数字政策办公室

信息安全

信息技术安全风险管理
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

信息技术安全风险管理是帮助组织主动识别和评估可能影响其目标的潜在信息技术安全风险并确定风险优先权的重要流程。本文件提供参考模型，以使信息技术安全风险管理实务和方法保持一致。通过参考该模型，管理用户、信息技术经理、系统管理员以及其他技术和操作人员能更好地了解信息技术安全风险管理流程，亦能了解必要的准备事项、关键考虑因素和可实现结果。本文件旨在为决策局 / 部门提供全面框架，以开展符合其特定需求和背景的有效定制信息技术安全风险管理实务。

1.1 目的

本文件描述了信息技术安全风险管理的总体框架，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）。

本实务指南适用于所有参与信息技术安全风险管理的员工，以及为政府信息技术安全风险管理流程提供支持的信息技术安全顾问或审计师。

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
- 信息安全、网络安全和私隐保护-信息安全管理系统-要求，ISO/IEC 27001:2022
- 信息安全、网络安全和私隐保护-信息安全控制措施，ISO/IEC 27002:2022
- 信息安全、网络安全和私隐保护-信息安全风险管理指南，ISO/IEC 27005:2022
- 风险管理-指南，ISO 31000:2018
- NISTIR 8286 整合网络安全和企业风险管理（ERM）
- NISTIR 8286A 识别和评估企业风险管理的网络安全风险
- NISTIR 8286B 确定企业风险管理的网络安全风险优先权
- NISTIR 8286C 为企业风险管理和治理监管对网络安全风险分级
- GB/T 31722-2015 信息技术-安全技术-信息安全风险管理
- GB/T 20984-2022 信息安全技术-信息安全风险评估方法
- GB/T 24353-2022 风险管理-指南
- GB/T 22080-2016 信息技术-安全技术-信息安全管理体系-要求

- 信息技术安全威胁管理实务指南
- 安全风险评估及审计实务指南

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》[S17]和《信息技术安全指南》[G3]内所使用，以及以下的定义及惯用词。

缩写及术语	
信息技术安全	信息技术安全是保护网络、装置和数据免遭未获授权访问或非法使用的技术，是确保信息机密性、完整性和可用性的实践。
风险管理	指导和控制组织风险的协调活动。
信息技术安全风险管理	持续对与人为和/或操作问题相关的潜在信息技术安全风险进行识别、确定其优先权并采取风险缓解和控制措施以使其达到可接受且可管理水平的过程。
利益相关者	可能受决策或活动影响或认为自己会受决策或活动影响的个人或组织。

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、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，并采取信息安全的行业最佳实践。

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／部门可以利用威胁情报网络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。

人员亦可通过参加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）的专题网页来提高安全意识。

3. 信息技术安全风险管理

3.1 信息技术安全风险管理简介及其重要性

信息技术安全风险与信息、数据或信息（或控制）系统的机密性、完整性或可用性的丧失有关。该风险反映了对组织营运（即使命、职能、形象或声誉）、资产、个人、其他组织和社会的潜在不利影响。

有效的信息技术安全风险管理是一个重要的过程，涉及识别、评估和缓解组织的信息系统、数据和技术基础设施的风险，以及识别可能危及数字资产机密性、完整性和可用性的漏洞和威胁。组织有必要通过实施稳健的策略将信息技术安全风险缓解到其制定的可接受水平。

在数字化时代，信息技术安全风险管理对于保护敏感信息、关键基础设施和业务连续性至关重要。由于对技术的依赖日益增加，与信息技术威胁相关的潜在风险和漏洞越发普遍。通过实施稳健的风险管理实务，决策局 / 部门可主动识别和解决潜在安全漏洞，并实现以下目标：

- 保护敏感数据、知识产权、客户信息和关键系统等重要资产。
- 提高潜在信息技术安全风险的可见性，从而更好地分配资源和作出决策。
- 向管理层提供对现有信息技术安全风险状况和相应安全保障措施全面且系统的意见。
- 降低信息技术安全事故发生的可能性和影响，保持业务连续性。
- 确保组织遵行相关的信息技术安全法例和监管要求，避免潜在法律处罚和声誉受损。

风险管理不到位可能会给各决策局 / 部门带来严重后果。例如，数据泄露可能导致未获授权披露敏感信息，从而造成法律和监管影响。此外，关键数据的丢失或损害可能会扰乱政府的必要服务、破坏公众的信任和信心。

3.2 信息技术安全风险管理框架

为确保信息技术安全风险管理的一致性与有效性，决策局 / 部门须制定全面的信息技术安全风险管理框架，概述如何识别、评估、缓解和监控决策局 / 部门及其系统相关风险。稳健的框架能够提供管理信息技术安全风险的结构化方法，有助于组织全面了解潜在威胁和漏洞。按框架行事，决策局 / 部门可加强其信息技术安全态势并有效管理信息技术安全风险。

信息技术风险管理框架通过一系列的风险管理活动和职能来提供结构化的风险管理方法。信息技术安全风险管理的有效性取决于其在决策局 / 部门治理（包括决策）方面的融合程度，需要利益相关者，尤其是高层管理人员的支持。信息技术安全风险管理框架的关键组成部分如下图。

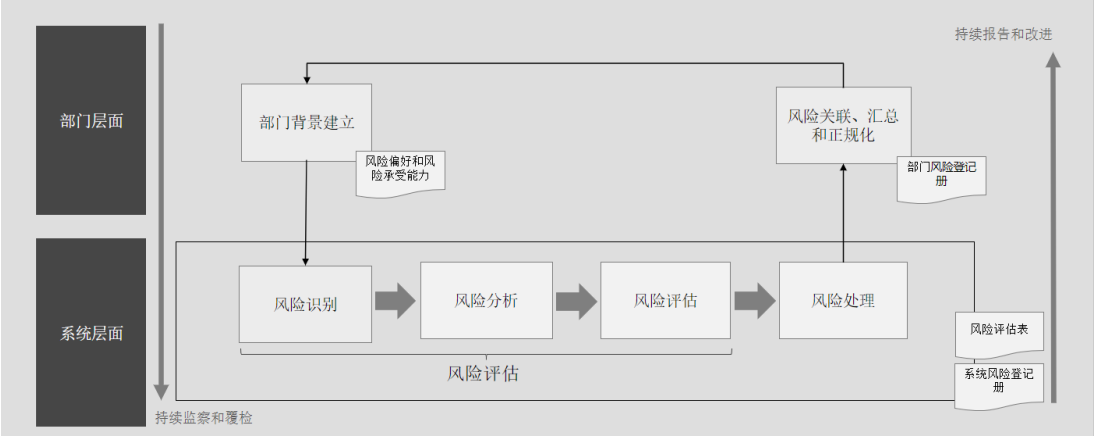

图 3.1：信息技术安全风险管理框架

i) 部门背景建立（第 3 节）
了解和制定可能影响决策局 / 部门信息技术安全风险整体管理的内部和外部背景。

ii) 风险识别（第 4 节）
识别和记录可能影响决策局 / 部门信息系统和数据的潜在信息技术安全威胁和漏洞。

iii) 风险分析（第 4 节）
进一步分析识别到的风险，了解其潜在影响和可能性。这有助于全面了解各项风险对决策局 / 部门营运和目标的潜在影响。

iv) 风险评估（第 4 节）
将经过分析的风险与决策局 / 部门风险标准进行比较，确定风险优先权。这有助于确定各项风险的重要性以及需要处理的风险。

v) 风险处理（第 4 节）
在风险评估后，建立适当的处理方案来管理风险。决策局 / 部门可通过采取控制措施来避免、转移、缓解或接受风险，具体取决于决策局 / 部门风险偏好。

vi) 风险关联、汇总和正规化（第 5 节）
审查风险之间的相互关系，总结和评估风险的总体影响，将风险计量正规化。这有助于全面了解决策局 / 部门风险环境并帮助其制定战略决策。

