安全风险管理流程

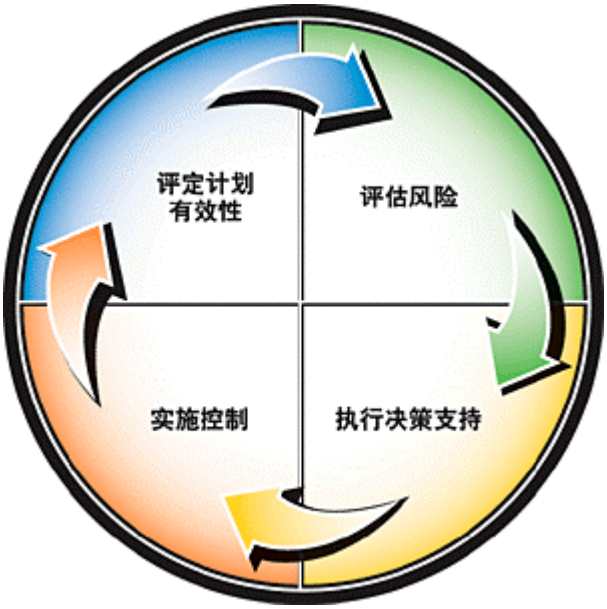
安全风险管理流程是一种混合方法，综合了两种传统方法的优点。 正如您将在后续章节中所见，本指南介绍了安全风险管理的一种独特方法，比传统的定量方法更为快速。 与传统的定性方法相比，这种方法还提供了更加详细的结果，并且能更加容易地向管理层证明。 通过将定性方法的简单性和简明性与定量方法的一些严格性结合起来，本指南为安全风险管理提供了一种有效且可使用的独特流程。 流程的目标是使风险承担者能够了解评估中的每一步骤。 此方法比传统的定量风险管理大为简单，最大程度地减少风险分析和决策支持阶段的结果面临的阻力，使一致意见的达成更为快速并在整个流程中都得到维护。

安全风险管理流程由四个阶段构成。 第一个阶段是评估风险阶段，综合了定性和定量风险评估方法。 用定性方法来快速类选安全风险的整个列表。 然后用定量方法更加详细地检查在此类选过程中确定的最严重的风险。 结果是一份相对较短的经过详细检查的最重要风险列表。

此短列表在下一阶段“ 实施决策支持 ”中使用，在该阶段中提议并评估潜在的控制解决方案，然后将最好的解决方案作为缓解顶级风险的推荐交给组织的安全筹划指导委员会。 在第三阶段“ 实施控制 ”中，缓解方案所有者实际实施控制解决方案。 第四阶段“ 评定计划有效性 ”用于验证控制措施实际提供预期的保护程度，并观察环境变化，例如可能改变组织风险配置的新业务应用程序或攻击工具。

因为安全风险管理流程是持续进行的，周期以各个新的风险评估重新开始。 周期重新开始的频率因组织不同而异；很多组织发现每年一次就已足够，因为组织正前瞻性地监控新的漏洞、威胁和资产。

图 2.2 安全风险管理流程的阶段



以上图 2.2 说明了安全风险管理流程的四个阶段。

本章在本指南中首先全面总结了安全风险管理流程。 此后，本章探讨了将有助于读者实施该流程的几个主题。 这些主题为安全风险管理计划的成功提供了坚实的基础，其中包括：

- 区分风险管理和风险评估。
- 有效地通告风险。
- 评价当前风险管理方法的完善程度。
- 定义角色和职责。

另请特别注意：风险管理只是较大的管理计划中的一部分，以便公司领导层监督业务并作出明智的决策。 尽管各管理计划有很大差异，但所有计划都要求有一个结构化的安全风险管理组成，从而确定安全风险优先级并缓解安全风险。安全风险管理流程概念可应用到任何管理计划，以帮助定义风险并将其降低到可接受水平。

第 3 章：安全风险管理概述

安全风险管理流程的四个阶段

第 2 章：“ 风险管理方法调查 ” 介绍了安全风险管理流程并将其定义为由四个主要阶段组成的持续过程：

1. 评估风险 — 确定企业面临的风险并确定其优先级。
2. 实施决策支持 — 根据已定义的成本效益分析流程确定并评价控制解决方案。
3. 实施控制 — 部署并实施控制解决方案以降低企业面临的风险。
4. 评定计划有效性 — 分析风险管理流程的效率，并验证控制措施提供了预期的保护程度。

