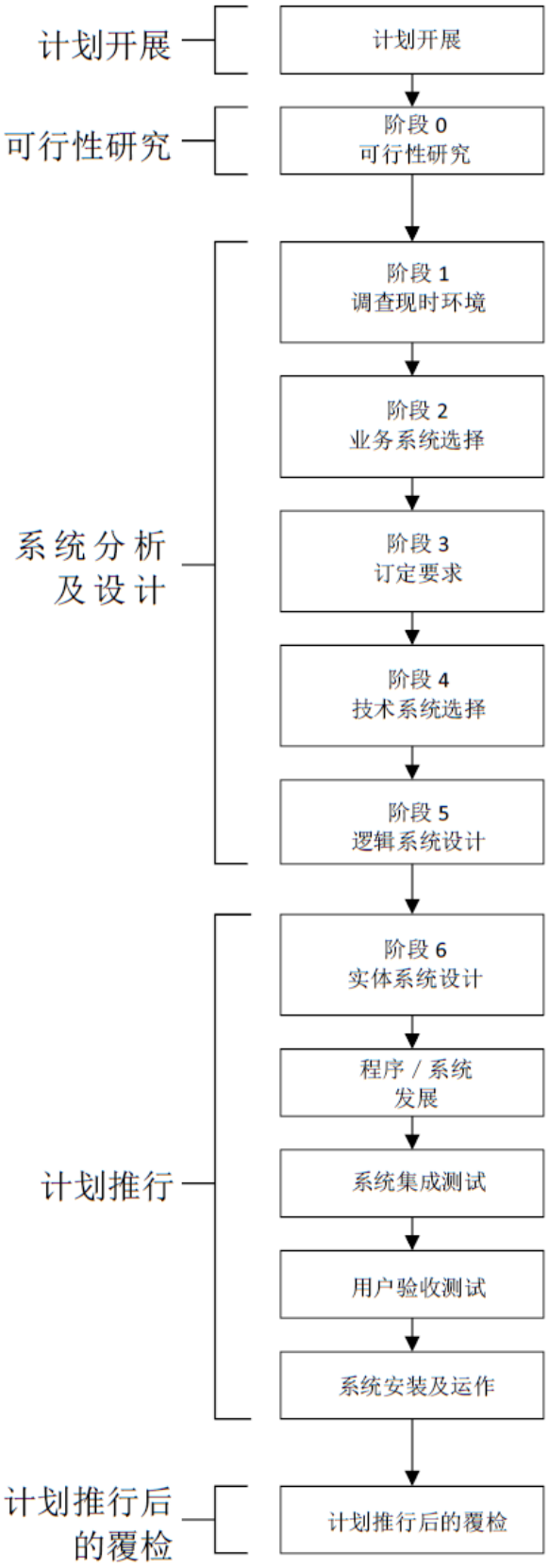

图 3.1：系统发展周期各个阶段

系统发展周期有不同模式，如瀑布式开发和敏捷式开发。瀑布式开发在各个阶段遵循线性和顺序进展，而敏捷式开发则以灵活性和适应性促进重复发展周期。根据计划性质，决策局／部门宜应计划需要，灵活采用多种软件开发方法并应用多种实践。

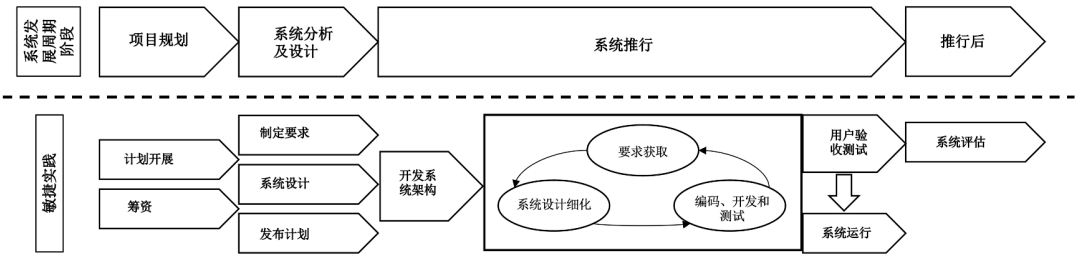

图 3.2：敏捷软件发展实务指引所述的敏捷式开发

有关敏捷软件开发的更多详细信息，请参阅以下文件：

- **敏捷软件开发执行指引**
  可于政府资讯科技情报网获取。
  (https://itginfo.ccgo.hksarg/content/bpg/Agile/agile.html)

本文件中描述的设计层面的安全框架适用于瀑布式和敏捷式发展周期。

3.2 设计层面的安全简介及其重要性

设计层面的安全属于系统开发概念，在整个发展周期中优先考虑和整合安全措施。设计层面的保安旨在发展过程的早期主动识别和解决安全风险和漏洞，减少产生安全漏洞的可能性，并确保创建稳健且具复原能力的系统。通过从一开始就纳入安全原则，决策局 / 部门可最大限度地降低发生代价高昂的安全事故的可能性，并保护其系统和数据的机密性、完整性和可用性。

设计层面的安全框架包括指导安全系统设计和发展的原则。而框架之间各有差异，以下是多种设计层面的安全框架中常见的原则：

- ***核心政府要求：***将设计层面的安全视为一项政府基本要求，保持其与策略目标、运作需求和法规要求一致。将安全性视为竞争优势，并将其与其他政府核心要求一同优先考虑，确保必要的关注、资源和执行支持。

- ***积极主动的方法：***在系统设计的早期阶段即采取积极主动的思维方式来解决安全问题。安全不应是事后考量，而应是发展过程中不可或缺的部分。

- ***端对端安全：***考虑整个系统的安全，包括硬件、软件、网络和用户界面。满足每一层面的安全要求，并确保它们的协同运作以提供全面保护。

- ***风险管理：***开展全面风险评估，以识别潜在的威胁、安全漏洞和影响。制定风险缓解策略，并根据风险级别和潜在影响决定安全措施的优先级。

- ***安全监管：***建立明确的职务、职责和流程，以在系统的整个生命周期内实施安全管理，包括制定问责制、决定权以及监察和执行安全要求的机制。

- ***安全架构：***设计安全且具复原能力的架构，其中包含各个层面的安全控制，包括网络设计、数据流、访问控制和职责分离。遵循已建立的架构模式和最佳安全实践。

- ***安全发展实践：***采用将安全性放在首位的安全编码实践和发展方法，包括安全编码指南、威胁建模、代码审查和安全漏洞测试。定期更新和修补软件组件，以解决已知的安全问题。

- ***第三方安全：***评估第三方组件、服务和供应商的安全状况。建立选择可靠和安全的合作伙伴的标准。在集成外部系统时，制定合同协议并尽职执行安全。

- ***整合到系统发展周期中：***将安全活动和注意事项嵌入到每个系统发展周期阶段，包括收集要求、设计、推行、测试、部署和维护。安全性在整个发展周期中应该是一个持续和重复的过程。