迭代法可在每次迭代时增加评估深度和细节，平衡识别控制所花费时间和精力，并确保风险得到适当评估。

3.3 信息技术安全风险管理政策

信息技术安全风险管理政策为正式的信息技术安全管理框架文件，应概述决策局 / 部门业务目标、需防范的威胁以及任何适用的法律和监管要求。信息技术安全风险管理政策还应自上而下说明需保护的资产，并且决策局 / 部门将不会容忍任何违规行为。在建立信息技术安全风险管理政策时，决策局 / 部门应参考本实务指南并根据其战略和目标确定风险管理方法，如风险评估方法、风险评级机制及关键绩效指标。信息技术安全风险管理政策就决策局 / 部门应如何保护其信息资产、系统和网络免受潜在威胁和漏洞提出要求并提供指南。政策的具体内容可能因决策局 / 部门规模、复杂程度、行业和监管要求而异，但通常包含以下要素：

- 目的和范围
- 职务和职责
- 在决策局 / 部门内部制定和执行安全风险管理框架
- 遵行和执行
- 培训和意识
- 政策的覆检和批准

决策局 / 部门应根据需要建基於此补充相应的标准和指南。

4. 部门背景建立

部门背景建立可定制风险管理流程，使决策局 / 部门能够有效评估并适当处理风险。

4.1 风险管理范围制定

制定各决策局 / 部门信息技术安全风险管理活动范围至关重要。

明确的范围可帮助决策局 / 部门针对性地开展有效的风险管理工作。风险管理范围制定包括建立全面的风险评估所涉信息系统及其组成部分清单。相关信息应记录在信息系统清单中。风险管理范围应包括网络图或系统架构图，直观呈现系统内部和外部的连接、决策局 / 部门对系统的控制范围及各系统所依赖的外部系统或服务。

制定风险管理范围至关重要，关系到决策局 / 部门了解自身对其他政府实体或外部利益相关者的依赖关系，有助于促成合作和协调，以应对不同领域的信息技术安全风险。

明确制定范围至关重要，同时需要考虑以下各方面要素：

- 待制定的目标和决策。
- 流程步骤的预期结果。
- 时间、地点、包含及不包含的具体内容。
- 合适的风险评估工具和技术。
- 所需资源、职责和记录方式。
- 与其他项目、流程和活动的关系。

通过建立明确制定的范围， 决策局 / 部门可以根据行业最佳实践加强其信息技术安全风险管理实务， 有效应对潜在风险。

4.2 了解风险背景

决策局 / 部门在其目标、资产、威胁、漏洞和法律/监管要求形成的独特风险背景下运作。全面评估和了解这一特定风险背景对决策局 / 部门至关重要。考虑这些因素能够深入了解潜在风险，从而制定合适的风险管理策略。决策局 / 部门应收集、考虑并了解内部和外部背景因素。

外部背景因素包括但不限于以下例子：

- 国际、国内、区域或本地的社会、文化、政治、法律、监管、金融、技术、经济和环境因素。
- 影响决策局 / 部门目标的关键驱动因素和趋势。

- 外部利益相关者的关系、看法、价值观、需求和期望。
- 合同关系和承诺。
- 网络复杂性和依赖关系。

内部背景因素包括但不限于以下例子：

- 愿景、使命和价值观。
- 治理、结构、职务和问责。
- 战略、目标和政策。
- 文化。
- 决策局 / 部门采用的标准、指南和模型。
- 根据资源和知识（如资本、时间、人员、知识产权、流程、系统和技术）理解的能力。
- 数据、信息系统和信息流。
- 与内部利益相关者的关系，对其看法和价值观的考虑程度。
- 合同关系和承诺。
- 相互依存和相互联系。

4.3 风险偏好声明及风险承受能力标准制定

风险偏好声明和风险承受能力标准对决策局 / 部门信息技术安全风险管理框架内的决策至关重要。其有助于建立可接受的风险水平并指导确定风险缓解工作的优先权。确保风险偏好和风险承受能力与风险管理框架相符，并根据活动的具体目的和范围进行调整。其还应反映决策局 / 部门的价值观、目标和资源，并与信息技术安全风险管理政策和指南相符。

风险偏好代表决策局 / 部门在实现目标时愿意接受的风险水平。而风险承受能力为一个阈值，超过该阈值的风险属于不可接受的风险。决策局 / 部门应在信息技术安全风险管理政策中注明其风险偏好及风险承受能力，据此建立风险管理战略方法。尽早建立风险偏好及风险承受能力并定期覆检，以确保其符合决策局 / 部门不断变化的目标和风险环境。

制定风险偏好声明及风险承受能力标准时应考虑决策局 / 部门的责任和利益相关者的意见。风险偏好声明及风险承受能力标准应在风险评估流程开始时建立，必要时应定期覆检和修订。

制定风险偏好声明及风险承受能力标准时应考虑以下因素：

- 可能影响结果和（有形和无形）目标的不确定因素的性质和类型。
- （正面和负面）影响和及其可能性的定义和衡量方法。
- 时间相关因素。
- 计量方法的一致性。
- 风险水平的确认方法。
- 对多种风险组合和顺序的考量。
- 决策局 / 部门的能力。

4.3.1 风险偏好

风险偏好反映决策局 / 部门根据其目标、战略目标、优先权和风险文化承担风险的意愿。高风险偏好意味着决策局 / 部门愿意承担较多风险以实现目标，低风险偏好意味着决策局 / 部门愿意承担的风险较少。风险偏好可以是定性的，也可以是量化的。决策局 / 部门应根据既定风险偏好调整其信息技术安全策略，为各部门安全意识和风险意识树立基调，从而使决策局 / 部门平衡创新与风险缓解措施，确保将风险控制在可接受范围。通过明确风险偏好，决策局 / 部门能够建立风险评估及应对框架，指导决策过程并与总体目标保持一致。定性或定量风险偏好在制定风险承担范围方面均会考虑潜在利益和负面影响。确定风险偏好有助于在部门层面采取一致且明确的风险管理方法。