此四部分的风险管理周期总结了安全风险管理流程，并用于组织本指南的整个内容。

然而，在定义安全风险管理流程的具体方法之前，需要了解更大的风险管理流程及其组成部分，这很重要。 周期的各个阶段都包括多个详细的步骤。 下表概括了各个步骤，以帮助您全面了解指南中每个步骤的重要性：

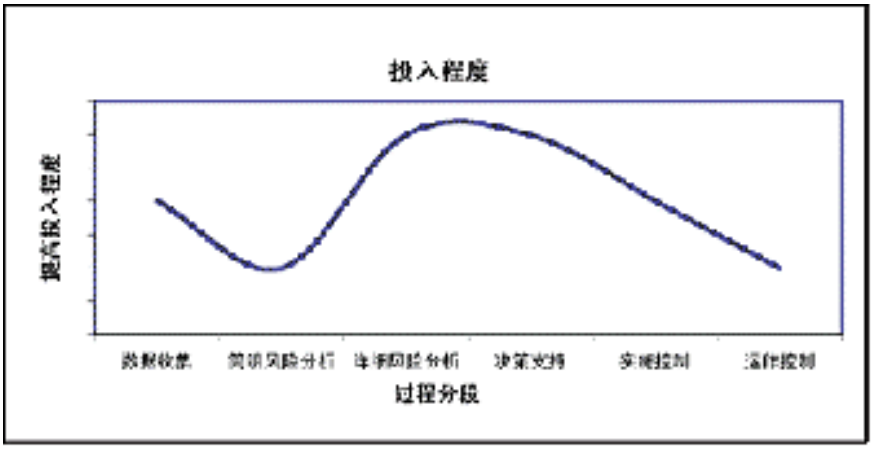
- 评估风险阶段
- 规划数据收集 — 探讨成功和准备指南的关键所在。

- 收集风险数据 — 概括数据收集流程并进行分析。
- 确定风险优先级 — 概括定性和定量风险的说明性步骤。
- 实施决策支持阶段
- 定义功能要求 — 定义功能要求以缓解风险。
- 选择可能的控制解决方案 — 概括确定缓解解决方案的方法。
- 审查解决方案 — 根据功能要求评价所提议的控制措施。
- 评估风险降低程度 — 努力了解降低的风险暴露程度或风险概率。
- 评估解决方案成本 — 评估与缓解解决方案相关联的直接或间接成本。
- 选择缓解策略 — 完成成本效益分析以确定最具成本效益的缓解解决方案。
- 实施控制阶段
- 寻求全局方法 — 将人员、流程和技术纳入缓解解决方案。
- 按纵深防御组织 — 在整个企业内组织缓解解决方案。
- 评定计划有效性阶段
- 制定风险评分卡 — 了解风险状态和进程。
- 评定计划有效性 — 评价风险管理计划，以寻找机会以进行改善。

本指南的其余各章依次说明了安全风险管理流程中的各个阶段。 然而，在开始实施此流程之前，需先考虑以下几个主要因素。

工作量

如果组织在风险管理方面相对来说没有经验，则需理解安全风险管理流程中的哪些步骤最需



要安全风险管理小组的工作，这对您会有所帮助。 下图根据在 IT 内实施的风险管理活动，显示整个流程中所需工作量的相对多少。 本说明帮助向新从事风险管理的组织说明整个流程及时间承诺。 工作量的相对多少也可提供帮助，以避免在整个流程的某一点上花费太多时间。 要总结整个流程中所需工作量的多少，本图说明：收集数据的工作量为中、总结分析的工作量较低，而建立风险的详细列表并实施决策支持流程的工作量为高。