- ***安全测试与验证：***在整个系统发展周期中，开展全面的安全测试和验证活动。包括漏洞扫描、渗透测试、配置审查和源码扫描，以识别和解决安全弱项和漏洞。

在所有系统发展周期阶段都应考虑这些注意事项。但系统发展周期的某些阶段亦有需要注意的特定范畴，该等范畴列载于下页图示右方栏内。

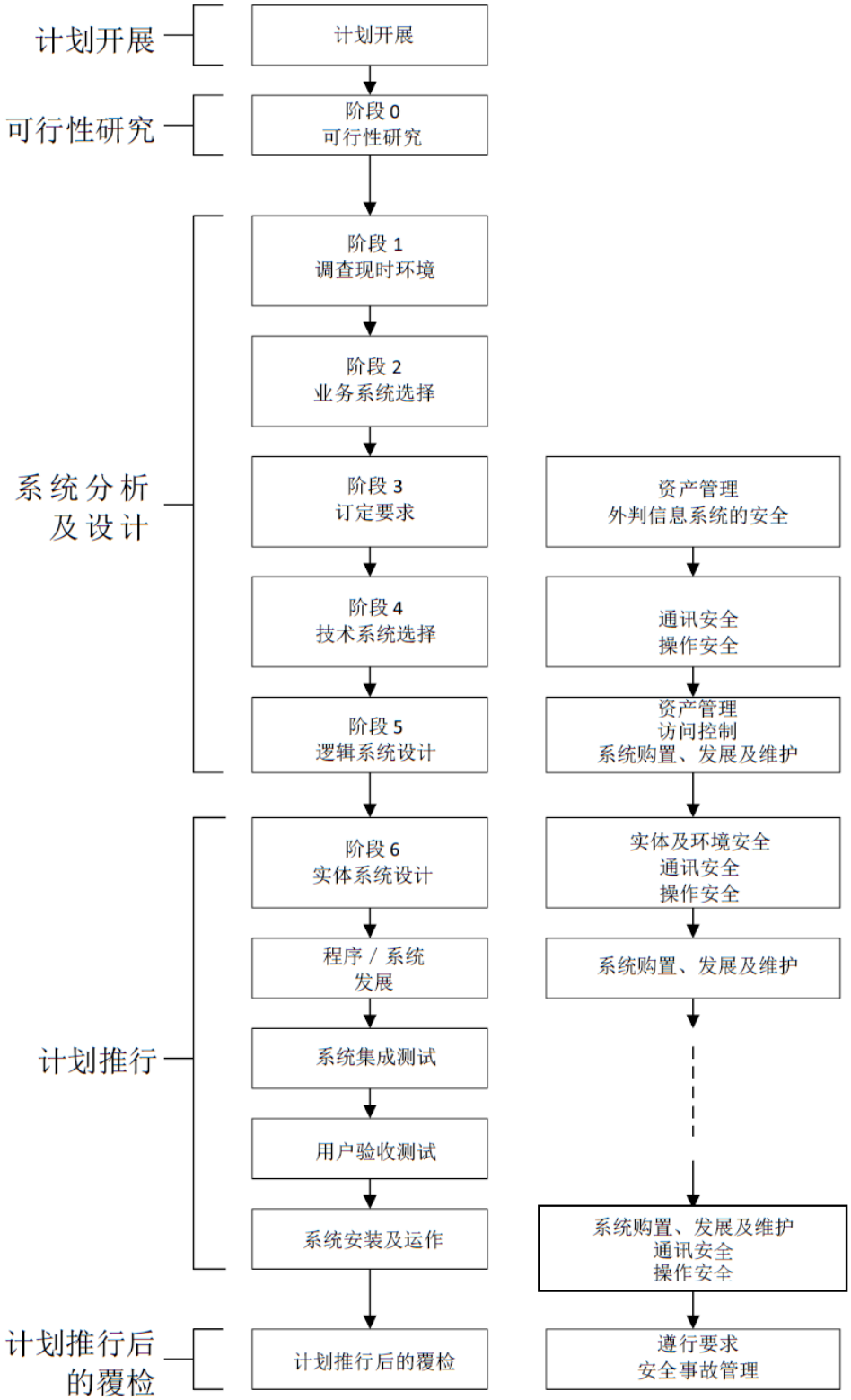

图 3.3：系统发展周期各个阶段

安全左移这一概念与设计层面的安全密切相关，它涉及从计划和评估阶段考虑安全性。

传统上，安全性往往只在测试阶段和软件构建后才得到解决。这可能会减慢发展速度，并且在测试阶段识别安全问题时通常需要重做。而安全左移则可以在测试之前执行安全控制活动，预测安全需求并减少发展后期的潜在问题。但有一点非常重要，设计层面的安全超越了系统发展周期和安全左移，涵盖整个系统设计和架构。设计层面的保安强调将安全注意事项和实践整合到系统设计、架构和推行中，而非将安全视为事后考量。

为确保在推行信息系统及应用系统时存在适当的安全及数据保护措施，决策局／部门应将设计层面的安全概念纳入系统发展周期。设计层面的安全强调从初步设计阶段到系统发展周期的所有阶段都采用安全实践。借此，决策局／部门可以主动识别和降低安全风险和漏洞，最终降低网络安全损害对其声誉、数据完整性和运营造成的潜在代价。

下文重点介绍了将设计层面的安全纳入系统发展周期的一些主要益处：

- ***缓解风险：***通过消除不必要和易受攻击的组件来减少攻击者可利用的潜在入口。

- ***节约成本：***最大限度地减少对发展流程后期阶段发现的安全问题的修复需求，这可能既昂贵又耗时。

- ***增强系统复原能力：***加入安全更新、增强功能和新功能，提高信息系统应对不断变化的保安要求和威胁的可扩展性和适应性，从而更好地保护信息系统免受未经授权的访问、数据泄露和其他安全事故的影响。

3.3 设计层面的安全周期和框架

3.3.1 设计层面的安全周期

在系统发展周期中，主要的关注点是有效开发系统，通常将安全作为事后考量。这种处理并修补安全漏洞的方式既不可靠，成本又高。从一开始就设计安全的系统是一种更有效的方法。

设计层面的安全周期通过将安全注意事项纳入每个阶段的流程中，与系统发展周期的各个阶段保持一致。其贯穿于所有阶段，因为需要在计划阶段及早识别安全风险，并在后续阶段加以解决。安全风险可通过以下方式解决：