风险偏好示例：

- 对重要系统的停机时间，组织的风险偏好为 0.2%的黄色阈值。
- 对特定国家办事处负面媒体报道，组织的风险偏好为 2 个及以上的红色阈值。
- 对国内供应链风险，组织的风险偏好较高。
- 对投资于可能实现显著营运改进和创新的领域，组织风险偏好较高。
- 对声誉风险或潜在利益冲突，组织风险偏好较低。

在确定风险偏好时，决策局 / 部门应考虑多种因素以确保采取全面和明确的方法。这些因素在确定风险偏好和指导决策过程中发挥着关键作用：

- 战略目标：风险偏好应与决策局 / 部门战略目标和使命 / 愿景相一致。决策局 / 部门应评估为实现这些目标愿意承担的风险，并认真评估其对组织长期目标的潜在影响。
- 风险文化：组织风险文化应考虑在内，包括对风险承担的态度以及接受创新举措或采取较保守方法的意愿。
- 利益相关者期望：应考虑政府、监管机构、客户和公众等利益相关者的期望和偏好。了解利益相关者对风险的看法对于形成风险偏好至关重要，有助于保持组织的信任度和满足社会期望。
- 法律和监管要求：遵守适用的法律法规和行业标准至关重要。决策局 / 部门应考虑与风险管理相关的法律和监管义务，并确保风险偏好设定符合相关要求。
- 行业和市场条件：决策局 / 部门的风险偏好受行业和市场条件影响。决策局 / 部门应评估竞争格局、市场波动、新兴风险和行业良好实践模式，以确定适当的风险偏好。
- 财务能力：应仔细评估决策局 / 部门承担和管理风险的财务能力。决策局 / 部门应考虑组织的财务资源、对财务影响的风险承受能力以及对股东和投资者等利益相关者的潜在影响。

- 组织复原能力：应考虑决策局 / 部门承受不利事故并从中恢复的能力。决策局 / 部门应评估组织复原能力，并确定在不影响有效应对和恢复能力的情况下合理承担的风险。

4.3.2 风险承受能力

风险承受能力指实现目标时可接受的绩效变动水平，通常在计划、目标或组成部分层面建立。决策局 / 部门应解释其风险偏好，建立具体的信息技术安全风险承受水平，同时确保这些水平符合总体目标和法律法规要求。

制定风险承受能力至关重要，因为其划定风险承担范围，并指导控制和缓解措施的实施。决策局 / 部门可通过建立明确的风险承受阈值，在预设限值范围内有效地管理信息技术安全风险。如此可确保资源优先用于重要领域，并使决策局 / 部门恰当分配风险处理工作。明确风险承受能力、强化决策，提升信息技术安全风险管理的资源配置效率。

风险承受能力示例：
在任何情况下，决策局 / 部门不接受任何在缓解措施实施后「高风险」事故引起的风险。同时，决策局 / 部门不接受任何在缓解措施实施后「中等风险」事故引起的风险（经部门信息技术安全主任批准的除外）。

为管理信息技术安全风险而建立明确的风险承受能力阈值时，决策局 / 部门应考虑以下因素：

- 主要目标：决策局 / 部门应确定主要目标。这通常涉及需防范信息技术安全风险的信息系统。
- 利益相关者咨询：利益相关者包括高层管理人员、法务合规团队、信息技术部门和外部专家，须向其咨询以收集意见并确保风险承受能力阈值的全面性和实用性。
- 监管要求和行业最佳实践：决策局 / 部门应随时了解与信息技术安全风险管理相关的监管要求和行业最佳实践，为设置风险承受能力阈值获取指南。
- 定期监察和覆检：应定期监察和覆检风险承受能力阈值，确保其持续的相关性和有效性。随着信息技术威胁形势的变化，决策局 / 部门应相应调整其风险承受能力阈值，并对其风险管理策略实施必要的调整。

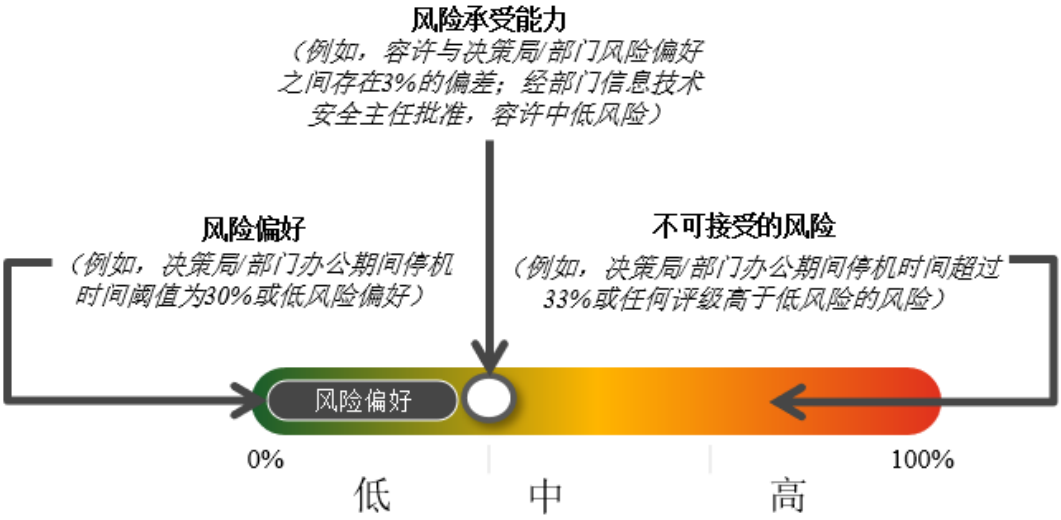

图 4.1：风险偏好、风险承受能力和不可接受风险说明

4.4 信息技术安全风险协调、整合及上报

协调并整合决策局 / 部门信息技术安全风险管理工作对于采取全面的风险缓解方法至关重要。决策局 / 部门应建立协调和整合流程，确保风险管理活动与总体目标一致，如促进相关团队、单位和利益相关者之间的合作，以分享信息、行业最佳实践和经验教训。此外，还应建立健全上报机制，保证信息技术安全风险透明、可问责，确保相关信息沟通及时。定期上报风险状况和风险缓解进展有助于决策局 / 部门各级作出明确决策。

信息技术安全风险协调、整合及上报是决策局 / 部门整体风险管理框架和流程的一部分。应在风险管理规划早期建立该流程，并随目标、风险和决策局 / 部门要求的变化而持续覆检及更新。