为安全风险管理流程奠定基础

在开始进行安全风险管理之前，有一点很重要：需充分了解安全风险管理流程的基础预备知识及其任务，它包括：

- 区分风险管理和风险评估。
- 清楚地通告风险。
- 确定组织风险管理的完善程度。
- 为流程定义角色和职责。

风险管理与风险评估

如第 2 章所述，风险管理和风险评估这两个术语是不可互换的。安全风险管理流程将其定义为把整个企业内的风险降低到可接受水平的流程。 将评估风险定义为确定企业面临的风险并确定其优先级的流程。 如上一个图表所示：风险管理由四个主要的阶段组成：评估风险、实施决策支持、实施控制和评定计划有效性。 在安全风险管理流程的上下文中，风险评估只是指在更大的风险管理周期中的评估风险阶段。

风险管理和风险评估的另一个区别在于各个流程启动的频率。 风险管理被定义为一个持续的周期，但它通常以一定的间隔重新开始，以更新管理流程中各个阶段的数据。 风险管理流程通常与组织的财务计帐周期一致，从而使控制措施的预算需求与正常的业务流程一致。风险管理流程最常见的间隔为一年，以使新控制解决方案与年度预算周期一致。

尽管风险评估是风险管理流程中必须的、谨慎的一个阶段，信息安全组仍可在当前的风险管理阶段或预算周期之外实施多个风险评估。 当潜在的与安全相关的事件在企业内发生时，如新业务方法之引入、漏洞之发现或基础结构之改变等，信息安全组可随时启动风险评估。这些频繁的风险评估通常被称为特别风险评估，或有限范围内的风险评估，应将其审查作为正式风险管理流程的补充。 特别风险评估的重点通常为业务风险内的一个方面，并不需要整个风险管理流程所需同等数量的资源。表 3.1：风险管理与风险评估

	风险管理	风险评估
目标	在整个企业内将风险降低到可接受水平	确定企业面临的风险并确定其优先级
周期	包括所有四个阶段的整个项目	风险管理计划中的单个阶段
计划	持续	按需要
一致	与预算周期一致	不可用

通告风险。

参与风险管理流程的不同人员对术语风险的定义也通常不同。 为确保风险管理周期的所有阶段的一致性， 安全风险管理流程要求每个参与人员都理解术语“ 风险 ”的唯一定义并对此达成共识。 如第 1 章“ 风险管理指南介绍 ”所定义，风险是企业遭受影响的可能性。 本定义要求同时包括影响陈述以及对影响何时可能发生的预计（即：影响可能性）。 当风险陈述中包括了两个风险要素（可能性和影响）时，流程将它称为格式正确的风险陈述。 使用此术语有助于确保对风险的复合特性的一致理解。 下图描述了最基本等级的风险。

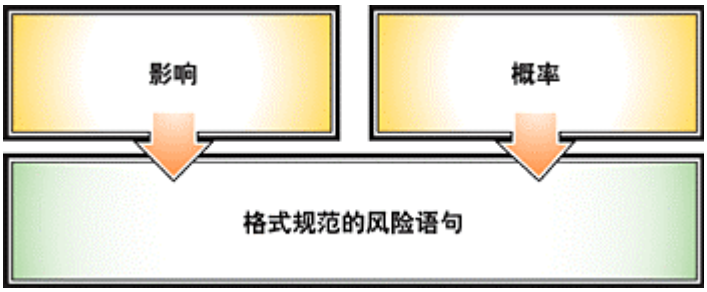


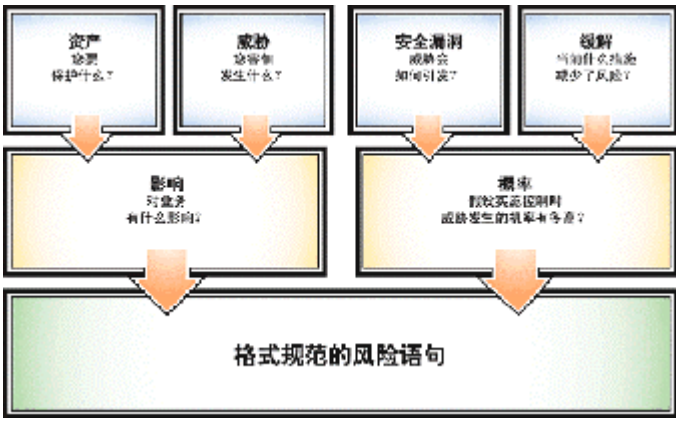
图 3.3 格式正确的风险陈述

参与风险管理流程的每个人都应理解风险定义中每个要素的复杂性，这很重要。 只有充分理解了风险，企业才能在管理风险时采取具体的措施。 例如，定义企业面临的影响时要求以下信息：什么资产受到影响，可能发生什么损坏，以及资产损坏的程度为多少。 其次，要定义影响发生的可能性，您必须理解每次影响可能如何发生，以及当前的控制环境在降低风险可能性方面的有效性如何。

