风险管理ITIL®4实践指南

AXELOS.com

申明：

- 本文档由长河（微信achotsao）在机译的基础上经初步整理分解，精细化翻译工作正由ITIL先锋论坛组织的ITIL专家团队进行之中，预计到2020年年底之前全部完成。需要下载最终翻译版本请关注微信公众号：IT管理精英圈，或访问www.itil4hub.cn或www.itilxf.com。
- ITIL先锋论坛专家团队只是只是进行了这些著作的语种转换工作，我们并不拥有包括原著以及中文发行文件的任何版权，所有版权归Axoles持有，读者在使用这些文件（含中文翻译版本）时需完全遵守Axoles和TSO所申明的所有版权要求。

内容

1 关于本文件

本文档为风险管理实践提供了实用指南。它分为五个主要部分，内容包括：

- 有关风险管理的一般信息
- 风险管理的流程和活动及其在服务价值链中的作用
- 风险管理中涉及的组织和人员
- 支持风险管理的信息和技术
- 合作伙伴和供应商的注意事项，风险管理的注意事项。

1.1ITIL®4 鉴证方案

本文档的选定内容可作为以下课程的一部分进行检查：

- ITIL专家：创建，交付和支持
- ITIL专家：直接，计划，改进。

有关详细信息，请参阅相应的教学大纲文档。

2 一般信息

2.1 目的和描述

风险管理实践的目的是确保组织理解并有效地处理风险。管理风险对于确保组织的持续可持续性以及为其客户共同创建价值至关重要。风险管理是所有组织活动的组成部分，因此对于组织的服务价值系统（SVS）至关重要。

风险管理在组织的所有级别上执行。战略性风险管理考虑了可能使影响具有组织执行其使命能力的长期风险。方案和项目风险管理考虑了可能影响中期目标的风险。运行的风险管理专注于短期目标。每个级别的风险管理必须基于组织调速器的指示。

服务的ITIL定义明确指出，代表服务消费者管理风险是每个服务的重要组成部分。

服务

一种通过促进客户想要实现的结果来实现价值共创的方法，而客户不必管理特定的成本和风险。

每个服务都消除了服务消费者的某些风险，但也对服务消费者施加了其他风险。服务提供者必须以受控方式理解和管理这些风险。服务的价值提议的一部分是消除的风险与施加的风险之间的平衡。

风险管理实践为组织提供了在所有服务管理四维模型上高效，有效地识别和管理风险所需的资源。

2.2 术语和概念

2.2.1 风险

风险

可能造成伤害或损失，或使其更难以实现目标的事态。也可以定义为成果的不确定性，并且可以在背景中用于测量阳性结果和阴性结果的概率。

通常避免使用风险，因为它与威胁相关联。尽管通常这是正确的，但风险也与机会相关。

任何不确定的成果都是风险。当风险为负时，不确定的成果将导致伤害或损失。但是，当风险为正时，不确定的成果将为一个或多个利益相关者带来利益。例如，组织可能会投资新的服务，以期吸引客户并产生收入。但是，不能保证成果的正值，而是不确定成果或风险。正风险有时称为机会。借此机会的失效可以是风险。不投资其服务或发展其客户关系的组织将不会保留其市场地位。组织在其中运行的环境一直在发展，而不断发展的失效可以为组织构成风险。

2.2.2 风险容量

风险容量由组织的治理定义。风险管理活动必须确保风险保持在风险容量以下。

如果组织中的风险级别太高，则组织可能具有主要的影响继续运行能力。组织的风险容量是组织可以忍受的风险的最大数量，并且通常基于诸如对声誉的损坏，资产等的因素。

2.2.3 风险的胃口

风险的食欲由组织的治理定义，用于促进决策和风险管理和活动。

一些组织选择承担重大风险以取得重大收益。其他组织更愿意冒险，但这也减少了机会。组织的风险需求是组织愿意接受的风险数量。它应始终小于组织的风险容量。

2.2.4 风险寄存器

保留已识别风险的记录，记录风险的当前状况和历史记录，这一点很重要。该记录被称为风险寄存器。风险寄存器中的每个条目都显示单个风险的历史记录和状况。通常，这将包括以下信息（但是可能会有所不同，具体取决于组织的需求）：

