OWASP 软件保障成熟度模型

（SAMM）V2.0

OWASP 中国

2020 年 8 月

目录

前言

OWASP 软件保障成熟度模型（SAMM）项目是 OWASP 的旗舰项目。自 2008 年创建以来，OWASP SAMM 项目已先后经历了 v1.0、v1.1.1、v1.5、v2.0 版本更新。本 v2.0 版是 OWASP SAMM 项目的最新版本。

OWASP 软件保障成熟度模型（SAMM）项目的使命是成为软件安全保障的主要成熟度模型。该模型为所有类型的组织提供了有效的、且可衡量的方式，来分析和改善其软件安全状况。OWASP SAMM 支持完整的软件生命周期，包括开发和获取，并且与技术和过程无关。它被特意设计为具有发展性和风险驱动性。

1、 治理

治理聚焦于与组织如何管理整个软件开发活动相关的过程和活动。更具体地说，这包括对开发中涉及跨职能小组的影响以及在组织级别建立业务流程的担忧。

1.1 战略与指标

软件保障涉及许多不同的活动和关注点。没有总体规划，您可能会花费大量精力来构建安全，而实际上，您的工作可能是不协调的、不成比例的，甚至会适得其反。战略与指标（SM）实践的目标是建立一个有效的计划，以在组织内实现软件安全目标。

一个软件安全计划筛选模型中的部分活动，并定义了优先级，作为您工作的基础。该实践致力于构建、维护和宣传该软件安全计划。

同时，您希望跟踪安全状况和计划的改进情况。本模型包含了一种以指标为导向的方法，以确保您对活动的准确了解。衡量就是为了要知道。

成熟度等级		活动流 A 创建和推广	活动流 B 衡量和改进
1 级	识别安全计划的目标以及衡量安全计划有效性的手段。	识别与组织的风险承受能力相关的组织驱动因素。	通过深入了解应用软件安全计划的有效性和效率来定义指标。
2 级	为组织内的软件安全建立统一的战略路线图。	发布统一的应用软件安全战略。	为衡量计划有效性的设置目标和关键绩效指标（KPI）。
3 级	使安全工作与相关的组织指标和资产价值保持一致。	调整应用软件安全计划以支撑组织的发展。	基于指标和组织的需求对战略产生影响。

1.1.1 创建与推广

1.1.1.1 成熟度等级 1

收益

对组织的安全状况形成基本认识。

活动

基于应用软件暴露的风险了解存在或可能存在哪些威胁，以及组织的高级领导层对这些风险的容忍度。这种理解是确定软件安全保障优先级的关键组成部分。为了确定这些威胁，需对业务所有者和利益相关者进行访谈，并记录组织所处行业的特定驱动因素以及组织所特定的驱动因素。收集的信息包括：对组织造成影响的最坏情况，以及通过优化软件开发生命周期和使用更安全应用软件后可能提供的差异化市场机会或创造的额外机会。

收集的信息为组织开发和推广其应用软件安全计划提供了基线。在计划中优先考虑消除威胁以及对组织最重要的机遇。基线被分为几个风险因素和与组织优先级直接关联的相关驱动因素，并通过记录它们在受到威胁时如何影响组织来帮助构建每个定制开发应用软件的风险状况。

基线和每个风险因素应予以发布，并提供给应用软件开发团队，以确保创建应用软件风险画像并将组织的优先事项纳入计划的过程更加透明。此外，应提供一组目标，这些目标应用于确保所有应用软件安全计划增强功能都能为组织当前和将来的需求提供直接支持。

问题

您了解您的应用软件在整个企业范围内的风险偏好吗？

质量标准

您把握了组织高管领导层的风险偏好。
组织的领导层审查并批准了一系列风险。
您为您的资产和数据识别了主要业务和技术威胁。
您记录风险并将其存储在可访问的位置。

回答

没有。
是的，它涵盖了一般风险。
是的，它涵盖了特定于组织的风险。
是的，它涵盖了风险和机遇。

1.1.1.2 成熟度等级 2

收益

可用且达成一致的应用软件安全计划路线图

活动

根据资产的数量、威胁和风险承受能力，制定安全战略计划和预算，以解决围绕应用软件安全的业务优先级。该计划涵盖 1 至 3 年，并包括与组织的业务驱动因素和风险相一致的里程碑。它提供了战术和战略计划，并遵循了使其与业务优先事项和需求保持一致的路线图。