采用第 1 章“ 风险管理方法指南介绍 ”中定义的术语，以下风险陈述为说明影响和影响可能性这两个要素提供指导。

风险是漏洞在当前环境下被利用的可能性，从而导致资产的机密性、完整性或可用性的一定程度的损失。

安全风险管理流程提供工具，以一致地通告和评定各个风险的可能性及损失程度。 本指南中的各章将完成整个流程，以建立格式正确的风险陈述的各个组成部分，从而确定整个企业内的风险并确定其优先级。 下图以之前讨论的基本风险陈述为基础，显示了各个风险要素之间的联系。



为了帮助通告风险陈述中影响的程度和可能性程度， 安全风险管理流程通过使用如高、中、低等相关术语确定风险优先级。 尽管此基本术语简化了风险级别的选择，但它不能在您实

施成本效益分析以选择最有效的缓解方案时提供充分的详细信息。 为解决此基本定性方法的弱点，本流程提供工具以生成风险的详细级别比较。 流程还采用了定量特性，以进一步帮助进行成本效益分析从而选择控制措施。

风险管理原则的一个常见缺陷是他们通常不考虑诸如企业面临的风险为高、中或低等定性定义。 您的安全风险管理计划可确定许多风险。 尽管安全风险管理流程提供指导，从而一致地应用定性和定量风险评估，但以确切的商业术语定义各价值的意义是安全风险管理小组的责任。 例如，企业面临的高风险可能意味着将在一年内发生的漏洞，从而导致组织最重要的知识财产在完整性上的损失。 安全风险管理小组必须给出格式完整的风险陈述中各个要素的定义。 下一章提供定义风险级别的说明性指导。 它将帮助您定义特殊业务的风险级别。该流程大大简化了实践，帮助在整个流程中达到一致性和可见性。

确定组织风险管理的完善程度。

在组织尝试实施安全风险管理流程之前，应检查安全风险管理的完善程度，这点很重要。 如果组织对于安全风险管理没有正式策略或流程，将会发现一次性把流程的各个方面都投入实践非常的困难。 即使组织具有一些正式策略和指导，良好地遵循了这些策略和指导的大多数雇员也会觉得流程有点令人不知所措。 基于这些原因，评估组织自身的完善程度很重要。如果发现组织还相对不成熟，则您可以历时数月循序渐进引入流程，在单个业务单元中试用直到多次完成流程。安全风险管理流程在整个试运行项目中的有效性显现之后，安全风险管理小组可以慢慢地将流程引入其他业务单元，直至整个组织都使用此流程。

如何确定组织的完善程度？ 作为信息和相关技术 (CobiT) 控制目标的一部分，IT 管理协会 (ITGI) 拥有一个 IT 管理完善程度模式。 您可以获得并审查 CobiT，从而为确定组织的完善程度找出详细方法。安全风险管理流程总结了 CobiT 中使用的要素，并根据 Services 开发的模式提供一个简单的方法。(也称为 ISO 17799) 基础之上。
通过将其与下表中的定义相比较，可以评估组织的完善程度。
表 3.2：安全风险管理的完善程度