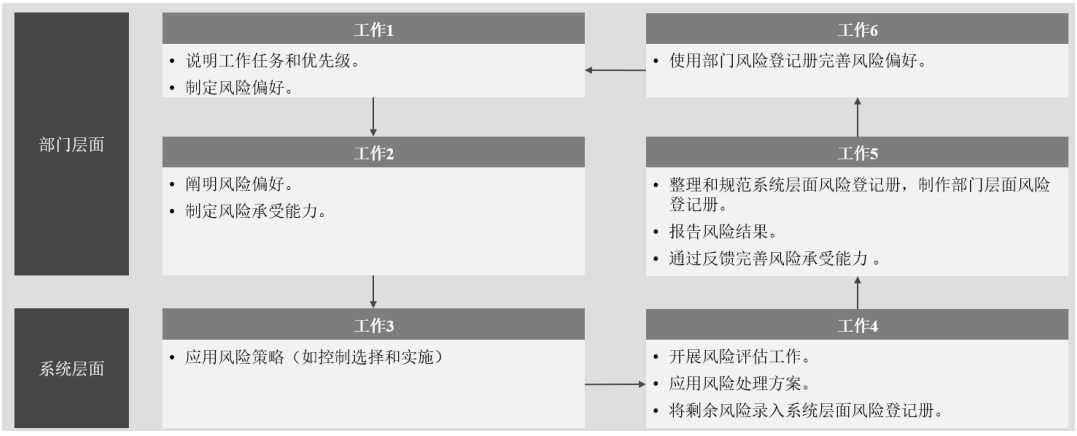

图 4.2：风险协调、整合及上报说明

4.5 职务和职责

决策局／部门应识别信息技术安全风险管理所涉及的主要职务，并制定其职责、上报关系及问责。决策局／部门应根据人员对所涉系统和流程的了解、经验和理解分配职务。信息技术安全职务和职责应在风险管理框架的计划或实施阶段制定。尽早确立职务和职责并定期覆检和更新至关重要，确保其符合不断变化的业务目标和风险环境。

职务和职责应涵盖各级员工，从制定风险偏好和风险承受能力的高层管理人员到执行风险处理措施的操作人员。

决策局／部门层面职务包括战略决策者和监督整体风险管理框架的人员。担任该层面职务的人员应全面了解和掌握决策局／部门的业务目标、风险偏好和风险承受能力，应负责制定决策局／部门信息技术安全风险框架，并确保其与决策局／部门使命和愿景保持一致。

系统层面职务可能包括管理具体信息系统并执行风险缓解措施的风险拥有者。担任该层面职务的人员应详细了解特定系统和已识别的风险。

4.5.1 风险拥有者

风险拥有者是获授权负责管理风险的个人或职能部门。风险拥有者可能担任流程负责人、职能负责人、项目经理或资产所有者或为高层管理人员或安全委员会成员。决策局／部门在确定风险拥有者时，应使用风险评估流程或建立相应标准。详情请参阅《安全风险评估及审计实务指南》。在确定风险拥有者时应考虑以下因素：

- 风险水平和存在风险的资产。
- 管理风险所需责任及授权。
- 了解问题和作出充分决策的能力（如确定如何缓解风险）。

风险拥有者职责参考示例如下。

- 识别和评估潜在信息技术安全风险。
- 建立和实施适当的战略和保障措施来缓解风险。
- 监控已识别的信息技术安全风险状态和风险缓解计划的有效性。
- 向职责范围内的利益相关者传达与风险相关的信息、政策和程序。
- 向高层管理人员和部门信息技术安全主任上报信息技术安全风险。

5. 信息技术安全风险评估与处理

信息技术安全风险评估过程应包括识别、分析和评估内部和外部风险。内部风险指决策局 / 部门的漏洞和威胁，如技术缺陷、操作漏洞和人为相关因素（包括人为错误或内部威胁）。另一方面，外部风险指来自决策局 / 部门外部的威胁，如信息技术安全攻击、黑客攻击和新兴威胁媒介。

识别和评估内部风险至关重要，因其有助于发现决策局 / 部门系统、流程和人员的潜在弱点和漏洞。具体内容包括评估现有安全措施的有效性、评估技术控制的稳健性以及识别恶意行为者可能利用的任何操作漏洞。此外，了解人为相关因素（如员工意识、培训和安全规约的遵行）对于缓解决策局 / 部门风险至关重要。

识别和评估外部风险也同等重要。具体内容包括分析威胁形势及随时了解新信息技术威胁和攻击途径。通过了解威胁者使用的战术、技术和程序，决策局 / 部门可主动采取适当的应对措施和预防措施。定期监察外部威胁和漏洞有助于识别潜在弱点，并迅速采取应对措施。更多详情请参阅《信息技术安全威胁管理实务指南》。

在风险评估过程中考虑技术、操作和人为相关因素，决策局 / 部门可全面了解其面临的信息技术安全风险。这对于建立针对性风险缓解策略和分配资源以有效应对已识别漏洞非常重要，同时有助于根据已识别风险的严重性和潜在影响确定风险处理工作的优先权。

如识别到信息技术安全风险，应进行分析并确定其优先权，决策局 / 部门应选择适当的风险处理方案，包括**风险接受**、**降低**、**避免**和**转移**。

为全面有效实施信息技术安全风险评估和处理流程，决策局 / 部门应参考**《安全风险评估及审计实务指南》**。该指南为识别、分析和评估政府机构信息系统中的信息技术安全风险提供了宝贵的指导意见和最佳实践。

在信息技术安全风险评估与处理过程结束时，将对收集和分析的信息进行编译和记录。该过程的结果是详细的风险评估表和风险登记册，风险登记册是追踪所有已识别风险的列表，提供存在什么风险以及如何解决这些风险的清晰记录。

6. 风险关联、汇总和正规化

6.1 建立风险登记册

建立和维护风险登记册对决策局 / 部门开展有效信息技术安全风险管理至关重要。风险登记册是记录已识别风险、风险可能性、影响和相关处理方案的中央存储库。风险登记册应于识别和记录风险时开始建立，记录的风险包括威胁决策局 / 部门信息系统和营运的内部和外部因素。

一旦风险被识别和评估，则应记录于风险登记册，并提供相关详情，如风险描述、指定的风险拥有者、当前风险水平和风险处理计划。定期更新风险登记册以反映风险环境的变化和风险处理活动的进展至关重要。通过全面维护风险登记册，决策局 / 部门可全面了解风险状况，有助于其作出明确的决策和资源分配。

决策局 / 部门应先建立单个的系统风险登记册，将其汇总为统一且全面的部门风险登记册。整合涉及风险关联、汇总和正规化流程。汇总风险登记册全面概述决策局 / 部门的所有信息技术安全风险，提供决策局 / 部门信息技术安全风险环境的全面观点。维护部门风险登记册的目的是为决策局 / 部门高层管理人员提供清晰、有序、全面的信息，使其了解决策局 / 部门需管理和定期覆检的已识别信息技术安全风险，有助于规划、资源分配和风险处理。关于将多个系统级风险登记册汇总为部门风险登记册。更多说明和示例，参见第 6.2 节。

应持续更新部门风险登记册，以反映风险环境的变化、控制措施的有效性或决策局 / 部门风险战略的变化。同时确保部门风险登记册对信息技术安全风险和主动风险管理的知情决策保持关联和实用性。

有关信息技术安全风险登记册模板的信息，请参阅**附件 A**。

6.2 执行风险关联、汇总和正规化

6.2.1 风险关联

风险关联指两种或以上风险值波动或变化的关联程度，用于衡量不同风险之间的统计数据关系或依赖关系，并揭示在风险环境中，这些不同风险因素如何相互作用或表现。决策局 / 部门应考虑并了解各系统风险之间的潜在联系和依赖关系。通过识别关联风险，决策局 / 部门可评估关联风险的整体影响，有效分配资源，并实施具有针对性的风险缓解措施。