a) 调整规定或部署，以避免已识别的安全风险。

b) 推行替代或缓解控制，将风险降至最低。

c) 必要时通过适当的风险管理流程接受风险。

d) 采用重复流程来评估每个阶段的安全性，并确定是否需要采取额外的安全措施来获得满意的结果。

下图说明设计层面的安全周期如何与系统发展周期并行：

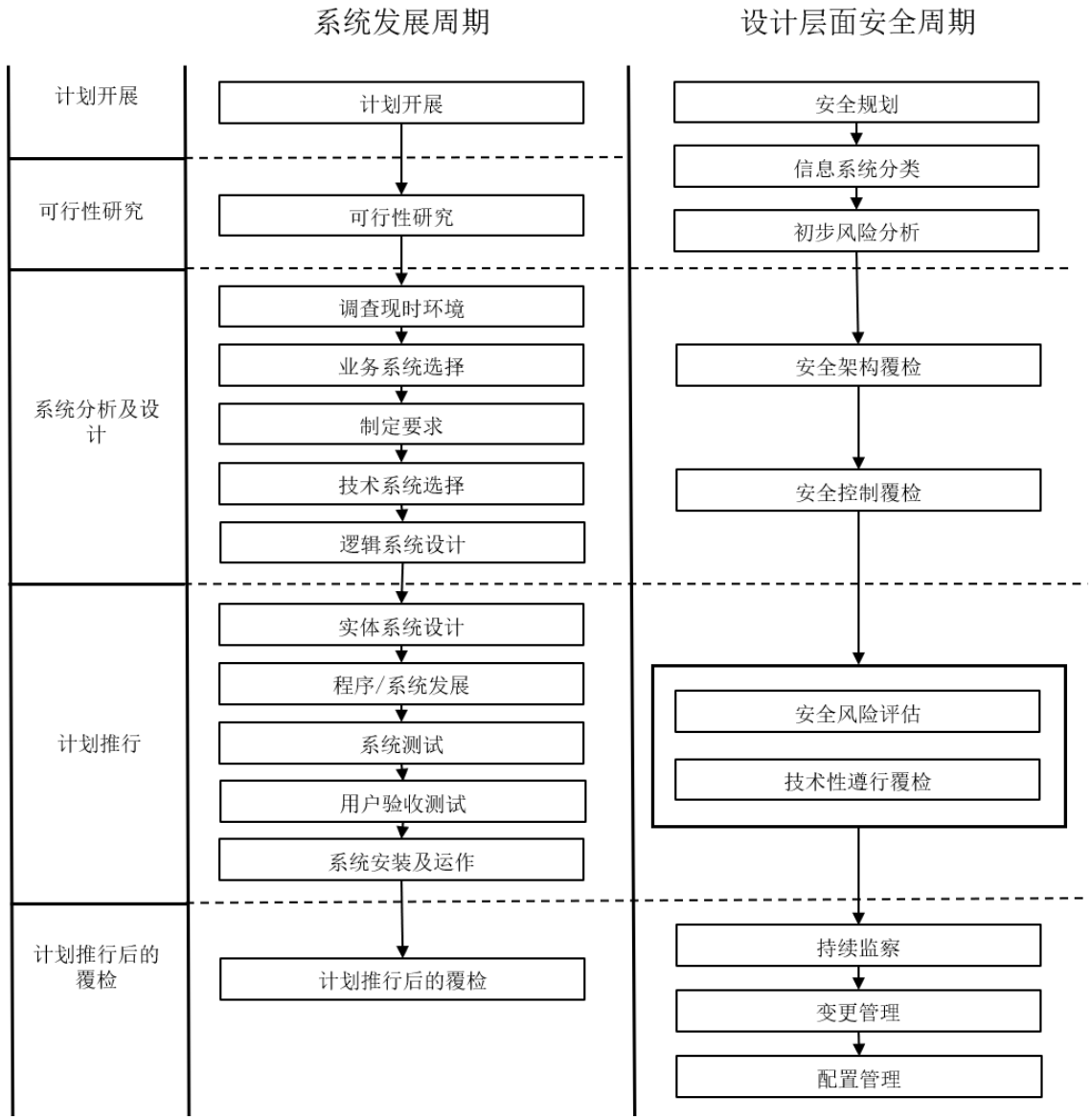

图 3.4：系统发展周期／设计层面安全周期

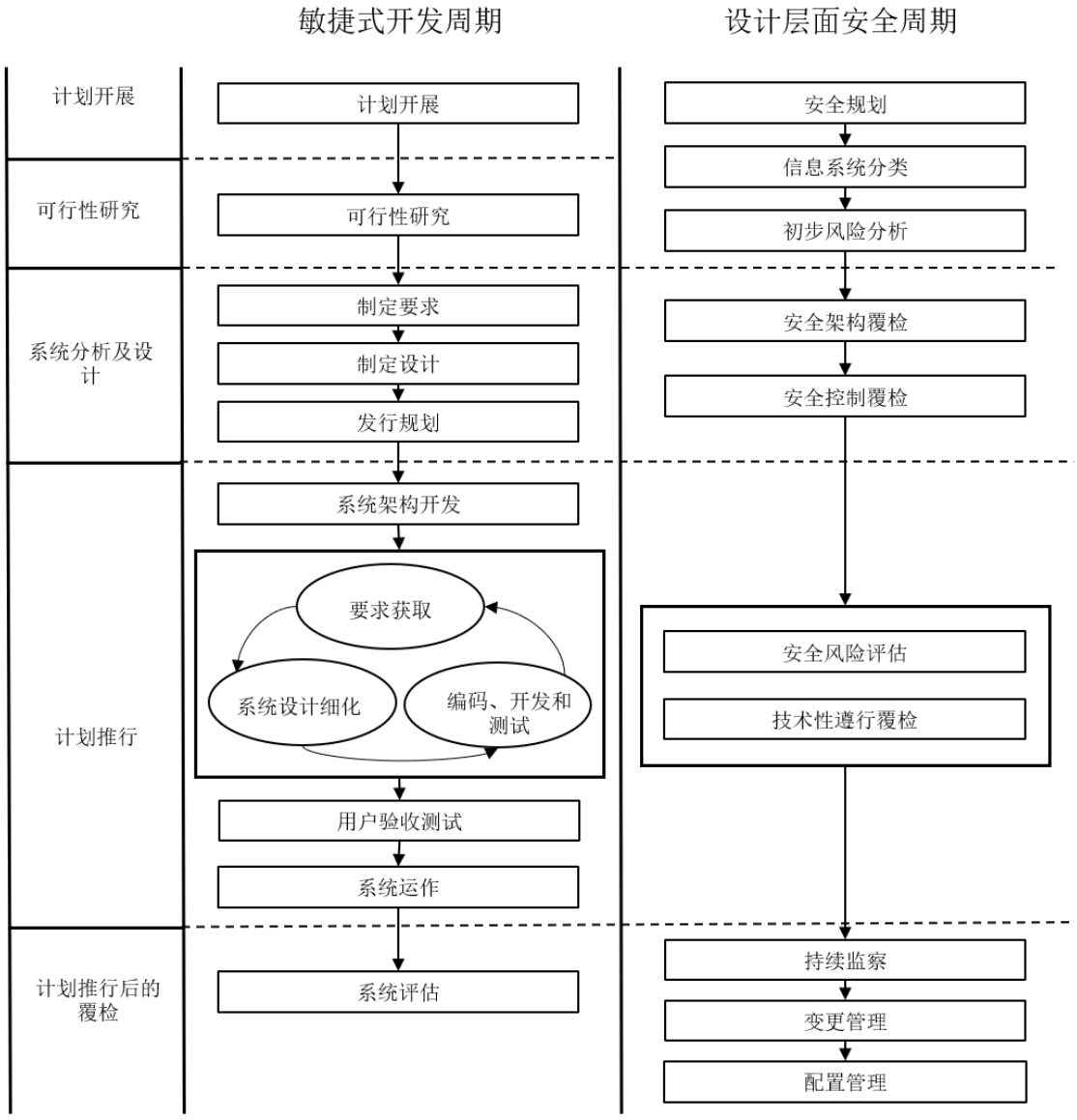

图 3.5：敏捷式发展周期／设计层面安全周期

在系统发展周期每个阶段引入安全性具有多种优势，它确保高级管理层和关键人员能够看到并充分了解安全风险，从而及时做出明智的决定，将风险降低到可接受的水平。通过在整个系统发展周期中纳入安全考量，决策局／部门可以主动解决安全问题，并更有效地将潜在风险降至最低。

3.4 设计层面的安全方法

设计层面的安全方法由三个部分组成，即：

- 生命周期：将安全相关流程与系统发展周期相结合，以指导计划实现设计层面的安全目标。
- 活动：支持安全周期流程的安全相关活动。
- 门控：从安全角度评估系统发展工作的时间点，以及管理层确定计划是否应按原样继续推进、改变方向或终止的时间点。

设计层面的安全方法对于将安全考量纳入安全周期流程各阶段至关重要。该等流程涉及将基本安全元素纳入系统发展周期方法的活动。设计层面的安全流程始于系统发展周期阶段的早期，在整个系统发展周期中对信息系统的安全功能和发展态势的形成发挥着关键作用。

如果未能在系统发展周期的各阶段充分执行该等流程，可能会导致更高的推行成本。因此，在系统发展周期各阶段确定安全流程的优先级，并有效执行，对于建立稳健且具有成本节约效益的安全框架至关重要。

将设计层面的安全方法纳入系统发展周期，对于开发稳健且安全的信息系统至关重要。决策局 / 部门应尽可能采用设计层面的安全原则。在系统发展周期中推行设计层面的安全目标包括：

- ***建立设计层面的安全框架：***创建一个全面的设计层面安全框架，在强制要求采用设计层面的安全方法时，供持份者参考。框架应概述系统发展周期的关键原则、标准和指南。
- ***推行设计层面的安全流程：***制定和推行设计层面的安全流程，确保开始时就管理安全风险，并在整个系统发展周期中持续开展评估。流程应纳入系统发展周期阶段，并遵循周期方法。
- ***开展安全风险评估：***安全风险评估是设计层面的安全流程的一部分，实施安全风险评估，以识别和评估潜在的安全风险和漏洞。定期评估和更新系统的风险状况，以确保采取适当的安全措施。
- ***推行安全活动：***将特定的安全活动纳入系统发展周期中，以有效管理安全风险。安全活动宜包括威胁建模、安全编码实践、安全测试、漏洞扫描和代码审查。确保在适当的系统发展周期阶段，开展安全活动。
- ***门控和决定点注意事项：***在系统发展周期各阶段建立门控和决定点，以确保在未对相关安全风险进行全面评估的情况下，不会作出任何决定。这包括在进入下一阶段之前，开展安全覆检并获得必要的批准。