在路线图中，您需要在变更所需的财务支出、流程和程序变更、及变更对组织文化的影响之间取得平衡。这种平衡可帮助同时完成多个里程碑，而不会超载或耗尽可用资源或开发团队。里程碑的频率足够高，可以帮助监视程序成功并触发及时的路线图调整。

为了使该计划成功，应用软件安全团队从组织的利益相关者和应用软件开发团队获得支持。需要支持或参与其实施的任何人都可以使用已发布的计划。

问题

您是否有针对应用软件安全的战略计划，并用来制定决策？

质量标准

该计划反映了组织的业务重点和风险承受能力。
该计划包括可衡量的里程碑和预算。
该计划与组织的业务驱动因素和风险相一致。
该计划为战略和战术计划制定了路线图。
您获得了利益相关者的支持，包括开发团队。

回答

没有。
是的，我们每年都要审查。
是的，我们会在做出重大决定之前先咨询核对计划。
是的，我们经常咨询核对该计划，并且该计划与我们的应用软件安全战略保持一致。

1.1.1.3 成熟度等级 3

收益

使应用软件安全计划与组织的业务目标持续保持一致。

活动

您需要定期检查应用软件安全计划，以确保其能持续适应和支持组织不断变化的需求和未来的增长。为此，您每年至少重复执行一次本安全实践前两个步骤的成熟度等级。该计划的目标是始终支持组织当前和将来的需求，以确保计划与业务保持一致。

除了审查业务驱动因素之外，组织还密切监视对每个路线图里程碑的成功实施。您可以根据广泛的标准来评估里程碑的成功，包括实施的完整性和效率、考虑的预算以及该计划所产生的任何文化影响或变化。您还需要查看未完成的或不令人满意的里程碑，并评估整个计划可能需要的变更。

组织为管理人员和负责软件开发的团队衡量和展示提供了当前状态，以监控路线图的实施情况。这些展示信息需要足够详细，以识别各个项目和计划，并清楚地了解该计划是否成功并且符合组织的需求。

问题

您是否经常审查和更新应用软件安全战略计划？

质量标准

您可以根据业务环境、组织或其风险偏好的重大变化来审查和更新计划。
计划的更新步骤包括与所有利益相关者一起审查计划，以及更新业务驱动因素和策略。
您可以根据从已完成的路线图活动中获得的经验教训，来调整计划和路线图。
您发布有关路线图活动的进度信息，以确保所有利益相关者都可以使用它们。

回答

没有。
是的，但是审核是临时的。
是的，我们会定期审查。
是的，我们至少每年审查一次。

1.1.2 测量与改进

1.1.2.1 成熟度等级 1

收益

对您应用软件安全计划的有效性和效率有基本见解。

活动

定义并记录测量标准，以评估应用软件安全计划的有效性和效率。这样就可以测量改进，您可以使用它们来确保将来对该计划的支持和资金。考虑到大多数开发环境动态变化的性质，应包括以下方面的测量指标：

- 投入：该标准衡量在安全上的投入，包括：培训时间、执行代码审查的时间、应用软件漏洞扫描的次数。
- 结果：该标准衡量安全工作的结果，包括：安全缺陷未修补的数量、涉及应用软件漏洞的安全事件数量。
- 环境：该标准衡量执行安全工作的环境，包括：应用软件数量或代码行数，以衡量难度或复杂性。

每种测量本身都可用于特定目的，但将两个或三个指标结合在一起时，则有助于解释测量趋势结果中峰值的含义。例如，漏洞总数的激增可能是由于组织采用了一些新的应用软件，而这些新应用软件以前并没有被应用软件所采用的安全机制检测到。作为选择，可替代地，在不相应增加工作量或结果的情况下环境指标提升，可能意味着安全计划是一个成熟和有效的。