值得注意的是，风险关联可以通过关联系数等统计指标进行定量评估，也可以根据专家判断和历史观察进行定性评估。风险建模和模拟技术可以分析风险之间的关联，并模拟它们对整体风险状况的潜在影响。例如，一个系统中的风险

可能会对其他领域的风险产生依赖或影响。了解这些关联有助于风险拥有者建立更加完善的风险管理方法。

风险关联示例：

假设某决策局 / 部门有两个独立的系统：一个用于客户数据管理，另一个用于交易处理。如果两个系统中都存在未获授权访问的漏洞，并且这两个系统都可以从同一网络访问，则这些风险具有关联。攻击者如果利用一个系统的漏洞获得访问权限，就有可能利用另一个系统的相同漏洞，从而导致更大规模的数据泄露。在这种情况下，风险拥有者应进行充分沟通与合作，以建立一个全面的方法来管理相关风险。

6.2.2 风险汇总

各决策局 / 部门应对各系统中相似类别的风险进行分组，以简化风险环境，使其更易于理解和管理。进行风险汇总的目的可包括但不限于以下方面：

- 汇总风险信息，以全面了解信息技术安全风险。
- 调整风险方向（如风险处理方案），优化决策局 / 部门的资源分配。
- 确保在各个层级进行监察和报告，以保持对风险环境变化的态势感知。

风险汇总是指将类似或相关的风险整合为一个汇总风险。通过这种方式，决策局 / 部门能够从一个更宏观的视角看待风险，并评估其累积影响。汇总风险可使决策局 / 部门更清楚地了解所面临的总体风险，并能更有效地确定缓解工作的缓急次序。风险汇总将系统信息技术安全风险登记册与其他登记册结合进行风险汇总。每个登记册中的信息技术安全风险的类别（如访问控制、数据安全）都可能是有限且一致的，因此登记表中的该列对初步分类工作极其关键。整合系统层面的所有类似类别的风险后，汇总便是直接的活动，但也可能需要做一些手动调整。不同的风险拥有者可能会对同一情景的风险描述不同。因此，应记录风险项的来源，以便于在原始登记册中追溯该风险。

有关风险汇总类别示例，请参阅**附件 B**。

风险汇总示例：

假设系统 A 和系统 B 是决策局 / 部门的两个系统；两个系统风险登记册将汇总为一个部门风险登记册。

系统 A 风险登记册												
编号	优先权	风险描述	风险类别	可能性	影响	系统等级	风险等级	风险处理方案	风险处理描述	风险拥有者	预计完成日期	状态
1	高	外部攻击者部署远程访问工具外泄决策局 / 部门的预算计划，导致敏感数据泄露。	访问控制	2	3	3	高	降低风险	对所有敏感系统的远程访问实施强身份验证机制，例如多	员工 A	2024 年 12 月 31 日	进行中

									重身份验证。			
2	高	识别系统中存在的未获授权访问的漏洞。	威胁管理	2	3	3	高	降低风险	应用系统供应商或开发人员提供的安全修补程序和更新，解决发现的安全漏洞。	员工 A	2024 年 12 月 31 日	进行中
3	中	系统使用不当，导致系统故障	人员安全	1	3	3	中	降低风险	为员工提供正确使用系统的安全意识培训。	员工 A	2024 年 12 月 31 日	进行中

系统 B 风险登记册

编号	优先权	风险描述	风险类别	可能性	影响	系统等级	风险等级	风险处理方案	风险处理描述	风险拥有者	预计完成日期	状态
1	低	洪水涌入一楼数据中心，导致多台数据库服务器进水受损，相关业务服务中断。	物理安全	1	2	2	低	接受风险	不适用。	员工 B	不适用	已完成
2	中	识别系统中存在的未获授权访问的漏洞。	威胁管理	2	3	2	中	降低风险	应用系统供应商或开发人员提供的安全修补程序和更新，解决发现的漏洞。	员工 B	2024 年 12 月 31 日	进行中
3	低	没有为系统制订事故应变计划和复原计划，导致在发生事故时服务中断。	事故应变计划和复原计划	2	3	2	中	降低风险	建立事故应变计划和复原计划	员工 B	2024 年 12 月 31 日	进行中

部门风险登记册

编号	优先权	风险描述	风险类别	可能性	影响	系统等级	风险等级	风险处理方案	风险处理描述	风险拥有者	预计完成日期	状态
系统 A 编号#1	高	外部攻击者部署远程访问工具外泄决策局 / 部门的预算计划，导致敏感数据泄露。	访问控制	2	3	3	高	降低风险	对所有敏感系统的远程访问实施强身份验证机制，例如多重身份验证。	员工 A	2024 年 12 月 31 日	进行中
系统 A 编号#2，系统 B 编号#2（注 1）	中（注 2）	识别系统中存在的未获授权访问的漏洞。	威胁管理	2	3	3，2	中（注 2）	降低风险	应用系统供应商或开发人员提供的安全修补程序和更新，解决发现的漏洞。	员工 A，员工 B	2024 年 12 月 31 日	进行中
系统 A 编号#3	中	系统使用不当，导致系统故障	人员安全	1	3	3	中	降低风险	为员工提供正确使用系统的安全意识培训。	员工 A	2024 年 12 月 31 日	进行中

系统 B 编号#1	低	洪水涌入一楼数据中心，导致多台数据库服务器进水受损，相关业务服务中断。	物理安全	1	2	2	低	接受风险	不适用。	员工 B	不适用	已完成
系统 B 编号#3	低	没有为系统制订事故应变计划和复原计划致在发生事故时服务中断。	事故应变计划和复原计划	2	3	2	中	降低风险	建立事故应变计划和复原计划。	员工 B	2024 年 12 月 31 日	进行中

注 1：将不同系统风险登记册中的类似风险项整合为一个汇总风险项。
注 2：根据决策局 / 部门的风险偏好、风险承受能力和资源，调整风险优先权和风险等级的差异。

6.2.3 风险正规化

在汇总系统风险登记册时，决策局 / 部门应确保风险信息的正规化。为方便进行有意义的比较和决策，决策局 / 部门内部风险信息的正规化亦至关重要。正规化涉及建立一个共同的方法或标准，用于评估和比较不同系统的风险。这可确保决策局 / 部门在评估和沟通风险时保持一致。至少，较高级别（如部门风险登记册）的风险正规化流程应使用相同的等级标准，以便进行比较和追踪。这通常包括衡量影响和可能性的定义，以便对评估结果进行比较。风险标准还可能描述在确定风险严重程度时应如何考虑时间因素，如风险速度。决策局 / 部门在正规化风险时应考虑以下活动：