4 设计层面的安全框架

4.1 框架概述

下图描绘了一种结构化和纪律化的方法，用于整合政府系统发展的安全流程。

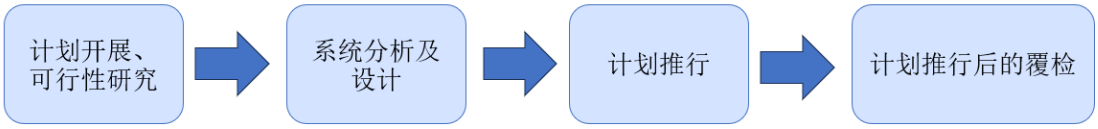

图 4.1：系统发展周期

设计层面的安全框架由四个主要阶段组成，强调持续风险管理，概述如下文。且每个阶段的活动在相应的章节中都有更详细的描述。为有效推行安全管理方法，决策局／部门应在所有安全流程中采用一致的风险管理方法，并应在系统发展周期的所有阶段考虑信息安全。

决策局／部门在系统发展中应采用设计层面的安全方法，确保信息资产的机密性、完整性和可用性，并处理其他安全事宜，以应对不断变化的威胁形势和技术。通过推行直接措施，决策局／部门有效降低并控制与人为和运作问题相关的潜在信息安全风险，将风险维持在可接受和可控的水平。决策局／部门亦应考虑采用适合其业务和运作环境的良好实践。

安全措施和控制措施应具有响应性和适应性，以抵御新出现的安全威胁并降低其风险。决策局／部门应充分了解系统发展中新出现的安全威胁及相关风险。

在设计层面的安全框架中，每个阶段都伴随着一组以安全为重点的活动，该等活动概述了需采取的关键行动。图 4.2 说明了活动相互保持一致及开展的方式。每项活动都包含必要信息，如对将要采取的行动的描述、关键人员的职务和职责以及预期输出，目的都是为了加强系统安全性。

在每个阶段完成后，决策局／部门应进行控制验证，以在进入下一阶段前，评估是否已经充分解决安全考量、是否已经推行足够的安全控制，以及是否已经彻底了解已识别的风险。

4.2 框架推行

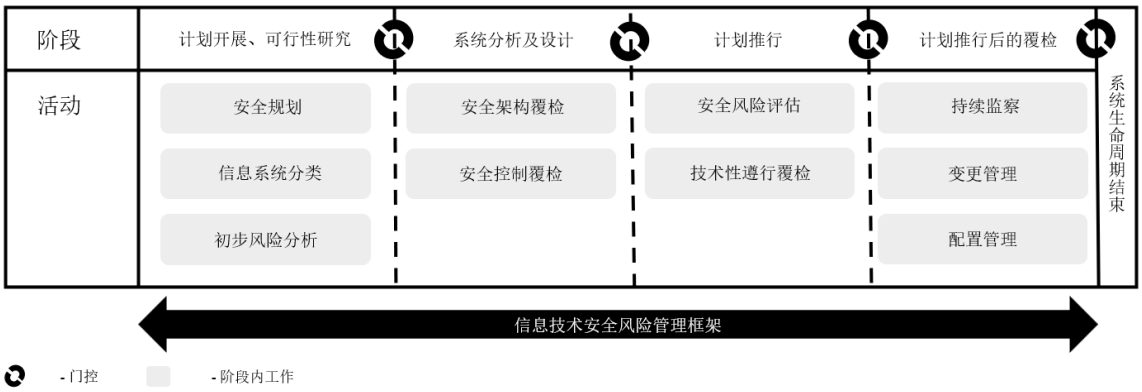

图 4.2 - 设计层面的安全框架

A. 计划开展、可行性研究（第 5 节）

适当的规划可确保识别必要的安全控制、政策和程序。在这一阶段，决策局 / 部门应清楚制定安全目标、范围和系统要求。

这一阶段涉及的主要活动包括：

- 安全规划
- 信息系统分类
- 初步风险分析

B. 系统分析及设计（第 6 节）

系统分析及设计是系统发展周期中的一个重要阶段，系统或应用系统在这一阶段根据制定的需求生成。其目的是评估安全架构，控制待开发的系统或应用系统。通过展开全面覆检，在部署系统前，识别并处理潜在安全漏洞和缺陷，从而增强系统的整体安全性。此外，决策局 / 部门应确保符合政府规例、信息技术安全政策和指南。

这一阶段涉及的主要活动包括：

- 覆检安全架构
- 覆检安全控制

C. 计划推行（第 7 节）

在这一阶段，决策局 / 部门应关注彻底的测试以验证功能，并准备部署系统。

这一阶段涉及的主要活动包括：

- 安全风险评估
- 技术性遵行覆检

D. 计划推行后的覆检（第 8 节）

系统部署后，决策局 / 部门应持续管理、监察和维护已部署的应用系统，以确保其在整个周期内保持安全、稳定和最佳表现。

这一阶段涉及的主要活动包括：

- 持续监察
- 变更管理
- 配置管理

4.3 职务和职责

决策局 / 部门应清楚地制定、识别和授权所有设计系统发展周期涉及的员工职务和职责。系统发展周期涉及的员工通常包括：

4.3.1 高层管理人员（适用于大规模公众面向的资讯科技系统）

- 提供战略性计划领导，并确保与决策局 / 部门的目标保持一致。

4.3.2 信息技术安全管理组

- 在推行安全控制方面的提供安全建议。

4.3.3 资料拥有人

- 制定信息的敏感性、机密性、完整性和可用性要求。
- 对信息进行分类，并将其安全要求传达给项目经理。
- 最终批准推行与其拥有的信息相关的安全控制。

4.3.4 项目经理

- 在商定的约束范围内管理计划，并协调所有活动。
- 协调安全风险管理活动，并确保符合相关的安全标准。
- 确保安全活动被整合到项目计划中。
- 促进团队沟通，以确保安全方法的一致性。
- 根据需要，上报安全风险和事项。

4.3.5 信息技术安全管理员

- 执行特定的安全任务，如识别和缓解系统安全漏洞。

4.3.6 局部区域网络 / 系统管理员

- 管理系统的日常操作，确保安全机制按照设计进行维护。
- 在信息技术安全管理员的指导下，推行配置更改和安全修补程式。

4.3.7 应用系统发展及维修小组

- 开发符合既定程序的系统，并从一开始就纳入安全要求。
- 开展安全编码实践并修复安全漏洞。
- 通过与资料拥有人密切合作，确保整个软件发展周期安全性的持续整合。

4.3.8 用户

- 根据其知识和需求，提供早期阶段输入的有关安全要求的数据。
- 提供有关系统安全性的反馈，并在安全审计中根据需要提供信息和帮助。
- 及时报告任何安全问题。

5 计划开展、可行性研究

适当和超前的规划可确保识别必要的安全控制、政策和程序。在这一阶段，决策局 / 部门应制定系统的安全目标、范围和要求。此外，初步风险分析有助于确定安全工作的优先级，并确定最有效的风险减缓策略。