在确定指标时，始终建议坚持指标符合以下多个条件：

- 持续测量；
- 以便宜的方式收集测量信息；
- 以基数或百分比表示；
- 以测量单位表示。

记录测量指标，包括对收集数据最佳和最有效的方法描述，以及将多个测量指标组合成为测量标准的推荐方法。例如，许多应用软件和所有应用软件中的缺陷总数本身可能并不有用，但当组合成为每个应用软件中的高危缺陷数量时，它们就成为了更具可操作性的指标。

问题

您是否使用一组指标来衡量应用软件安全计划的有效性和效率？

质量标准

您记录每个指标，包括来源描述、测量范围，以及有关如何使用它来解释应用软件安全趋势；
指标包括投入工作量、结果和环境三个类别；
大多数测量标准经常被测量，且数据收集方法方便、经济，并表示为基数或百分比；
由应用软件安全和开发团队发布指标。

回答

没有；
是的，使用了一个指标类别；
是的，使用了两个指标类别；
是的，使用了所有三个指标类别。

1.1.2.2 成熟度等级 2

收益

应用软件安全计划的执行情况公开透明

活动

一旦组织定义了其应用软件安全测量指标，就收集足够的信息以达到切合实际的目标。测试已确定的指标，以确保您可以在短时间内连续有效地收集数据。在初始测试期之后，组织应具有足够的信息来实现关键绩效指标（KPI）目标。

尽管有几种测量标准可用于监视信息安全计划及其有效性，但 KPI 包含最有意义和最有效的指标。旨在消除关键绩效指标（KPI）中有关应用软件开发环境的常见波动，以减少因临时或误导性的个别测量而产生不利结果的可能性。基于 KPI 的指标不仅对信息安全专业人员有价值，对应用软件整体成功的负责人和组织领导也很有价值。将 KPI 视为整个计划成功的确定指标，并认为它们是可行的。

完整记录 KPI，并将其分发给为计划成功而做出贡献的团队，以及组织领导。理想情况下，需简要说明每个 KPI 的信息来源以及数字高低的含义。需包括短期和长期目标，以及需要立即干预的不可接受测量范围。与应用软件安全和开发团队共享行动计划，以确保大家完全理解组织的真实目标。

问题

您定义的关键性能指标（KPI）是否来自于可用的应用软件安全指标？

质量标准

您在收集了足够的信息后，才定义了 KPI、建立了切合实际的目标；
您是由负责应用软件安全的领导层和团队来开发 KPI 的；
应用软件团队可以使用 KPI，其中包括可接受性的阈值和指南，以防团队需要采取行动；
根据已定义的 KPI，可以清楚地看到应用软件安全计划的成功。

回答

不是；
是的，某些指标是；
是的，至少有一半指标是；
是的，大多数或所有指标是。

1.1.2.3 成熟度等级 3

收益

根据结果持续改进计划。

活动

根据 KPI 和其他应用软件安全指标定义影响应用软件安全计划的准则。这些准则将应用软件开发过程、过程的成熟度、及不同指标结合在一起，以使计划更高效。以下示例显示了测量与提升应用软件安全改进方法之间的关系：

- 通过主动应用安全措施，聚焦软件开发生命周期的成熟度，以降低每个缺陷的相对成本。
- 监视投入、结果和环境指标之间的平衡，以提高计划的效率，并证明采用其他自动化方法和其他方法可以改善总体的应用软件安全基线。
- 每个安全实践都可以提供每个应用软件安全计划成功或失败的指标。
- 投入指标有助于确保应用软件安全的工作针对更相关和更重要的技术和领域。