- 去除重复并汇总相同或相似的风险：若识别出与内部威胁相关的类似风险，将它们汇总为单个风险项目。此步骤可以全面评估并实施适当的控制措施。例如，决策局 / 部门内发现两个类似的风险，第一个风险是「员工未获授权访问财务系统的数据」，而第二个风险是「员工对人力资源系统的恶意行为」。由于这两种风险都涉及员工未获授权访问不同的信息系统，因此可以将它们汇总为一个「访问控制」风险项：员工未获授权访问信息系统（财务系统和人力资源系统）。
- 根据决策局 / 部门的风险偏好、风险承受能力和敏感度调整风险：由于已在系统和部门层面建立了风险等级，因此有必要审查其累积影响和可能性，并建议更高或更低的风险评级调整。例如，决策局 / 部门高度重视突破界限和乐意采纳技术进步。然而，它对与第三方供应商管理相关的风险的风险承受能力较低。因此，与特定关键第三方供应商相关的多重风险进行了调整，以反映决策局 / 部门的更高关注。
- 处理信息技术安全风险登记册中的差异：例如，如果对相同或相似风险有不同的风险等级和风险处理方案，风险拥有者应相互沟通并决定：(1) 在汇总风险项中同时显示风险等级和风险处理方案；或 (2) 如果可以一起处理和追踪这些风险，则考虑调整具有相同风险等级和相同风险处理方案的风险。
- 裁定关键风险：例如，负责的管理层强调并覆检与支援决策局 / 部门业务连续性的关键系统相关的高风险，而这些风险需要在部门信息技术安全风险登记册进行追踪和进一步沟通。

通过正规化风险，从各种系统信息技术安全风险登记册得出的结果，可以保证风险处理和沟通的一致性。此外，决策局 / 部门应识别并处理各系统风险登记册中风险处理的差异，特别是当风险拥有者对相似情景采取不同的描述导致的差异。虽然不同的背景和情况可能导致差异，但了解根本原因并承认差异很重要。决策局 / 部门通过开展合作讨论，邀请相关风险拥有者参与，并力求在风险处理方案上保持一致，从而使其信息技术安全风险管理实务保持一致性和合理性。

风险正规化示例：

系统 C 风险登记册												
编号	优先权	风险描述	风险类别	可能性	影响	系统等级	风险等级	风险处理方案	风险处理描述	风险拥有者	预计完成日期	状态
1	低	员工使用共享账户访问系统。	访问控制	2	2	2	低	接受风险	不适用。	员工 C	不适用	已完成

系统 D 风险登记册												
编号	优先权	风险描述	风险类别	可能性	影响	系统等级	风险等级	风险处理方案	风险处理描述	风险拥有者	预计完成日期	状态
1	中	员工使用共享账户访问系统。	访问控制	3	2	2	中	降低风险	为目标员工提供安全培训。	员工 D	2024 年 12 月 31 日	进行中

正规化风险后：

部门风险登记册												
编号	优先权	风险描述	风险类别	可能性	影响	系统等级	风险等级	风险处理方案	风险处理描述	风险拥有者	预计完成日期	状态
系统 C 编号 #1， 系统 D 编号 #1	中	员工使用共享账户访问系统。	访问控制	3	2	2	中	降低风险	为目标员工提供安全培训。	员工 C，员工 D	2024 年 12 月 31 日	进行中

7. 风险监察与报告

7.1 监察已识别的风险和风险处理活动

风险监察的目的包括但不限于以下方面：

- 确保风险处理方案的有效性、效率和成本效益。
- 收集信息以加强未来的风险评估。
- 分析事故、变化、趋势、成功和失败并从中汲取教训。
- 发现内部和外部环境（如风险标准和新兴风险）的变化，从而调整风险处理方案和优先权。

监察已识别的风险和风险处理活动，是进行有效信息技术安全风险管理的关键。一旦识别风险并将其记录在风险登记册中，定期评估其状态并监察风险处理活动的进展至关重要。通过这种方式，可确保已实施的措施能够有效缓解已识别的风险并降低其潜在影响。

维护全面的风险登记册允许对不同程度的风险活动进行持续监察。风险拥有者应定期评估每项已识别的风险以确定其状态、可能性和潜在影响。评估可以通过专家判断、数据分析和历史信息。同时，定期更新风险登记册，有助于决策局／部门记录并适应不断变化的威胁和风险环境。

此外，决策局／部门应定期监察和评估计划实施或已实施的风险缓解措施是否达到预期结果并保持关联。这可能涉及收集利益相关者的反馈意见，利用绩效指标，或重新评估风险的影响和可能性。应记录任何与计划有关的变化或偏差并进行适当地沟通。根据监察结果对风险处理方案进行必要的调整，有助于确保采用积极的和适当的方法来缓解风险。决策局／部门通过定期监察和评估，可以主动管理其信息技术安全风险，并确保其风险处理工作的有效性。

7.2 监察风险环境

决策局／部门应积极监察其风险环境，以了解风险环境的变化。风险环境包括可能影响决策局／部门运营和目标的所有潜在威胁和安全漏洞。威胁管理是更宏观的风险管理所组成的部分，其重点在于发现、评估和应对决策局／部门所面临的威胁。

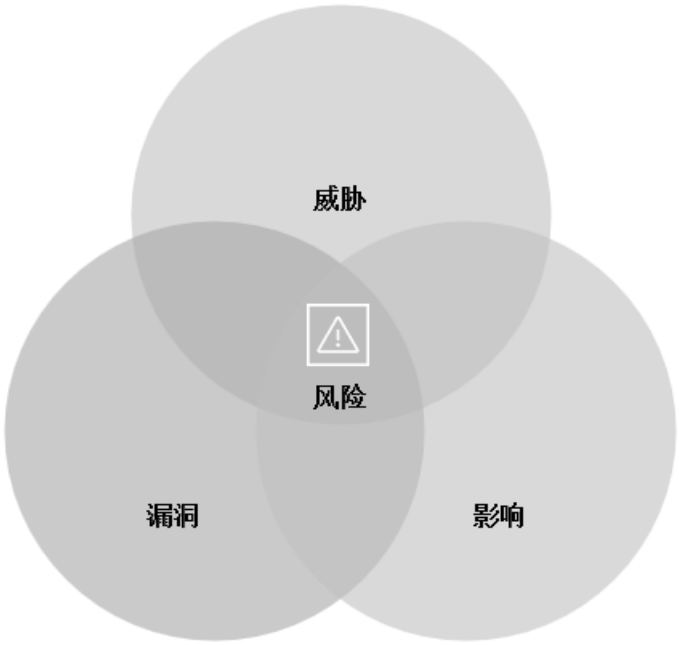

图 7.1：风险与威胁之间的关系

通过监察风险环境，决策局 / 部门可以洞察新兴威胁和趋势，从而能够积极主动地强化其信息技术复原措施，以应对潜在风险。

为有效监察风险环境，决策局 / 部门可采用以下行动：

- 定期进行漏洞扫描和渗透测试，发现和确定安全漏洞数量。
- 利用威胁情报，随时了解最新的网络安全威胁和漏洞。
- 通过资产管理流程追踪新的和现有的资产。
- 定期审查用户访问权限，确保其符合当前的角色和职责。
- 定期审查和更新决策局 / 部门的风险偏好声明。