5.1 活动

规划和评估涉及的主要活动如下：

- 安全规划
- 信息系统分类
- 初步风险分析

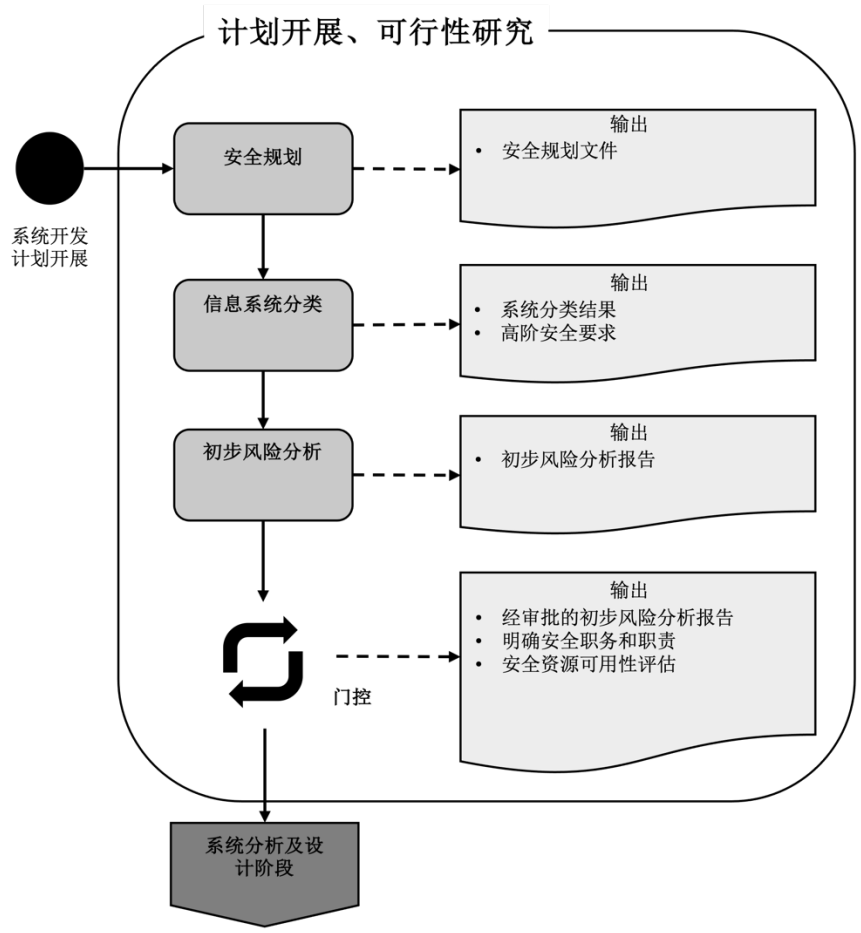

图 5.1：计划开展、可行性研究

5.1.1 安全规划

决策局 / 部门应制定安全规划，并至少涵盖以下内容：

- 制定信息系统安全目标、范围和要求；
- 建立监管架构，明确在系统发展周期内纳入安全的责任；
- 确定相关安全标准、规例和可指导安全计划程序的良好实践；以及
- 概述关键安全事故和活动。

5.1.2 信息系统安全分级

决策局 / 部门须评估信息系统的分级，确保系统受到与相应风险水平相匹配的安全控制措施的保护。有关系统分级的更多详细信息，请参阅以下文件：

- **信息技术安全指南[G3]**
  可于政府资讯科技情报网获取。
  (https://itginfo.ccgo.hksarg/content/itsecure/docs/Guidelines/DocRoadmap_sc.shtml)

5.1.3 初步风险分析

初步风险分析旨在识别信息系统面临的威胁和安全漏洞，明确信息系统面对的风险水平，并推荐适当的保护级别。

该分析流程应包括：

- 识别并分析所有系统资产和相关流程。
- 评估可能影响系统机密性、完整性或可用性的威胁。
- 识别系统安全漏洞和相关威胁。
- 评估潜在影响和风险。
- 确立减低风险的保护要求。
- 选择适当的安全措施，分析风险关系。

在购置情况下，决策局 / 部门应明确具体的安全要求，例如根据信息系统级别确定更严格的安全要求，已确定的风险缓解措施或应包含在招标文件中选定的安全措施。

5.2 职务和职责

5.2.1 应用系统发展及维修小组

- 提供有关高阶安全需求和系统开发风险的技术专业知识。
- 协助系统分级，并从开发角度进行风险分析。

5.2.2 项目经理

- 概述并将关键安全事故和活动写入计划中。
- 确保适当的系统和信息分级，并且及时开展了全面的初步风险分析。
- 协调初步风险分析，确定和评估威胁、漏洞和风险，并确定适当的保护措施。

5.2.3 资料拥有人

- 根据信息分类，传达高阶安全需求。
- 参与风险分析，给出对于特定业务威胁和风险的见解。

5.2.4 用户

- 从用户角度提供对于安全要求和操作风险的见解，增强风险分析的实用性。

5.3 预期输出 / 交付

- 安全计划文件，包含:
  - 信息系统安全目标、范围和要求的清晰定义。
  - 制定的监管架构，明确的具体责任以在系统发展周期内确保安全。
  - 已知确定可指导保安规划流程的相关安全标准、规例和良好实践。
  - 关键安全里程碑和活动的时间线。
- 系统分级结果和依据系统分级的高阶安全需求。
- 初步风险分析报告，报告详述可能影响操作的潜在威胁和风险，以及需推行以减低风险至可接受水平的安全控制。

5.4 门控

计划开展和可行性研究是计划成功进行的基础，建议的控制验证应包含：

控制验证	验证标准	门控操作
批准初步风险分析报告	• 确保初步风险分析报告内容全面且已获得批准，并可用于制定详尽的安全要求和控制。 • 验证初步风险分析报告内容是否包括对潜在影响和风险的评估以及保护要求和建议的安全措施。	• 覆检和批准风险初步分析报告。 • 确认初步风险分析报告将告知详细安全要求和系统设计的后续发展。 • 加入高阶安全需求。
加入高阶安全需求	• 确认初步风险分析报告中囊括所有高阶安全需求。 • 验证高阶安全需求是否指定为需加入系统设计中的安全控制。	• 确保高阶安全需求向详细的系统安全控制过渡过程清晰可溯。
确认职务和职责	• 在项目组中建立并清晰记录职务和职责，尤其是系统发展周期内安全监管有关职务和职责。	• 覆检监管架构和职责文档。 • 从所有项目组成员处获知其安全相关的具体职务和职责。
评估安全资源可用性	• 评估所需时间内用于支持计划的安全资源（包括人员、技术和预算）是否可用和充足。	• 如有必要，展开资源差距分析，并制定资源分配计划。 • 根据资源的可用性、计划时间的可行性，决定计划的进行／不进行状态。

6 系统分析及设计

系统分析及设计是系统发展周期中的重要阶段，系统或应用系统基于制定的需求开始成形，其目的是评估正在开发中的系统或应用系统的安全架构和控制。在部署系统前，通过全面覆检识别并处理潜在安全漏洞和缺陷，从而增强系统的整体安全性。此外，涉及购置第三方或商业现成软件时，决策局／部门应确保所购置的系统或服务符合政府规例、信息技术安全政策及指南。