- 唯一身份
- 类别（将相似类型的风险分组）
- 描述
- 可能性
- 影响
- 总体评分或分数
- 所有者
- 治疗
- 治疗后更新的评分或评分（剩余风险）
- 性能或绩效日期。

一个组织可能具有多个风险寄存器，具体取决于组织的大小和结构以及所管理风险的数量和类型

2.2.5 风险所有者

风险所有者可能不负责管理风险所需的操作，但是它们必须确保这些操作是适当的并且已被实际采取。

每个风险必须有一个分配的所有者，负责确保已理解和适当地管理风险。一旦确定了风险，就应立即分配风险所有者，并应将其记录在风险寄存器中。

2.2.6 风险处理

有时可以消除风险，但这是不寻常的。在了解了风险的概率和影响之后，风险所有者必须就处理风险的合适方法达成一致。表2.1中显示了可以用来处理风险的操作

表2.1 风险处理选项

治疗	描述	例
风险避免	通过不执行危险的实现价值来防止风险	通过拒绝建议投资的商业案例，避免投资的风险无法交付预期的价值
风险修改（或风险减少）	实施控件以减少风险的可能性或影响	在网络上传输敏感信息时对其进行加密，以减少被拦截的可能性
风险分享	通过将一些风险传递给第三方来减少影响	为火灾或网络攻击购买保险
风险保留（或风险销售活动）	故意决定接受风险，因为它低于可接受的阈值（并且在风险的胃口之内） 组织)	通过接受建议投资的商业案例，接受未能交付预期的价值的投资的风险

在处理正风险（机会）时，术语通常略有不同。避免风险成为风险的开发，而减少风险成为风险的增强。但是，术语风险修改涵盖正风险和负风险。

2.2.7 控制

控制

管理风险，确保实现业务目标或遵循流程的方法。

风险的修改要求实施控件以减少风险的可能性。

控制可以基于技术，例如防火墙或弹性网络配置，但它也可以与服务管理的其他任何尺寸有关。表2.2中显示了每个维度的一些控件示例

表2.2控件示例

域	控件示例
组织和人员	● 办公桌策略 ● 安全认知培训
信息和技术	● 网络防火墙 ● 审计记录
供应商和合作伙伴	● 将供应商认证为质量管理体系标准的合同要求 ● 供应商的常规审计活动
价值流和流程	● 部署之前评价的更改 ● 员工招聘期间的参考检查

2.2.8 剩余风险

风险处理通常不能完全消除风险。因此，在控制完应用程序之后，有必要执行新的风险评估。这是为了了解新的可能性和影响，然后计算残差风险。组织然后可以选择应用更多控件来进一步减小风险。或者，组织可以接受剩余的风险，应将其记录在风险寄存器中，并以与其他保留的风险相同的方式传达给感兴趣的涉众。

2.3 范围

风险管理的范围非常广泛。大多数活动和组织中的所有人在风险管理中都可以玩一些角色。服务提供者必须理解和管理与每个服务和每个客户相关的许多风险。ITIL 4中描述的许多管理实践要求风险管理作为其活动的一部分。这些包括：

- 项目管理
- 信息安全管理
- 组合管理
- 问题管理
- 事件管理
- 服务连续性管理
- 持续改进
- 服务级别管理。

尽管活动仍与风险管理密切相关，但仍有多个活动和职责范围未包含在风险管理实践中。表2.3中列出了这些内容，并提供了对实践指南的引用。重要的是要记住，ITIL实践只是价值流的背景中使用的工具的集合；根据情况，应将它们组合在一起。

表2.3其他实践指南中描述的与风险管理实践相关的活动

实现价值	实践指南
管理的特定风险	所有做法
实施变更以减轻风险	组织变革管理变更使能
	发布管理部署管理
	软件开发和管理服务验证和测试基础设施
	和平台管理劳动力和人才管理
	项目管理

成本控制，财务评价的风险和风险缓解选项	服务财务管理
愿景的定义和风险管理的战略目标	战略管理

2.3.1 项目管理

项目管理的重要部分是管理项目风险。应根据与战略目标，成本，风险，收益和进度的一致性来分析每个项目。这将导致创建一个项目风险寄存器，该寄存器将在项目生命周期的整个范围内维护，并用于确保妥善管理项目风险。