在定义总体指标战略时，请牢记最终目标，并定义因 KPI 和指标发生变化而可以做出的决策，以帮助指导指标的开发。

问题

您是否根据应用软件安全指标和 KPI 更新了应用软件安全战略和路线图？

质量标准

您每年至少审查一次 KPI 的效率和有效性；
KPI 和应用软件安全指标触发了对应用软件安全战略的大部分更改。

回答

没有；
是的，但是审查是临时的；
是的，我们会定期审查；
是的，我们每年至少审查一次。

1.2 策略与合规

策略与合规（PC）的实践重点是理解和满足外部法律和规范要求，同时推动内部安全标准以确保符合组织业务目的的合规。

在此实践中，进行改进的一个驱动因素是将组织的标准和第三方义务描述为应用软件需求，从而在 SDLC 中实现高效且自动化的审核，并不断证明满足了所有期望。

综合而言，实施该实践既需要组织范围内对内部标准和外部合规驱动因素的理解，也需要与项目团队保持及时检查，以确保没有可见性的项目无法按预期运行。

成熟度等级		活动流 A 政策与标准	活动流 B 合规管理
1 级	识别并记录与组织相关的治理和合规驱动因素。	确定代表组织策略和标准的安全基线。	识别第三方合规驱动因素和要求，并映射到现有策略和标准。
2 级	建立特定于应用软件的安全和合规基线。	制定适用于所有应用软件的安全需求。	发布特定于合规的应用软件要求和测试指南。
3 级	测量对策略、标准和第三方要求的遵守情况。	测量并报告单个应用软件对策略和标准的遵守情况。	测量并报告单个应用软件是否符合第三方要求。

1.2.1 策略与标准

1.2.1.1 成熟度等级 1

收益

对组织最低安全等级有明确的期望。

活动

开发策略和标准库，以管理组织中软件开发的各个方面。策略和标准基于现有的行业标准，并且适用于组织的行业。由于各种特定于技术的限制和最佳实践，请与各个产品团队一起审查建议的标准。为了提高应用软件和计算基础设施的安全性，我们的首要目标是邀请产品团队就标准中可能不可行或不具有成本收益的方面提供反馈，以及产品团队需要对标准进一步投入力量的机会点。

对于策略，应强调不依赖于特定技术或托管环境的应用软件安全高层定义和方面。关注组织更广泛的目标，以保护其计算环境的完整性、数据的安全性和隐私性、软件开发生命周期的成熟度。对于大型组织，策略可能会根据数据分类或应用软件功能来满足特定要求，但其详细程度不足以提供特定于技术的指导。

对于标准，结合策略提出的要求，专注于特定技术的实施指南。这些特定技术能识别和利用不同开发语言和框架的安全功能。标准需要高级开发人员和架构师的意见，而架构师被认为是组织所使用各种技术的专家。创建标准，并允许对它们定期更新。标识或标记出策略或第三方要求的各个要求，以使维护和审计工作更加容易和高效。

问题

您在整个组织中是否拥有并应用一套通用的策略和标准？

质量标准

您已经采用了适合于组织所在行业的现有标准，以解决特定域的问题；
您的标准与策略保持一致，并纳入特定于技术的实施指南。

回答

没有；
是的，对于某些应用；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

1.2.1.2 成熟度等级 2

收益

对产品团队如何遵守安全策略形成共识。

活动

为了帮助对策略和标准的持续执行和合规验证，对每个可用的要求开发适用的应用软件安全测试脚本。将这些文档组织到库中，并提供给所有的应用软件团队，以合适的格式应用在每个应用软件中。清楚地标记文档，并将它们链接到它们代表的策略和标准，以帮助进行不断的更新和维护。每次迭代更新的版本策略、标准、包含详细信息的更改日志，使不同产品的 SDLC 中变得容易。

以与现有需求管理流程一致的格式编写应用软件安全需求。您可能需要多个版本来满足不同的开发方法或技术。目的是使各个产品团队能够轻松地将策略和标准纳入其现有的开发生命周期，而这些需求仅需提供最少的注解信息。

测试脚本通过对应用软件功能的明确预期，能够强化应用软件的安全需求，并指导可能已经在开发过程中发挥作用的自动化测试或人工测试。这些投入不仅可以帮助每个团队建立对现有策略和标准的当前合规状态，还可以随着应用软件的不断变化而确保合规。

问题

您是否以测试脚本或运行手册的形式发布组织的策略，以方便开发团队进行解释？

质量标准

您创建了验证清单列表和测试脚本，并与策略要求和相关标准中的实施指南保持一致；
您创建了适用于组织所使用每种开发方法和技术的版本信息。

回答

没有；
是的，有一些内容；
是的，至少有一半的内容；
是的，有大部分或全部内容。

1.2.1.3 成熟度等级 3

收益

理解组织对政策和标准的合规情况

活动

制定一个能衡量每个应用软件是否符合现有策略和标准的计划。应当激发强制性要求，并在所有团队中一致地报告。尽可能将合规状态关联到自动化测试中，并针对每个版本进行报告。合规报告包括策略和标准的版本以及适当的代码覆盖情况。