6.1 活动

这一阶段，主要有两项活动：

- 覆检安全架构
- 覆检安全控制

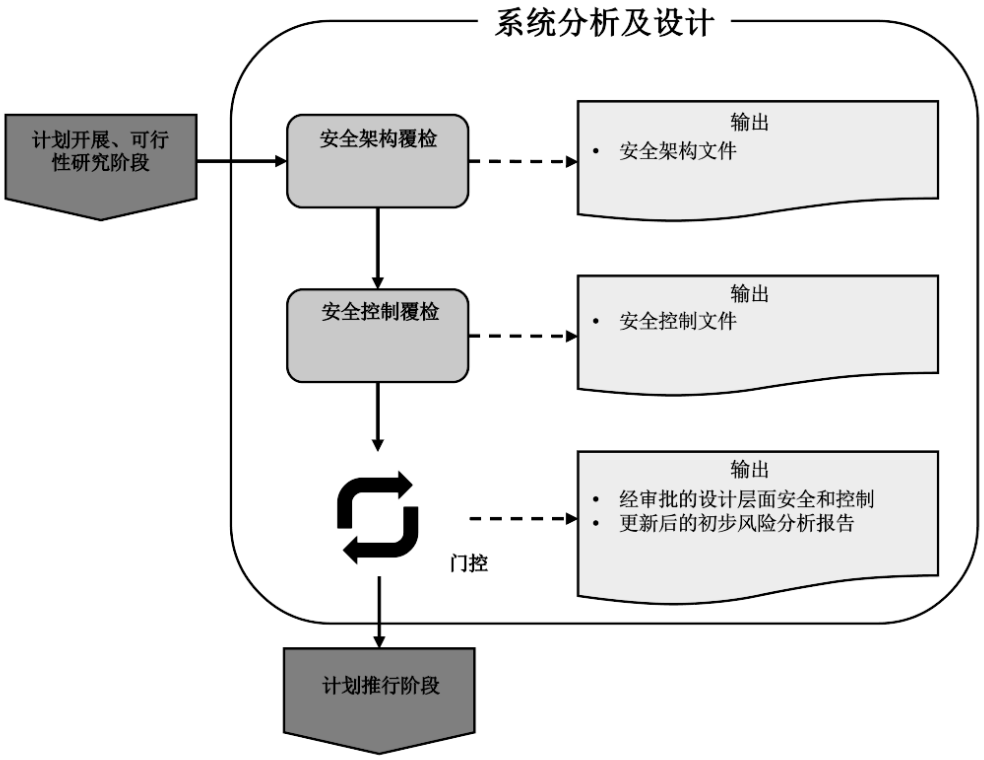

图 6.1 系统分析及设计

6.1.1 覆检安全架构

决策局 / 部门应全面覆检系统或应用系统的安全架构，评估安全措施的设计和推行情况，识别任何潜在差距或安全漏洞。决策局 / 部门应重点覆检确保安全架构与行业良好实践，规管和政府安全要求一致，包括所需安全控制，遵行相关标准和规例，安全数据处理要求以及供应商的任何具体安全期望。

6.1.2 覆检安全控制

决策局 / 部门应评估系统或应用系统内推行的安全控制的有效性，确保安全控制保护系统或应用系统能够抵御潜在威胁，缓解风险，并与制定的安全要求和标准保持一致。如购置，决策局 / 部门应评估潜在供应商的安全能力是否满足制定的安全要求。

决策局 / 部门评估潜在供应商的安全能力时，宜评估以下方面：

- 安全管理实践；
- 事故应变能力；以及
- 安全认证。

决策局 / 部门应根据评估结果制备一份报告，用作供应商选择流程中的决定依据。

该报告应包括以下内容：

- 第三方风险评估
- 遵行和认证情况
- 评估标准和得分情况
- 建议及决定

该报告应为选择合适供应商的综合依据，确保系统性地解决了所有安全考量。

6.2 职务和职责

6.2.1 信息技术安全管理组

- 在系统设计阶段，提出必要的安全措施和控制的专业建议。

6.2.2 资料拥有人

- 根据信息分类制定信息安全要求。
- 批准用于保护资料拥有人所拥有信息的安全控制。

6.2.3 项目经理

- 确保将安全措施无缝集成到系统设计中。
- 协调新系统的安全架构审查，确保符合相关标准。
- 确保建议的安全架构和控制措施符合决策局 / 部门的业务目标和安全要求。
- 确保各方就安全考量沟通一致。
- 确保制定的安全要求与投标要求一致，如购置，确保已提出安全评估建议并已纳入投标评估。

6.2.4 信息技术安全管理员

- 在系统设计阶段执行安全相关具体工作，例如建议设计的安全漏洞评估。

6.2.5 局部区域网络 / 系统管理员

- 提出对建议安全架构可管理性和可维护性的见解。
- 计划未来将推行的安全配置和修补程序管理。

6.2.6 应用系统发展及维修小组

- 开发包含安全控制的系统设计。
- 计划对设计潜在安全漏洞的补救。
- 负责在系统发展周期其余阶段持续整合安全。

6.2.7 用户

- 为系统提供安全要求和期望。
- 对系统设计中安全措施相关的潜在可用性问题提供反馈。
- 承诺报告任何在建议设计中发现的安全缺陷。

6.3 预期输出 / 交付

- 安全架构文件：
  全面概述了系统或应用系统中的安全架构，包括：

  - ***系统概况：***对系统、系统组件和系统用途的整体描述。
  - ***安全目标：***确立机密性、完整性和可用性的安全目标。
  - ***网络架构：***网络设置的架构图和说明，包括分段、防火墙和非军事区。
  - ***组件设计：***各系统组件的详细安全信息，包括服务器、数据库和应用系统。
  - ***数据流：***数据在系统内流动的可视化呈现或描述，以识别数据可能有风险的地方。
  - ***访问控制：***认证机制和授权机制的描述，包括基于角色的访问控制矩阵。
  - ***加密方法：***静止和传输中的数据加密标准详情。
  - ***入侵检测防御：***概述侦测和预防未授权访问或异常的机制。
  - ***安全规约：***所有安全规约的清单，比如通讯安全的传输层安全协议。
  - ***遵行标准：***识别相关遵行标准和系统架构的遵行情况。
  - ***安全域：***网络安全域的定义和其分隔及保护方法。
  - ***复原能力和容错能力：***，确保系统即使在组件故障或受到攻击期间仍能安全运行的设计选择。

- 安全控制文件：
  详述了所推行的具体安全措施以及其对构建系统整体安全态势的作用。
  - ***控制清单：***所有推行的安全控制清单，包括防火墙、杀毒软件、入侵检测系统等。
  - ***控制描述：***详细描述在系统中每一项控制的功能、配置和操作。
  - ***风险缓解：***分析每一项控制如何具体缓解的已识别风险。
  - ***分层防御：***说明安全控制如何协同工作，以创造分层（或纵深防御）安全策略。
  - ***遵行对应映射：***安全控制与遵行要求的相互参照，显示每个安全控制如何满足特定要求。
  - ***控制拥有权：***每项控制的负责人信息，包括控制拥有者或保管人的联系信息。

6.4 门控

决策局 / 部门在开发系统前，应验证并接受建议的安全设计和控制。初步风险评估的更新和变更应反映安全要求和设计变更。建议的控制验证包括以下内容：

控制验证	验证标准	门控操作
验证安全设计和控制	安全设计与控制与决策局 / 部门架构标准和政策一致。	覆检并批准建议的安全设计和控制。
与决策局 / 部门架构一致	决策局 / 部门现有架构中整合的系统设计，包括安全组件。	确认决策局 / 部门架构中已加入系统设计并保持一致；寻求批准。
遵行安全要求	所有议定的安全要求已在系统设计阶段履行。	验证要求是否已履行；记录持份者正式接受系统设计。
正式接受系统设计	关键持份者同意建议的系统设计满足项目目标和安全要求。	获得关键持份者对系统设计的正式批准。
初步风险分析的更新与变更	初步风险分析反映当前安全要求和设计。	更新风险分析以包含变更；重新验证安全风险与控制。

7 计划推行

在计划推行阶段，决策局 / 部门应循序渐进，首先进行全面的安全风险评估和严格的技术性遵行覆检。这流程在验证系统功能，识别、分析和评估安全风险以及确保遵行技术标准中发挥关键作用。在此阶段，持续监察对确保随着系统演化而相应调整安全态势至关重要。