一些项目风险可能需要在项目之外进行管理，并且为此，可能会将其包含在其他风险寄存器中。

2.3.2 信息安全管理

信息安全管理的目的是保护组织进行业务所需的信息。这包括了解和管理与信息的保密性，完整性和可用性以及信息安全的其他方面有关的风险，例如身份验证（确保某人是他们声称的身份）和不可抵赖性（确保某人无法否认他们所声称的身份） 性能或绩效）。这意味着风险管理在信息安全管理实践中扮演着非常重要的角色。理想情况下，这不应与风险管理的其他方面分开。组织可以选择保留信息安全管理的风险寄存器，但是安全的任何重要信息也应出现在组织的风险寄存器中。其中一些信息安全风险可能由信息安全经理，服务所有者或实践所有者拥有和管理，但其他风险则需要升级为高级管理，因为它们可能对组织构成现有的威胁。

信息安全管理通常会创建和管理许多控件，并随着威胁和漏洞的发展而维护它们。

2.3.3 组合管理

组织的投资组合可以映射到管理风险的基础投资组合。当服务管理有效时，服务目录和流水线中的产品和服务将为为客户，组织和其他利益相关者创建和捕获价值提供机会。否则，由于与它们吸引的需求模式相关联的失效，它们所需的承诺以及它们产生的成本，这些产品和服务可能构成威胁。战略实施通常需要更改生产和服务组合并管理相关风险。

2.3.4 问题管理

问题管理主要与风险管理有关。问题管理实践的目的是通过确定事件的实际和潜在原因并管理变通办法和已知错误，以减少事件的可能性和影响。

造成事故的潜在原因是风险，并降低了可能性，而影响是风险管理实现价值。ITIL 4 Foundation指出，'问题管理活动可以被组织为风险管理的特定情况：它们旨在识别，评估和评估任何服务管理四维模型中的风险。为问题管理'采用风险管理工具和技术很有用。

ITIL与风险管理的其他方面不同地对待问题管理。这是由于问题的性质和频率以及管理这些问题所需的资源所致。但是，组织可以将所有问题都视为风险，并以与其他风险完全相同的方式来管理这些问题，这是可以接受的。

2.3.5 事件管理

尝试诊断和解决事件时采取的措施可能会导致风险。管理重大事件时采取的措施可能会对服务提供者和服务消费者涉及大量风险。这意味着涉及需求的每个人都应使用风险管理做法，以确保他们了解所涉及的风险，以便可以对这些风险进行适当的管理。

2.3.6 服务连续性管理

服务连续性管理是控制，用于管理可能对影响，可用性或性能或绩效服务产生的各种风险。有效的服务连续性管理实践可以对风险管理做出重大贡献。

2.3.7 持续改进

持续改进优先考虑和管理改进点机会。风险管理考虑了通常称为机会的正风险以及负风险。

许多组织将所有正风险中的管理视为持续改进实现价值，而仅将风险管理用于负风险。结果，风险寄存器仅包含负风险，而持续改进登记册包含正风险。只要控制所有风险，这就是一种完全可以接受的方法。

2.3.8 服务级别管理

服务级别管理与确保达到服务级别有关。这包括识别和管理影响服务可能存在的任何风险，并将这些风险报告给可能需要咨询或告知的客户和其他利益相关者。

良好的服务级别报告包括识别将来可能影响和服务的风险，以及如何管理这些风险的说明。通常，风险管理需要来自客户和用户的输入或由他们采取的行动。

2.4 实践成功因素

实践成功因素（PSF）

实践的复杂职能型组件，是实践实现其目的所必需的。

实践的成功因素（PSF）不仅仅是一项任务或实现价值；它包括所有服务管理四维模型的组件。活动的性质和实践中PSF的资源可能有所不同，但它们共同确保实践有效。

风险管理实践包含以下PSF：

- 建立风险管理的治理
- 培育风险管理文化并确定风险
- 分析和评估风险
- 处理，监控和审查风险。

2.4.1 建立风险管理的治理

所有风险管理活动都需要清楚地了解组织的风险，容量和风险的胃口。这些不能由从业者定义；它们是组织治理的关键方面。这意味着风险管理取决于组织的整体治理。

如果未提供此治理，则从业人员需要做出响应，并确保管理（或等效产品）的董事会对此负责。如果在没有治理的情况下执行风险管理，那么将很难根据组织的长期需求做出决策。

某些风险会给组织带来现存的威胁。这些风险应由组织的治理主体拥有。理想情况下，应该在董事会会议上定期讨论风险管理的治理。此外，还应该在董事会会议上讨论，商定和定期审查风险，容量，风险的食欲和战略风险。