持续监察至关重要，因为风险情景、资产价值、威胁、漏洞、可能性和影响可能在没有任何迹象的情况下突然发生变化。通过持续监察这些因素，决策局 / 部门可检测风险环境的变化，例如：

- 新的风险来源，包括新报告的安全性漏洞。
- 纳入风险管理范围的新资产。
- 资产价值的必要变动（例如，由于业务需求变化）。
- 确定已识别的漏洞，以便找出暴露于新威胁或重新出现的威胁之漏洞。
- 现有技术或新技术使用模式的变化，为攻击提供可乘之机。
- 法律法规的变化。
- 风险偏好以及对可接受和不再可接受风险的认知发生变化。
- 决策局 / 部门内部和外部的信息技术安全事故。

新的风险来源或可能性或影响的变化可能使之前评估的风险增加。因此，应定期重复风险监察活动，并定期检视所选的风险处理方案。

为监察风险环境的趋势，决策局 / 部门可以观察关键风险指标，并设法确定各方面的情况，例如：

- 已识别风险的可能性是否在增加。
- 后果的严重程度是否在上升。
- 是否出现新的风险。
- 控制措施是否失效。

有关用于监察内部风险环境的风险指标示例，请参阅**附件 C**。

如果风险环境发生重大变化，决策局 / 部门可以采取以下行动：

调整风险处理方案：
- 如果这一变化属于新型风险，如零日攻击，应考虑任命一名风险拥有者，负责了解风险、建立风险缓解策略并持续监察风险。
- 根据环境变化，覆检和更新风险处理方案。调整风险处理方案，通过对特定风险场景采取特定行动，以消除不一致性或实现不同结果。
- 这可能涉及加强风险处理措施，以减轻总体风险，或在接受一定程度的风险增加的情况下，放宽限制以获得好处。可逐步实施这些变化，确保决策局 / 部门各个层级的全面风险管理。

利益相关者沟通与参与：
- 就风险环境的变化以及缓解潜在影响的步骤与利益相关者进行沟通。
- 如有必要，考虑寻求外部专家建议和 / 或协助，以了解这些变化带来的影响，并帮助建立缓解潜在影响的策略。

改变策略方向：
- 根据共同商量的结果（提高或放宽风险限制），更新风险偏好声明，调整策略方向。这可能涉及调整具体的量化目标，并修改对风险承受能力的理解，以利用机会或最小化不利风险的可能性和影响。

监察和指标：
- 当决策局 / 部门变更其风险方向或方法时，修改关键绩效指标或关键风险指标以提高辨识度。风险拥有者可能会更改所监察的关键绩效指标和关键风险指标。若当前的关键绩效指标和关键风险指标无法充分体现影响和 / 或可能性的变化，则可合理引入不同的或额外的指标。若风险的影响和 / 或可能性的变化超过现有的监察频率，则需要提高监察频率。

风险相关方可能会发现，在监察过程中建立一份要采取的各项行动的清单很有帮助。例如，在确定某一风险领域发生重大变化时，可采取的行动包括：

- 成立工作组，讨论并确定下一步行动。
- 将类似的风险项分配给专门的风险拥有者，以减少差异并确保问责。
- 确定其他安全控制措施，以提高对那些可能发生且具有影响力的风险的防御、检测和应对能力。这些过程可能包括添加额外的工具（如日志记录和事件编排）、进行应变培训（如事故应变处理演习）或覆检保险范围。

7.3 定期风险报告

决策局 / 部门应建立系统化的风险报告流程，以便风险拥有者向高层管理人员、部门信息技术安全主任和其他相关方沟通风险状态和风险处理活动。应通过适当的机制记录和报告风险管理过程及其成果，旨在：

- 在决策局 / 部门内传达风险管理活动和成果。
- 为决策提供信息。
- 改进风险管理活动。
- 促进与利益相关者的互动，包括负责风险管理活动的人员。

定期报告风险对决策局 / 部门内部进行有效沟通和决策至关重要。这是信息技术安全风险管理管治架构的重要组成部分。通过报告风险提高与利益相关者的对话质量，并为高层管理人员和监督机构履行其职责提供支持。报告应考虑的因素可能包括但不限于以下内容：

- 不同的利益相关者及其特定的信息需求和要求。
- 报告的成本、频率和时间表。
- 报告的方法。
- 报告中的信息与决策局 / 部门的目标和决策的相关性。

风险报告应包括已识别的风险、其当前状态以及相关风险处理活动进展的全面信息。应提供风险等级、可能性、潜在影响和关键风险指标等关键指标，以便利益相关者做出知情的决策。此外，报告还应强调需要立即关注或采取行动的任何新兴风险或风险环境的变化。应定期和在发生重大风险变化时编制并分发这些报告。

为提高决策效率和及时应对新兴风险，报告清晰简明至关重要。风险报告中提供的信息应通俗易懂，避免使用专业术语或不必要的复杂表达。通过这种方式，利益相关者能迅速掌握关键信息，并就决策局 / 部门的资源分配、风险缓解策略和整体信息技术安全状况作出知情的决策。

8. 持续改进

8.1 反馈和经验教训

为培养持续改进的文化，决策局 / 部门应建立反馈机制，从以往事故、几乎发生的事故或安全漏洞中汲取经验教训。这些机制可包括事故报告系统、事故后覆检或与利益相关者开展定期反馈会议。决策局 / 部门通过积极寻求反馈，可以发现待改进领域，并巩固其信息技术安全实务。基于这些经验，培养持续学习和改进的文化至关重要，可确保决策局 / 部门更加成熟且有效地应对新兴信息技术威胁。

为收集反馈意见，以及总结风险管理活动中的经验教训，决策局 / 部门可采取以下步骤：

(a) 收集：建立一种机制，从参与风险管理活动的利益相关者（如项目经理、风险拥有者和团队成员）收集对风险管理框架的反馈意见。这可通过调查、访谈、工作坊或定期风险审查会议等方式进行。
(b) 文件记录：记录从风险管理活动中获得的反馈和经验教训，包括具体实例、建议和改进措施。将这些信息传达给利益相关者，并将其纳入未来的风险管理实务中。
(c) 知识分享：鼓励决策局 / 部门的风险管理工作者分享知识。建立规约，在各项目和部门之间分享经验、行业最佳实践和汲取的教训。这有助于营造持续学习和改进风险管理的文化。
(d) 覆检和更新：根据反馈和经验教训，定期审查和更新风险管理流程、程序和准则。将改进措施纳入信息技术安全风险管理框架，以便在未来加强风险管理工作。

8.2 绩效衡量

为评估决策局 / 部门内信息技术安全风险管理的有效性，确定绩效衡量指标尤为重要。决策局 / 部门应建立符合其目标的指标，为风险管理绩效提供可量化的标准。定期进行绩效衡量和报告，有助于追踪进展、确定待改进领域和验证控制措施的有效性。决策局 / 部门通过分析绩效指标，可以了解趋势，以行业标准为基准，并作出知情的决策，以强化其信息技术安全体系。