7.1 活动

计划推行阶段的主要活动如下：

- 安全风险评估
- 技术性遵行覆检

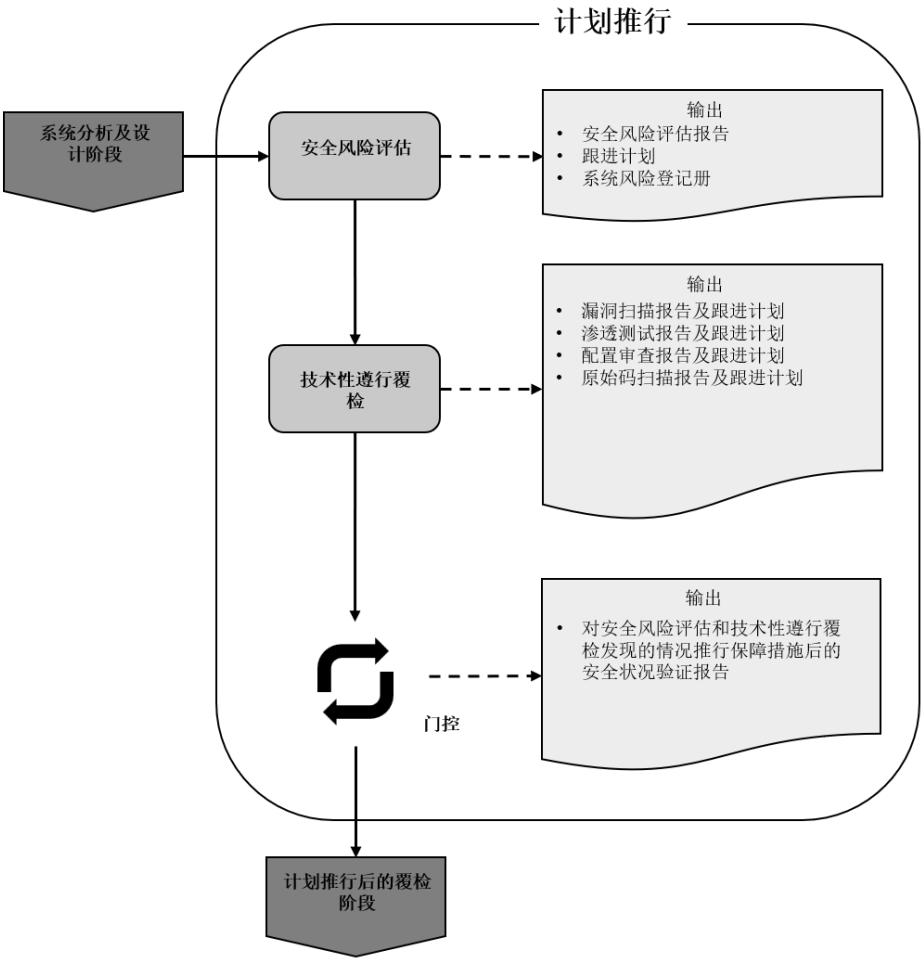

图 7.1 计划推行

7.1.1 安全风险评估

决策局 / 部门应展开安全风险评估，以识别、分析和评估安全风险，并决定风险处理措施，以将风险降至可接受的水平。系统评估的过程应包括识别并分析：

- 系统所有资产和相关流程
- 可能影响系统机密性、完整性或可用性的威胁
- 系统安全漏洞和相关威胁
- 威胁的潜在影响和风险
- 缓解风险的保护要求
- 选择适当的安全措施并分析风险关系

为使分析结果精确可用，应提供一份系统的完整清单和安全要求，作为识别和分析活动的输入。与相关者访谈，例如局部区域网络 / 系统管理员、资料拥有人、用户等，也可以为分析提供额外资料。根据评估范围、要求和方法，分析宜使用自动化的安全评估工具。评估所有收集的信息后，应报告所发现风险清单。就每项发现的风险，决策局 / 部门应确定在系统推行前部署适用的安全措施。

有关开展安全风险评估的更多详细信息，请参阅以下文件：

- **安全风险评估及审计实务指南**
  可于政府资讯科技情报网获取。
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

7.1.2 技术性遵行覆检

决策局 / 部门应在计划推行阶段进行安全漏洞扫描、渗透测试、配置审查和 / 或原始码扫描。在系统运作或提供正式服务前，应评估所确定的安全漏洞及问题，并采取适当修正行动处理。决策局 / 部门应制定建议跟进计划，包含计划推行时间表，并在计划推行保护措施后，覆检安全状况。

有关技术性遵行覆检的更多详细信息，请参阅以下文件：

- **信息技术安全指南[G3]**
  可于政府资讯科技情报网获取。
  (https://itginfo.ccgo.hksarg/content/itsecure/docs/Guidelines/DocRoadmap_sc.shtml)

7.2 职务和职责

7.2.1 信息技术安全管理组

- 在需要时就系统推行过程中的安全措施和控制提供建议。

7.2.2 项目经理

- 安排安全风险评估和技术性遵行覆检流程。
- 监察技术性遵行覆检的执行情况，确保已识别的漏洞得到解决。
- 确保在系统运作前，已采用并验证评估建议。

7.2.3 信息技术安全管理员

- 协助进行安全风险评估和技术性遵行覆检。

7.2.4 局部区域网络 / 系统管理员

- 协助进行安全风险评估和技术性遵行覆检，提供信息配置详情，采纳变更建议。

7.2.5 应用系统发展及维修小组

- 参与安全风险评估，提供有关系统组件和潜在安全漏洞的信息。
- 按照既定的时间线修复在技术性遵行覆检期间发现的任何安全漏洞。

7.2.6 用户

- 协助开展安全风险评估和技术性遵行覆检，反馈用户对系统安全的关注点。

7.3 预期输出 / 交付

- 安全风险评估报告及其跟进计划
- 系统风险记录册
- 安全漏洞扫描报告及其跟进计划和验证报告
- 渗透测试报告及其跟进计划和验证报告
- 配置审查报告及其跟进计划和验证报告
- 原始码扫描报告及其跟进计划和验证报告

7.4 门控

在计划推行阶段，建立并测试系统。决策局/部门应评估所推行安全措施的有效性。建议的控制验证包含以下：

控制验证	验证标准	门控操作
记录安全风险和缓解风险的措施	将所有识别的安全风险和采取的缓解威胁的策略准确记录在风险记录册中。	• 覆检风险记录册，确保信息完整和准确。 • 在推进前，批准风险记录册。
与决策局 / 部门架构保持一致	根据系统设计阶段的要求推行安全控制。	• 根据要求检查和验证安全控制。 • 在推进前，确认已正确且完整地推行安全控制。
完成缓解风险工作	妥善处理并记录在安全风险评估与技术性遵行覆检中开展的缓解风险工作。	验证每项缓解风险工作，确保充分缓解安全风险或安全风险可接受，并获得正式批准。