2.4.2 培育风险管理文化并确定风险

识别风险后，组织可以在风险寄存器中对其进行记录并进行管理。然而，由于没有简单的流程或规程来识别风险，而且大多数组织都有大量未知风险，因此识别风险可能非常困难。

在3.2.1节中讨论了可以帮助识别风险的方法，但是支持这一点的最重要的管理实现价值正在培育风险管理文化。组织中的每个人都应负责识别和报告他们发现的任何风险。这需要文化，人们可以安全地识别自己和他人所犯的错误，

不用担心遭到报复。因此，经理和领导者需要培养一个开放而诚实的文化。

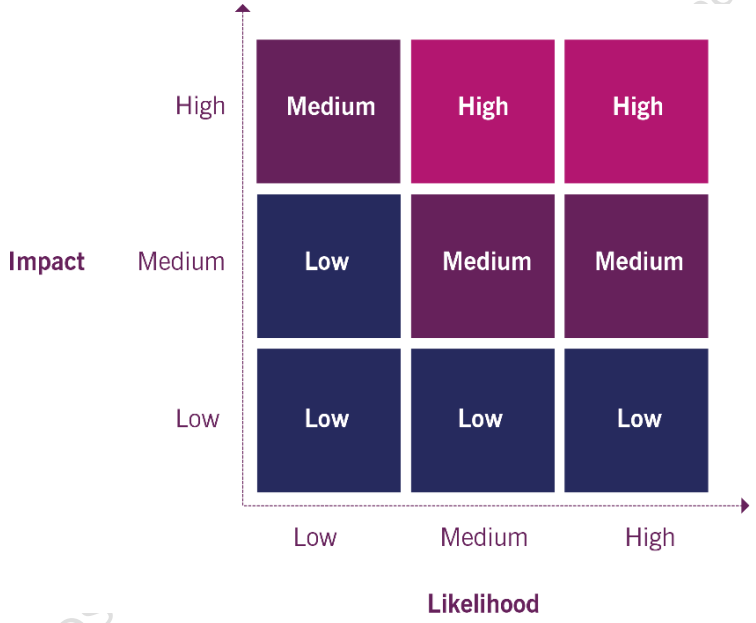
当风险管理嵌入组织的文化中时，员工将预见潜在的问题。然后，员工可以考虑如何减轻风险的负担以及他们是在从事战略计划还是例行公事运行的任务。

2.4.3 分析和评估风险

风险分析涉及了解每个风险的可能性和潜在影响。分析可以是定性或定量。

2.4.3.1 定性风险分析

定性风险分析使用简单的标度（例如高，中或低）来区分影响和影响的不同可能性。定性风险分析通常会使用一个表格，该表格用于从影响的水平和可能性中得出总体风险的水平，如图片2.1所示。



图片2.1用于定性风险分析的示例矩阵型

风险分析的输出确定风险的级别，该级别记录在风险寄存器中，并用于决定所需的风险处理。在图片2.1的示例中，具有中等似然性和高影响的风险将被评为高风险。此结果特定于组织，无法与来自不同组织的风险分析进行比较。