0	不存在	未记录策略（或流程）。而且之前组织完全不了解与此风险管理有关的企业风险。 因此，没有关于此问题的通告。
1	特别	显然，组织的一些成员已得出结论：风险管理具有价值。 然而，风险管理工作是以特别方式进行的。 没有记录流程或策略，且流程不可完全重复。 总的来说，风险管理计划看来混乱且不协调，也未评定和审核其结果。
2	可重复	整个企业都了解风险管理。 风险管理流程是可重复的，但尚不完善。 未完全记录此流程，但活动定期发生，且组织正在建立一个完整的风险管理流程，其中高层管理人员也有参与。 没有关于风险管理的正式培训或通告，实施的责任落在了单个雇员身上。
3	已定义流程	组织已正式决定全面地采用风险管理，以推动其信息安全项目。 已制定了基准流程，其中明确定义了为获得和评定成功而记录了流程的目标。 此外，还向所有职员提供一些基本的风险管理培训。 最终，组织将要开始积极实施记录的风险管理流程。
4	已管理	组织的各个层面都已充分理解风险管理。 存在风险管理步骤、良好地定义了流程、广泛地理解了流程，提供了严格的培训，并采用了一些初级评定形式以确定有效性。 已向风险管理计划投入了充分的资源。组织的许多部门都从中受益，且安全风险管理小组能够持续改进其流程和工具。 有一些技术工具可帮助进行风险管理，低许多（不是绝大多数）风险评估、控制措施验证和成本效益分析程序都是人工的。
5	已优化	组织已投入了重要资源进行安全风险管理。公司成员期待着再次进行尝试以确定问题和解决方案在数月或数年之后会如何。 公司成员充分理解风险管理流程，而且通过工具的使用（无论是内部开发的还是从独立软件供应商获取），流程已大为自动化了。 已确定所有安全问题的根本原因，并已采取了适当行动使风险的重复率最小。向工作人员提供了各级专业培训。

组织风险管理完善程度的自我评估

以下问题列表为评定组织完善程度提供了更为严格的方法。 这些问题的答案具有主观性，但通过仔细思考每个答案，您应该可以确定组织在实施安全风险管理流程方面的准备程度如何。 将以前的完善程度定义作为指南，在 0 到 5 分之间为组织评分。

1.
信息安全策略和步骤清楚、准确、记录良好而又完整。

2.
已清楚确定了工作职责与信息安全有关的所有员工岗位，并且员工已透彻了解了其角色与职责。

3.
良好地记录了第三方对业务数据进行安全访问的策略和步骤。 例如，对内部业务工具实施应用程序开发的远程供应商拥有丰富的网络资源，从而能够有效地合作并完成工作，但他们只持有最少量的访问所需权限。

4.
硬件、软件和数据库等信息技术 (IT) 资产详细目录是准确且最新的。

5.
采用了适当的控制措施，保护业务数据免于被未经授权的外部和内部用户访问。

6.
实施了有效的用户知晓项目，如有关信息安全策略和方法的培训和新闻邮件。

7.
通过采用有效的控制措施，限制了对计算机网络和其他信息技术资产的物理访问。

8.
根据组织的安全标准，按照标准化方式，采用磁盘映像或编译脚本等自动化工具配置了新的计算机系统。

9.
有效的补丁程序管理系统可以自动将来自大多数供应商的软件更新发布到组织内的绝大多数计算机系统。

10.
已成立了事件响应小组，而且已制定并记录了处理和追踪安全事件的有效流程。 调查所有事件，直至确定了根本原因并解决了所有问题。

11.
组织具有全面的防病毒程序，其中包括多层防御、用户理解培训和响应病毒爆发的有效流

程。

12.
用户装备流程已被良好记录并至少部分自动化，因而可保证新雇员、供应商和合作伙伴及时获得访问组织信息系统的适当权限级别。 这些流程也应支持在不再需要时及时禁用和删除用户帐户。