8 计划推行后的覆检

决策局 / 部门应维持在所部署系统的持续管理、监察及维护的机制，确保解决方案在其整个生命周期内持续、安全、稳定和发挥最佳性能。

8.1 活动

测试和计划推行阶段的主要活动如下：

- 持续监察
- 变更管理

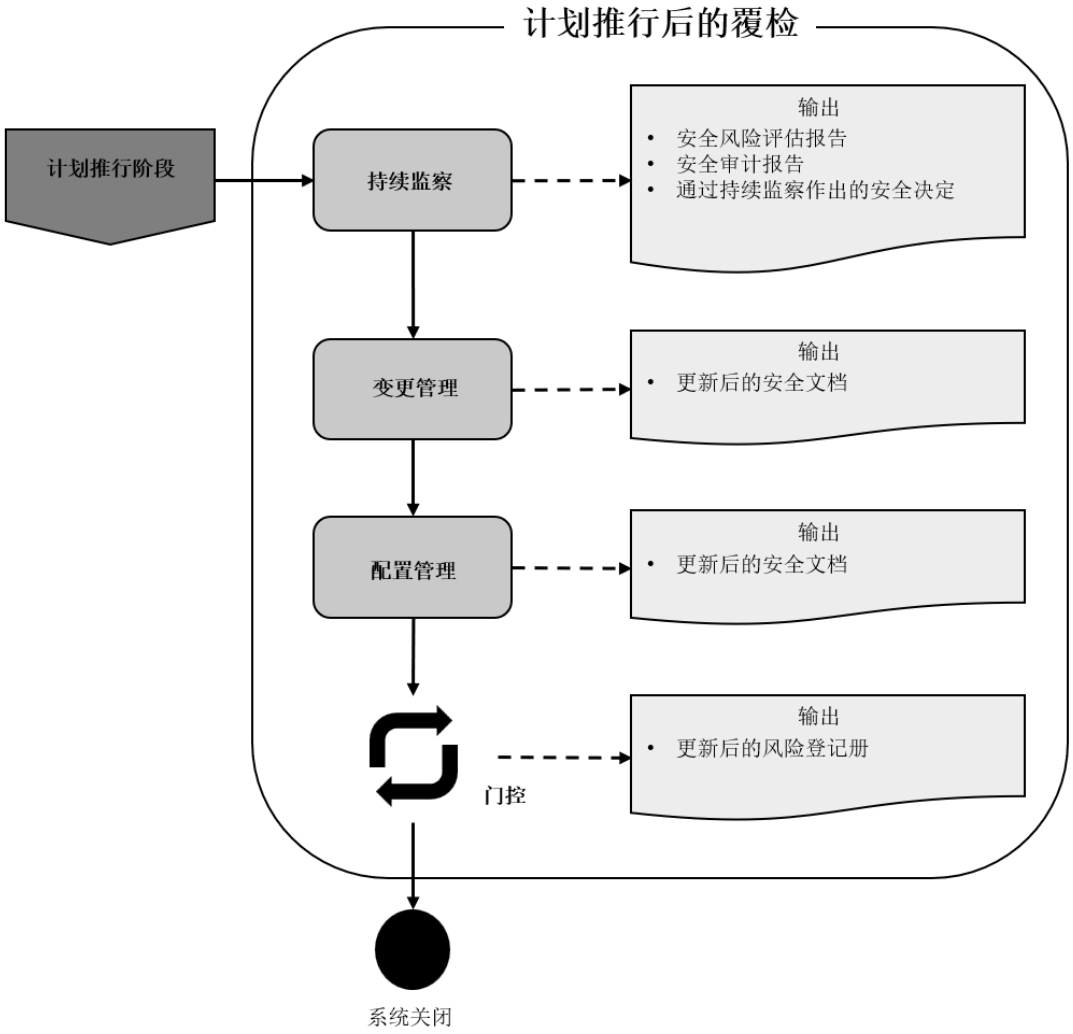

图 8.1 计划推行后

8.1.1 持续监察

决策局 / 部门应定期开展全面的安全风险评估，评估系统安全控制政策和程序，从而识别潜在安全漏洞或缺陷。持续监察属于安全审计内容。随着时间的推移，考虑到系统和环境变更，持续监察是确保安全控制有效性的重要活动。

安全风险评估应包含技术资产、技术安全控制，并涉及对安全政策的全面覆检，例如与可接受使用和网络权利相关的政策。这流程将决定行政上安全控制的效力。

通过安全审计，决策局 / 部门可持续监察安全架构，以验证安全控制是否按预期运行，并根据任何发现修改或更新安全措施。这种积极主动的方法确保安全措施发展与安全威胁的动态性质和决策局 / 部门不断变化的环境保持一致。

8.1.2 变更管理

决策局 / 部门应以可控且安全的方式管理并执行系统变更，定期更新安全文件为基础。系统变更控制不足是系统或安全故障的常见原因。从开发到生产阶段，操作环境的任何变更都会显著影响系统的安全态势。

为解决此问题，决策局 / 部门应：

- ***记录所有建议的变更：***保留所有建议系统变更的详细记录，并分析其潜在的安全影响。
- ***更新安全文件：***确保安全文件随系统的任何变更更新，以反映系统的新状态以及对安全控制或程序的任何变更。
- ***进行安全影响分析：***在推行变更之前，执行严格的安全影响分析，了解变更可能对系统安全性产生的影响。
- ***沟通变更：***与所有持份者沟通任何变更和相关的安全影响，更新培训材料以补充新的安全实践。
- ***监察变更推行后：***在推行变更之后，监察系统以验证安全控制是否依然有效，并且更新的文档是否准确显示系统的新状态。

通过此流程，决策局 / 部门将确保系统安全，及所有持份者可访问最新且准确的安全信息，从而推动持份者做出明智的决定，并在整个变更管理周期内，维护安全态势的完整性。

8.1.3 配置管理

配置管理是建立并维护系统安全基准必不可少的环节，可准确控制并保持系统变更清单。鉴于系统配置变更可显著影响系统安全，因此在配置管理流程中加入更新后的安全文档十分重要。关键考量和良好实践包括：

- ***维持更新后的基准：***建立并记录配置基准，确保每当发生变更时都会更新此基准。该文档应随时反映系统配置的当前状态。

- ***通过文档更新进行持续监察：***持续监察并定期审核配置变更，更新安全文档，以撷取系统配置的任何变更。这确保可追踪和评估所有变更的安全影响。

- ***明文规定的备份和复原程序：***推行并记录配置备份和复原程序。更新后的安全文档应包括复原程序、职务、职责和时间线，以确保在发生配置相关事故时能迅速复原。

- ***在安全文档中加入配置变更：***确保所有已批准的配置变更及时在安全文档中反映，包括记录变更理由、安全影响分析，以及推行的任何缓解措施。

- ***自动化工具和人工覆检：***按照安全程序中的明文规定，利用自动化扫描工具并进行人工覆检，以验证配置已正确设置，且符合安全良好实践。应记录使用的工具和覆检的结果，并用于更新安全基准和实践。

配置管理的目标在于识别和修正可能导致安全漏洞的潜在错误配置，进而危及信息系统安全。在确保配置管理中加入更新的安全文档后，决策局 / 部门可维持稳健的安全态势，以回应变化并反映最新的配置状态。

8.2 职务和职责

8.2.1 信息技术安全管理组

- 对变更管理和配置管理实践的安全方面提供建议。

8.2.2 资料拥有人

- 确保在持续监察、变更和配置管理活动中考虑信息的安全分类。

8.2.3 信息技术安全管理员

- 领导持续监察活动，以识别和评估潜在的漏洞。
- 因系统变更对系统保安产生的潜在影响进行评估。
- 因配置变更对系统保安产生的潜在影响进行评估。
- 协助推行已批准的变更和配置调整。

8.2.4 局部区域网络 / 系统管理员

- 执行配置变更和安全修补程式，作为变更管理指令的一部分。
-
- 通过维护操作安全控制来支持持续的监察工作。

8.2.5 应用系统发展及维修小组

- 确保已安全并入通过持续监察反馈做出的变更。
- 管理应用系统发展和维护中的配置变更。

8.2.6 用户

- 参与持续监察，报告遇到的任何异常或安全问题。
- 遵行新的配置或变更，作为变更管理沟通的一部分。
-

8.3 预期输出 / 交付

- 安全风险评估报告及其跟进计划
- 安全审计报告及其跟进计划
- 通过持续监察作出的安全决定
- 更新安全文件
- 更新风险记录册

8.4 门控

使用系统时，决策局 / 部门应依据用户反馈、技术变更、政策变更、新出现的威胁和安全漏洞以及其他业务相关问题，定期重新评估系统状态。建议的控制验证包含：

- 验证安全风险评估和安全审计报告，确保已处理系统和环境变更。
- 定期覆检之前的安全风险评估报告和风险记录册，确保风险仍然有效并持续处理风险。

控制验证	验证标准	门控操作
持续监察活动	• 内建控制的有效性。 • 监察报告的时间线和准确性。	• 按需要调整监察策略。 • 更新控制配置。 • 提供针对新出现威胁的培训。
验证安全风险评估和审计报告	• 风险的相关性和覆盖范围。 • 根据系统 / 环境变更进行充分的控制。	• 更新风险评估方法。 • 修复识别的差距。 • 上报重大风险至高层管理人员。
定期覆检之前的安全风险评估和风险记录册	• 验证之前的风险评估。 • 风险记录册中风险的当前状态。	• 按照风险的缓急次序采取措施。 • 分配资源作减低风险。 • 更新风险记录册。

完