鼓励不合规的团队查看可用资源（例如：安全需求和测试脚本），以确保不合规不是由于指导不足而导致的。将因指导不足而导致的问题提供给负责发布应用软件需求和测试脚本的团队，以将其包括在将来的版本中。对于没有能力解决应用软件安全风险以达到策略与标准要求的团队，将他们产生的问题升级。

问题

您是否定期报告策略和标准的合规情况，并使用该信息指导合规工作的改进？

质量标准

您具有定期生成合规报告的过程（如果可能的话，以自动的形式生成报告）；
您将合规报告提供给所有相关的利益相关者；
利益相关者使用报告的合规状态信息来确定需要改进的地方。

回答

没有；
是的，但是报告是临时的；
是的，我们会定期报告；
是的，我们每年至少报告一次。

1.2.2 合规管理

1.2.2.1 成熟度等级 1

收益

安全策略和标准与外部合规驱动因素保持一致。

活动

创建包含了所有合规要求的列表，包括可以帮助确定哪些应用软件属于特定范围内的所有触发要素。在考虑范围内的合规要求，可以根据地理位置、数据类型、与客户或业务合作伙伴之间的合同义务等因素纳入范围。与适当的专家和法律人员一起检查每个已确定的合规要求，以确保了解义务。由于许多合规义务的适用性会根据在整个计算环境中如何处理、存储、传输数据而有所不同，因此，合规驱动程序应始终指出通过更改数据处理方式来降低总体合规负担的机会。

评估发布合规矩阵，以帮助确定哪些因素可以使应用软件符合特定的法规要求。使矩阵表明哪些合规要求适用于组织级别，并且不依赖于各个应用软件。该矩阵至少提供了对于有用的合规要求的基本理解，以审查围绕不同应用软件的义务。

由于许多合规标准都集中在安全最佳实践方面，因此，许多合规要求可能已经成为组织发布“策略和标准”库的一部分。因此，一旦您查看合规要求，请将其映射到任何适用的现有策略和标准。只要有差异，就更新策略和标准以包括组织范围内的合规要求。然后，开始创建仅适用于单个合规要求的特定于合规的标准。目标是拥有一个合规矩阵，该矩阵指示哪些策略和标准具有有关合规要求的更详细信息，并确保各个策略和标准都引用适用的合规要求。

问题

您对外部合规义务有完整的了解吗？

质量标准

您已确定外部合规义务的所有来源；
您已从所有来源捕获并协调了合规义务。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

1.2.2.2 成熟度等级 2

收益

对产品团队如何符合外部合规驱动程序形成共识。

活动

开发应用软件需求和测试脚本库，以建立和验证应用软件的法规遵从性。其中，与诸如 PCI 或 GDPR 之类的个人合规要求相关联，而其他一些则主要是全球性的合规要求，如 ISO 标准。该库可用于所有应用软件的开发团队，它包括确定所有适用要求的指南，而这些指南则包含了减少合规成本投入和范围的考虑因素。实施一个定期重新评估每个应用软件合规要求的流程。重新评估包括检查所有应用软件的功能和机会，以缩小范围，从而降低合规总成本。

需求需包括足够的信息，供开发人员了解不同合规的功能和非功能需求。它们包括对策略和标准的引用，及对法规的明确引用。如果对特定要求的实施有疑问，法规的原始文本可以帮助开发人员更准确地理解其意图。每个需求都包括一组用于验证符合性的测试脚本。除了协助质量检查人员进行合规验证外，还可以帮助开发人员阐明合规要求，并使合规流程透明化。需求信息可以被导入到各个需求库中。