13.
通过用户验证和授权、数据的限制性访问控制列表、以及前瞻性政策违背监控来控制计算机和网络的访问权限。

14.
向应用程序开发商提供指导，使其清楚地了解软件创建和代码质量保证测试的安全标准。

15.
明确定义且良好记录了企业持续性和企业持续项目，并通过模拟和操练定期进行测试。

16.
确保所有员工以符合法律要求的方式执行工作任务的项目已开始并且有效。

17.
定期进行第三方复查和审核，以验证安全企业资产相对于标准方法的符合性。

通过合计之前所有各项的分数计算企业的分数。 理论上来说，分数应在 0 至 85 之间；然而，极少数企业会得到两端的分数。

分数高于或等于 51，表明组织已经为引进和使用安全风险管理流程做好了充分准备。 分数为 34 至 50，表明组织已采取许多重要步骤来控制安全风险，并已准备好逐步引进本流程。在此范围内的组织应考虑把流程应用到整个组织之前，先花几个月的时间将流程推动到一些业务单元中。 分数低于 34 的组织应考虑创建核心安全风险管理小组，并在开始的几个月中将流程应用到单个业务单元中，从而非常缓慢地开始使用安全风险管理流程。 待到使用该流程的业务单元成功降低了风险，从而体现出流程的价值之后，企业可灵活地将流程扩展到其他两到三个更多的业务单元中。 但是仍应逐步缓慢引进，因为流程引起的变化可能很重大。 请不要过分干扰组织，以免影响其有效实现工作目标的能力。 在这方面充分发挥您的判断力 — 尚未保护的每个系统都处在潜在的安全和责任风险中，您对自己系统的了解是最重要的。 如果您急需使用该流程，则可以忽略缓慢引进的建议，按自己的观点做吧。
您需要仔细考虑将哪个单元作为运行项目的试点。 需考虑的问题包括：安全对此业务单元的重要程度，安全在其可用性、完整性以及信息和服务的机密性方面定义如何。 这样的例子包括：