风险管理中的绩效衡量包括评估风险处理活动的有效性和效率，以及评估风险缓解成效。这有助于决策局 / 部门了解他们的风险管理成效，以及所实施的策略和控制措施是否达到预期效果。可根据与信息技术安全风险管理目标的吻合度来制定关键绩效指标，如已识别的风险、风险缓解效果、响应时间、缓解成本，以及事故或违规行为。

有关评估风险处理活动有效性的绩效指标示例，请参阅**附件 C**。

决策局 / 部门应定期覆检和分析绩效数据，了解趋势、差距和待改进领域。在完善策略，强化风险缓解工作并巩固风险管理框架时应考虑这些信息。

8.3 管理层覆检及调整

有必要定期对信息技术安全风险管理行为进行管理覆检，以评估该行为的有效性并进行必要调整。高层管理人员应定期覆检决策局 / 部门的风险管理流程，以确保其持续性、适用性、充分性和有效性。这些覆检应涉及高层管理人员和主要利益相关者，以确保与决策局 / 部门的目标和优先次序保持一致。在覆检过程中，高层管理人员应评估现有的风险管理策略、政策和程序的执行情况。此外，高层管理人员还应处理识别出的差距或待改进的领域，并作出调整，以提高计划的整体有效性。高层管理人员的参与和支持对推动必要变革以及将信息技术安全风险管理活动纳入治理框架至关重要。

管理层覆检及调整旨在确保和提高信息技术安全风险管理活动的质量和有效性，并应贯穿整个风险管理流程。

以下是在决策局 / 部门实施管理层覆检及调整过程的示例：

工作	**信息技术安全风险管理层覆检及调整示例（由决策局 / 部门填写）**	**状态（若已完成，请勾选）**
定期管理层覆检	对信息技术安全风险管理框架进行年度覆检。	
评估有效性	评估当前风险评估流程的有效性。	
必要调整	计划采用一种新的且更全面的风险评估方法。	
确保持续的适用性、充分性和有效性	覆检风险管理流程，识别可以更全面的风险评估流程。	
高层管理人员和主要利益相关方的参与	决策局 / 部门的高层管理人员、部门信息技术安全主任、信息技术安全管理组、系统拥有人和风险拥有者参与覆检过程。	
与决策局 / 部门的目标和优先次序保持一致	决定采用符合决策局 / 部门提升信息技术安全目标的风险评估新方法。	

工作	信息技术安全风险管理层覆检及调整示例（由决策局 / 部门填写）	状态（若已完成，请勾选）
推动必要的变革，将信息技术安全风险管理纳入治理框架	让高层管理人员参与推动风险管理框架的变革。	
确保和提高信息技术安全风险管理活动的质量和有效性	监察在下次覆检中调整后的结果，以确保质量和有效性得到提高。	

完

附件 A：信息技术安全风险登记册模板示例

编号	优先权	风险描述	风险类别	影响	可能性	系统等级	风险等级	风险处理方案	风险处理描述	风险拥有者	预计完成日期	状态
1												
2												
3												

- 编号（风险标识号）：风险登记册中某一风险的连续数字标识。
- 优先权：风险登记册中表示该条目重要性的相对指标，可以用序号值（例如，1、2、3）或参考给定等级（例如，高、中、低）表示。
- 风险描述：对（可能）会影响系统或决策局 / 部门的信息技术安全风险的情景作简要描述，风险描述通常以因果关系的格式编写，例如「如果发生X，则发生Y」。
- 风险类别：风险类别分组，例如按安全和私隐控制系列进行分类（例如，访问控制、供应链风险管理，如NIST SP 800-53中记录的风险类别）。类别可以是任何有助于汇总风险信息并整合信息技术安全风险登记册以提供决策支持的分类法。
- 影响：分析如果没有提供另外应对措施的情景的潜在好处或后果。这也可以视为风险周期第一次迭代的初步评估。
- 可能性：在任何风险应对之前，对发生这种情景的概率的估计。这也可以被视为风险周期第一次迭代的初步评估。
- 系统等级：系统关键性的级别。
- 风险等级：基于影响、可能性和其他因素（例如系统关键性）的组合而确定的的计算结果。
- 风险处理方案：用于处理已识别风险的风险处理选项。
- 风险处理描述： 风险处理的简要描述。例如，「实施软件管理应用程序XYZ以确保对软件平台和应用程序进行盘点」或「制定并实施流程以确保及时收到来自[特定信息共享论坛和来源的名称]的威胁情报」。
- 风险拥有者：指定的个人或业务单元，负责确保按照相关要求维护风险。
- 预计完成日期：风险处理的目标完成日期。
- 状态：用于追踪当前风险状况和任何后续活动。状态可以是简单的指标（例如进行中、已完成、待定、放弃、转移），也可以是更详细的描述（如「风险已接受，待1月24日季度风险委员会会议审查」）。风险状态应该是一套连贯的指标，有助于汇总风险信息并整合信息技术安全风险登记册，从而为决策提供支持。

附件 B：风险汇总的风险类别示例

- 资产管理
- 业务环境
- 治理
- 法规（遵行）
- 威胁管理
- 风险管理
- 安全系统开发
- 供应链风险管理
- 人员安全
- 实体安全
- 访问控制
- 数据安全
- 密码学
- 防护技术
- 信息技术基准维护
- 信息技术事故管理
- 检测技术
- 持续监察
- 检测过程
- 事故应变计划与复原计划
- 事故沟通
- 事故分析
- 事故缓解
- 事故改进

附件 C：相关风险偏好、风险承受能力、控制措施、关键绩效指标和关键风险指标示例

以下是相关风险偏好、风险承受能力、控制措施、关键绩效指标和关键风险指标示例：

	示例 1	示例 2	示例 3
风险偏好	必须保护关键信息系统免受已知网络安全漏洞的影响。	为了确保受保护的健康信息的安全性，我们必须首先确保只有获授权方能访问我们的计算机系统。	我们的客户将可靠性与公司的业绩挂钩，因此必须尽量避免面向客户的网站出现服务中断问题。
风险承受能力	对于被指定为关键的信息系统，必须在发现其存在重大软件漏洞（严重程度为 10 分）后的 14 天内，应用修补程序。	我们将发放独一无二的用户账户，并且计算机系统将审查成功和失败的登录事件。	区域经理可允许不超过 5%的客户遭遇持续 2 小时的网站中断。
控制措施	定期漏洞评估 部署修补程序的能力	独一无二的用户账户验证方法 审计日志 审计日志警报 / 评估	发电机 空调机组 上游网络提供商 网络负载均衡器 网络服务器
关键绩效指标	漏洞修补百分比	1 小时内登录失败的次数	服务中断时长（小时）
关键风险指标	在 10 天内未修复的重大漏洞（通用漏洞评分系统评分为 10）的计算机数量	单个用户 5 次登录失败 所有用户 30 次登录失败	当前的网站服务中断时长超过 2 小时并影响了超过 5%的客户的故障