问题

您是否有一套标准的安全需求和验证程序来解决组织的外部合规义务？

质量标准

您将每个外部合规义务映射到一组定义明确的应用软件需求；
您定义验证程序（包括自动测试），以验证是否符合相关要求。

回答

没有；
是的，有一些义务；
是的，至少承担一半义务；
是的，对于大部分或全部义务。

1.2.2.3 成熟度等级 3

收益

了解您的组织有关外部合规驱动因素的合规情况。

活动

开发一个测量和报告不同应用软件合规状态的计划。应用软件需求和测试脚本有助于确定合规状态。利用自动化测试手段，迅速检测到频繁更新的应用软件中存在的不合规情况，并确保通过不同的应用软件版本保持合规。当无法进行全自动测试时，质量保证、内部审计或信息安全团队则通过手动测试和访谈相结合的方式定期评估合规状态。

百分之百合规始终是最终目标，因此，需在计划中包含追踪补救措施和定期更新。定期审查合规修复活动，以检查团队是否取得了适当的进展，并且该修复策略将有效地实现合规目标。为了进一步改善流程，需开发一系列标准报告和合规记分卡。这些可以帮助各个团队了解当前的合规状态，并且组织管理层可以协助更有效地弥补合规差距。

与相关专家一起审查需要大量投入或开发的合规差距，并将其与减少应用软件功能、最小化范围或消除合规要求的成本进行比较。长期的合规差距需要得到管理层的批准和正式的合规风险接受，因此，它们需要组织领导层的适当关注和审查。

问题

您是否定期报告外部合规义务的遵守情况，并使用这些信息来指导有关缩小合规差距的工作？

质量标准

您已经建立了明确定义的合规指标；
您定期测量和报告应用软件的合规指标；
利益相关者使用报告的合规状态信息来识别合规差距，并确定差距补救工作的优先级。

回答

没有；
是的，但是报告是临时的；
是的，我们会定期报告；
是的，我们每年至少报告一次。

1.3 教育与指导

教育与指导（EG）的实践重点是为软件生命周期中的相关人员提供知识和资源，以设计、开发和部署安全的软件。通过对信息访问的优化，项目团队可以主动识别和减轻适用于其组织的特定安全风险。

跨目标改进的一个主题是为员工提供培训，并提升他们的安全意识。培训方式可以是讲师授课或是上机实操。随着组织的进步，建立起广泛的培训基础，从开发人员开始，然后转移到其他角色，最后增加基于角色的培训，以确保适用性和有效性。

除了培训外，此实践还要求组织在改善组织文化方面进行大量投资，以通过团队之间的协作来提高应用软件安全。协作工具以及技术和工具之间更高的透明度也支持了此方法，以提高应用软件安全。

成熟度等级		活动流 A 培训和意识	活动流 B 组织和文化
1 级	为员工提供有关安全开发和部署主题的可访问资源。	为所有软件开发涉及的人员提供安全意识培训。	在每个开发团队中确定一个“安全专家（Security Champion）”。
2 级	对软件生命周期中的所有人员提供有关安全开发技术和针对特定角色指导的教育。	提供技术和特定角色的指导，包括每种语言和平台的安全细微差别。	开发一个安全软件中心，以显著促进开发人员和架构师的思想领导力。
3 级	开发由不同团队开发人员共同推动的内部培训计划。	围绕组织的安全软件开发标准形成标准化的内部指导。	建立一个软件安全社区，包含所有参与软件安全的组织内部人员。

1.3.1 培训和意识

1.3.1.1 成熟度等级 1

收益

所有相关员工的基本安全意识。

活动

对当前参与软件管理、开发、测试、审计的所有角色进行安全意识培训。目的是提高人们对应用软件安全威胁和风险、安全最佳实践以及安全软件设计原则的认识。在组织内部创建培训，或从外部购买培训。理想情况下，应提供面对面的培训，以便参与者可以进行小组讨论，但是也可以选择基于计算机的上机培训。

课程内容应包括与应用软件安全和隐私相关的一系列主题，同时非技术受众也可以参与。安全设计原则中的适用概念，如：最低特权、纵深防御、安全故障保护、完全消减、会话管理、开放式设计和心理可接受性。此外，培训还应包括为提升应用软件安全而定义的所有组织范围内的标准、策略和过程的参考资料。OWASP Top 10 中的安全脆弱点应得到重点覆盖。