一些组织使用的是五点量表，而不是图片2.1中所示的简单的三点量表（高，中或低），但是方法仍然相同。

2.4.3.2 定量风险分析

定量风险分析在财务基础以及其他数字基础上考虑了风险影响。可能性被认为是概率。该风险分析支持可以在商业案例中使用的计算，以证明管理风险可能需要的投资是合理的。

年发生率（ARO）

特定风险将在一年内出现的可能性。

单一预期损失（SLE）

每次发生风险时，由于风险造成的预期财务损失。

年度预期损失（ALE）

风险造成的预期财务损失，平均为一年。ALE是通过将单个预期损失（SLE）乘以年发生率（ARO）

每年的发生率是根据对风险发生频率的预期得出的。例如，预期每五十年发生一次的事态的ARO为2%。

根据发生风险时产生的平均成本计算SLE。这通常以财务术语表示，但在某些组织中，可能以其他可衡量的方式表示，例如销售损失。

ALE通过将SLE乘以ARO来计算。然后可以将结果与控件的成本进行比较，以便可以决定在管理特定风险方面需要投入多少资金。

2.4.3.3 结合定性和定量风险分析

定量风险分析比定性风险分析花费更多的时间，因此通常将两者结合在一起使用数据来分析数据。这涉及对每个已识别的风险进行定性风险分析。然后，针对缓解水平的风险和成本，针对超出特定阈值的那些风险执行定量风险分析。例如，组织的风险管理策略可能声明，如果控件的成本低于5,000英镑，则将使用控件来管理低风险。如果控件的成本高于£5,000，将执行定量风险分析。

2.4.4 处理，监控和审查风险

每个风险必须以相同的方式处理。即使已决定接受风险，也并不意味着不会采用性能或绩效。应当记录接受的风险，将其传达给相关的利益相关者，并定期进行审查，以确保考虑对控件的可能性，影响或成本进行更改。

在决定管理风险时，需要设计和实现合适的控件。必须保持这些控制措施，以确保它们保持相关性，并正确实施它们以提供商定的保护级别。例如，如果组织的办公桌策略整洁，那么将其传达给所有可能在办公桌上留下文件的员工，并定期进行加固和审核，这一点很重要。同样，一个控制需要所有

运行最新的防病毒软件的计算机必须具有适当的技术，以识别任何不是最新的计算机。

定义控件的某些方面将在3.2.1节中描述，但处理监控和审查风险要求在所有服务管理四维模型之间保持适当的平衡。这不仅是流程的问题。

2.5 关键指标

应在每个实践所贡献的价值流的背景内评估ITIL实践的效果和性能或绩效。与任何工具的性能或绩效一样，只能在应用程序的背景内评估实践的性能或绩效。但是，设计和质量的工具可能会有很大差异，这些差异定义了工具的潜力，或根据用途使用能力才有效。有关度量标准，关键性能或绩效指标（KPI）的其他指南以及可以帮助您解决此问题的其他技术，请参见度量和报告实践指南。

风险管理实践的关键指标已映射到其实践成功因素。它们可以用作价值流的背景中的KPI，以便评估实践对那些价值流的效果和效率的贡献。表2.4中给出了一些示例。

表2.4 实践成功因素的关键指标示例

实践成功因素	关键指标
建立风险管理的治理	• 自上次审核和更新风险胃口以来的时间 • 具有明确记录的可能性，影响，所有者，治疗计划和下一个性能或绩效日期的战略风险百分比
培育风险管理文化并确定风险	• 表示愿意在匿名调查中发现风险和错误的员工比例 • 非特定风险管理角色的人员所确定的风险数量
分析风险	• 具有明确记录的可能性的风险寄存器，影响和所有者上的风险百分比
处理，监控和审查风险	• 带有明确记录的处理计划和下一个性能或绩效日期的风险寄存器上的风险百分比 • 最近六个月中已审查的风险寄存器中的风险百分比 • 受到控制约束的控件的百分比 最近六个月内的评审和审计

将指标正确汇总到复杂的指标中，将使数据更易于用于正在进行的价值流的管理，以及用于风险管理实践的定期评估和持续改进。没有单一的最佳解决方案。指标将基于整体服务战略和组织的优先级，以及实践所贡献的价值流的目标。

3 价值流和流程

3.1 价值流量贡献

像任何其他ITIL 管理实践一样，风险管理实践也有助于多个价值流。重要的是要记住，价值流永远不会由单个实践形成。风险管理实践与其他实践相结合，可以为消费者提供高质量服务。实践为所有价值链活动做出了重大贡献。