- 与整个组织相比，此业务单元的安全风险管理完善程度是否超出了平均水平？

- 业务单元的所有者是否会积极地支持此项目？

• 业务单元在整个组织中是否具有高度的可见性？

• 如果安全风险管理流程试运行项目成功，是否会有效地向组织其余部分通告其价值？

在选择业务单元来扩展项目时，也应考虑这些问题。

定义角色和职责

出于跨部门交流和职责区分的要求，建立明确的角色和职责是任何风险管理计划的关键成功因素。 下表描述安全风险管理流程中的主要角色和职责。

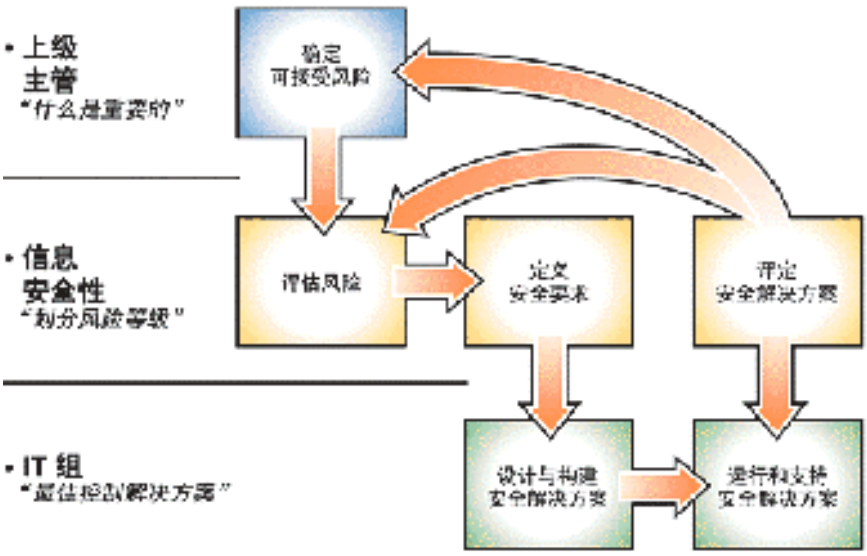
表 3.3：安全风险管理流程中的主要角色和职责

职务	主要责任
上级主管	主持有关企业管理风险的所有活动，例如为安全风险管理小组进行开发、提供资金、授权和支持等工作。 通常由主管人员如首席安全官或首席信息官担当此角色。此角色还是定义企业可接受风险的最后汇报人。
企业所有者	负责企业的有形及无形资产。 企业所有者还负责确定企业资产优先级并定义资产所受影响的级别。 企业所有者通常负责定义可接受风险级别，然而，上级主管拥有采纳信息安全组反馈的最终决策权。
信息安全组	负责较大的风险管理流程，包括评估风险和评定计划有效性阶段。 还定义功能性安全要求，并评定 IT 控制措施和安全风险管理计划的总体有效性。
信息技术组	包括 IT 体系结构、工程以及操作。
安全风险管理小组	负责推动整个的风险管理计划。 还负责评估风险阶段，并确定企业面临风险的优先级。 小组至少应由主持者和记录者组成。
风险评估主持者	作为安全风险管理小组的领导角色，开展数据收集讨论。 该角色可能还领导整个的风险管理流程。
风险评估记录者	在数据收集讨论过程中详细记录的风险信息。
缓解方案所有者	负责实施并维持控制解决方案，以将风险降低至可接受水平。 包括 IT 小组，有时还包括企业所有者。
安全筹划指导委员会	由安全风险管理小组、IT 小组代表和特定企业所有者组成。 上级主管通常是此委员会的主席。 负责选择缓解策略，并定义企业的可接受风险。
风险承担者	一般术语请参考特定流程或项目的直接或间接参与者，在整个 Microsoft 安全风险管理流程中使用。 风险承担者还可能包括 IT 之外的其他小组，如：财务、公共关系和人力资源。

安全风险管理小组可能会遇到风险管理流程的首次参与者，他们可能不会充分理解其角色。经常制造机会向参与者提供流程概述。 其目标是建立共识并强调一个事实：参与者都是管理风险的主人公。 下表总结了关键参与者并显示了其高级关系，有助于通告之前定义的角色和职责，并提供了风险管理计划的概述。

要进行总结，上级主管最终负责定义可接受风险，并向安全风险管理小组提供对企业风险评级的指导。 安全风险管理小组负责评估风险并定义功能性要求，以将风险缓解到可接受水平。 安全风险管理小组随后则与负责选择、实施和操作缓解方案的 IT 小组合作。 以下定义的最终关系为：安全风险管理小组对评定控制措施的有效性进行监督。 这通常以审核报告的形式出现，这也将向上级主管汇报。

表 3.5：安全风险管理流程中的角色和职责概述



建立安全风险管理小组

在开始风险评估流程之前，请勿忽略在安全风险管理小组内明确定义角色。 因为风险管理的范围包括整个企业，所以非信息安全组成员也可能需要成为风险管理小组的成员。 如果这种情形发生，需明确概括每个成员的角色，并需与上述总体风险管理计划中定义的角色和责任一致。 尽早进行角色定义可减少混淆，并有助于在整个流程中制定决策。 小组的所有成员都必须理解信息安全组对整个流程负责。 定义负责关系很重要，因为信息安全在流程的每个阶段（包括管理报告）都是唯一一组关键的风险承担者。

安全风险管理小组角色和责任

在组建了安全风险管理小组之后，要建立具体的角色并在整个流程维持这些角色，这点很重要。 风险评估主持者以及风险评估记录者的主要角色描述如下：

风险评估主持者必须对整个风险管理流程有着全面的理解，并充分了解业务以及构成企业功能基础的技术安全风险。主持者必须在实施风险讨论时能够将业务情形转换为技术风险。例如 :风险评估主持者需要理解移动工作者的技术威胁和漏洞,以及这些工作者的业务价值。例如：如果移动工作者无法访问企业网络，则无法处理客户付款。 风险评估主持者必须理解类似的情形，并能够确定技术风险和潜在控制要求，如移动设备配置和验证要求。 如果可能，请选用一名曾实施过风险评估并了解业务的总体优先级的风险评估主持者。

如果不能找到具有风险评估经验的主持者，则可以寻求一名合格的合作伙伴或顾问的帮助。但是请确保涵盖了熟悉业务的信息安全组成员及风险承担者。

注：向外寻找风险评估主持角色可能比较吸引人，但要小心，当顾问离开时可能会失去风险承担者关系、业务和安全知识。 不要低估风险管理流程将给风险承担者及信息安全组带来的价值。

风险评估记录员负责获取笔记并记录规划和数据收集活动。 此责任的角色定义在本阶段可能看来太不够正式；然而，可靠的笔记技能将在流程稍后的优先排序和决策支持阶段中获得成功。 管理风险的最重要方面之一是以风险承担者能理解的方式通告风险，并能应用到他们的业务中。 一个优秀的记录员可以随时提供书写记录，从而简化流程。