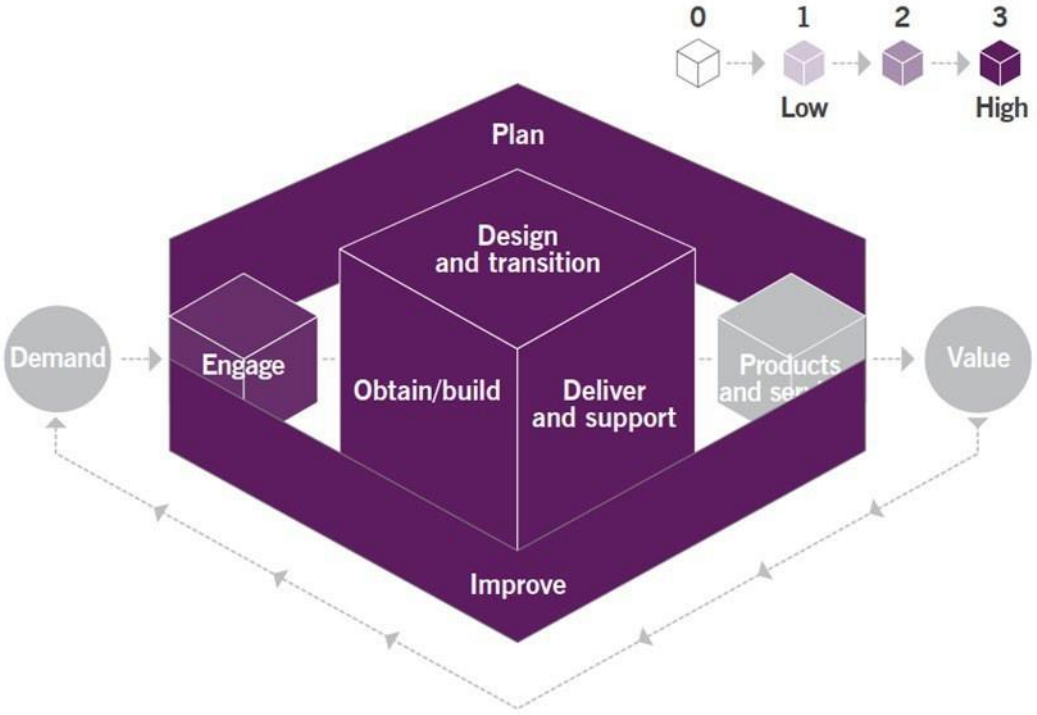
图片3.1中显示了风险管理实践对服务价值链的贡献。

3.2 流程

每个实践可能包含一个或多个流程和活动，它们对于实现该实践的目的可能是必需的。

流程

一组相互关联或交互的活动，可将输入转换为输出。流程接受一个或多个定义的输入，并将其转换为定义的输出。流程定义动作的顺序及其依赖性。



图片3.1 风险管理实践对价值链的贡献的热图活动

风险管理活动形成三个流程：

- 风险管理的治理
- 风险的识别，分析和处理
- 风险监控和评审。

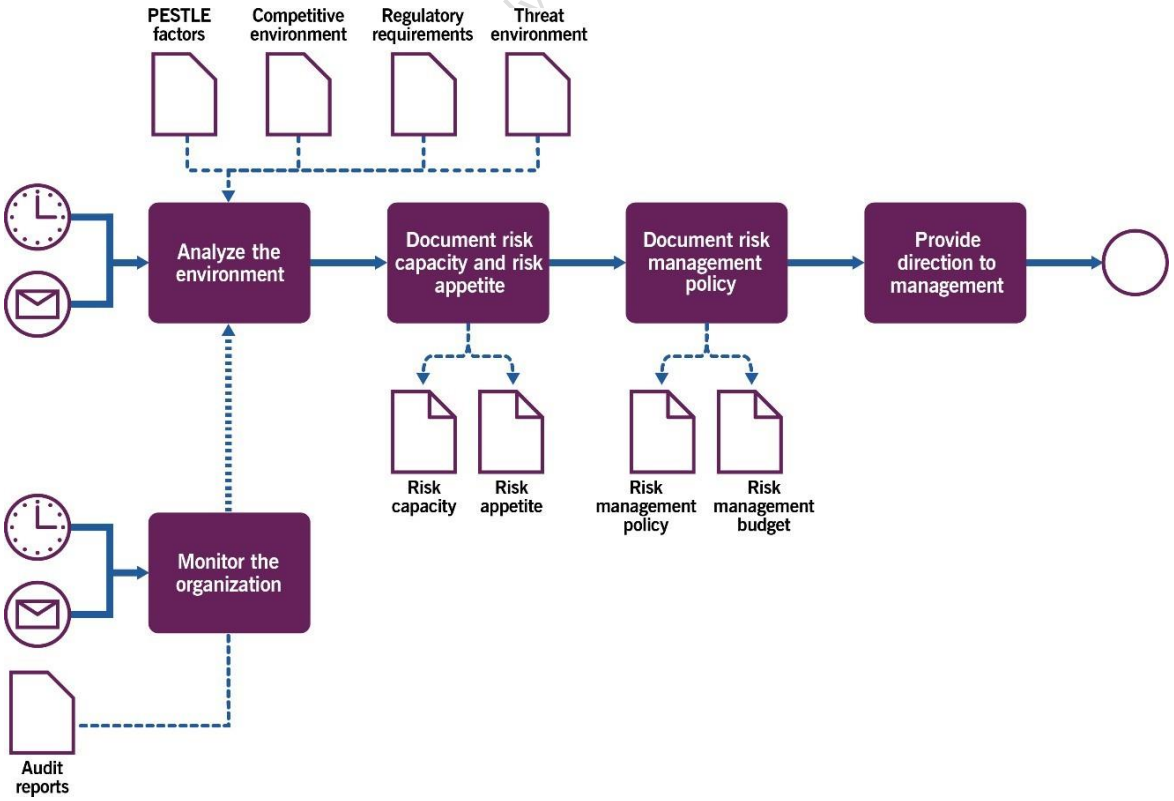
3.2.1 风险管理的治理

该流程包括表3.1中列出的活动，并将以下输入转换为输出。

表3.1 风险管理的治理的输入活动和输出流程

关键输入	活动	关键输出
• 环境因素（PESTLE） • 竞争环境 • 威胁环境 • 法规要求 • 组织策略	• 分析环境 • 风险，容量和风险的胃口 • 文档风险管理策略 • 向管理提供指导 • 监控组织	• Risk capacity • 风险的胃口 • 风险管理策略 • 适用于风险管理的预算 • 提供给管理的方向

图片3.2显示了流程的工作流程图



图片3.2 风险管理的治理的工作流程流程

成功风险管理所需的许多治理活动都不特定于风险管理实践。治理主体需要这些活动才能控制组织。

表3.2 风险管理的治理的活动流程

实现价值	例
分析环境	该实现价值并非特定于风险管理。治理主体分析： ● 限制和影响力和组织（政治，经济，社会，技术，法律和环境）的PESTLE因素 ● 法规要求 ● 竞争产品环境 ● 威胁环境 基于这些因素和其他因素，他们制定了总体组织策略，其中包括风险管理的策略。 该实现价值通常按计划进行，通常每年一次，但也可以由任何事态触发，而影响可以采用组织的策略。
风险，容量和风险的胃口	基于对环境，组织的文化和组织的策略的分析。治理主体建立并记录组织对风险，容量和风险的胃口。
文档风险管理策略	风险管理策略指定了用于识别，分析和管理风险的方法。这可能包括采用特定的标准和准则，例如ISO31000。创建此策略需要风险管理的专业知识，但决定和授权仍由治理主体承担。 治理主体为风险管理分配了预算，该数量必须足以支持策略的要求。
向管理提供指导	该实现价值并非特定于风险管理（但要提供的特定方向是关于风险管理）。 治理主体适当地共享风险容量，风险胃口和风险管理策略，并确保整个组织中的管理意识到各自的责任。 至风险管理。

监控组织	尽管可能存在特定的风险管理方面，但该实现价值并非特定于风险管理。 治理主体审查审计报告并监视组织，以确保风险管理正在按照其意图进行操作。如果存在重大缺陷，则可能会触发需求分析环境和评审风险容量，胃口和策略。

3.2.2 风险的识别，分析和处理

该流程包括表3.3中列出的活动，并将输入转换为输出。

表3.3标识，分析和处理流程的输入，活动和输出

关键输入	活动	关键输出
• Risk management policy • 风险的胃口 • 适用于风险管理的预算 • 现有风险寄存器 • 服务组合 • 服务型号 • 确定为其他活动一部分的风险 • 标准和框架 • 第三方提供的威胁评估和脆弱性评估服务	• 风险识别 • 风险分析和评价 • 风险处理	• 更新的风险寄存器 • 新增和更新的控件