所有参与软件开发的员工和承包商都必须接受培训，其中包括可审计的签字文件以证明培训的合规性。可以考虑采用创新的交付方式（如游戏化），以最大程度地发挥效果并确保培训脱敏。

问题

您是否要求涉及应用软件开发的员工接受 SDLC 培训？

质量标准

培训是可重复的、持续的，并且对任何参与软件开发生命周期的人员都可用。
培训在适当的情况下包括最新的 OWASP Top 10，并包括诸如最低权限、纵深防御、安全故障保护、完全消减、会话管理，开放式设计和心理接受性的概念。
培训需要参加者的签字或确认。
您在最近 12 个月内更新了培训。
在员工入职过程中提供了培训。

回答

没有；
是的，要求其中一些；
是的，要求至少有一半；
是的，要求大多数或全部。

1.3.1.2 成熟度等级 2

收益

根据员工的具体角色对相关员工角色进行培训

活动

从核心开发团队开始，针对组织的角色和技术进行讲师授课或上机实操安全培训。组织根据每个小组的技术需求为产品经理、软件开发人员、测试人员和安全审核员定制培训。

- 产品经理对与 SAMM 业务功能和安全实践相关的主题进行培训，重点是安全需求、威胁建模和缺陷跟踪。
- 开发人员对其使用的技术进行编码规范和最佳实践方面进行培训，以确保培训直接有益于应用软件安全。他们对 OWASP Top 10 安全脆弱点或类似弱点相关的技术和使用的框架（如：移动应用）、以及对每个问题最常见的消除策略，具有扎实的技术理解。
- 测试人员对组织中使用的不同测试工具、相关技术的最佳实践、以及识别安全缺陷的工具进行培训。
- 安全审核员对软件开发生命周期、组织中使用的应用软件安全机制、以及提交安全缺陷进行修复的过程进行培训。
- 安全专家对 SDLC 各个阶段的安全主题进行培训。他们接受与开发人员和测试人员相同的培训，但也了解威胁建模和安全设计以及可以集成到构建环境中的安全工具和技术。

包括此活动流“成熟度等级 1 级”活动中的所有培训内容，以及其他特定于角色和特定于技术的内容。其他方面的内容不必包含。

理想情况下，确定每种技术的主题专家，以协助采购或开发培训内容并定期进行更新。培训包括使用故意包含安全缺陷的应用软件（如：OWASP WebGoat、OWASP Juice Shop）进行漏洞利用的演示，并将先前渗透的结果作为漏洞和已实施的补救策略的示例。可获得渗透测试人员协助，开发漏洞利用的演示示例。

所有参与软件开发的员工和承包商都必须接受培训，其中包括可审计的签字材料，以证明培训的合规性。只要有可能，培训还应包括考试，以确保培训内容得到了训参与者的理解，而不仅仅是遵守。每年更新并提供培训，包括组织、技术和趋势方面的变化。向培训参与者进行培训反馈调查，以评估培训的质量和相关性，并收集有关于培训参与者工作或环境的建议信息。

问题

培训是否对不同角色（如：开发人员、测试人员或安全专家）进行量身定制？

质量标准

培训包括“成熟度等级 1”中的所有培训主题，并增加了其他特定的工具、技术和演示；
所有员工和承包商都必须参加培训；
培训包括组织内部专家和受训人员的输入信息；
培训包括组织内部开发的工具和技术演示；
使用培训反馈信息对培训进行优化。

回答

没有；

是的，对于一些培训；

是的，对于至少一半的培训；

是的，对于大多数或所有培训。

1.3.1.3 成熟度等级 3

收益

在员工执行关键任务前，确保员工具有足够的安全知识。

活动

实施正式的培训计划，该计划要求与软件开发生命周期有关的任何人员在入职过程中完成适当的角色和特定于技术的培训。根据应用软件的重要性和用户角色，考虑限制员工的访问权限，直到完成入门培训为止。尽管组织可以从外部获取一些培训模块，但该计划是在内部进行促进和管理的，并且包括特定于组织的内容，而这些内容超出了常规的安全最佳实践。该计划具有明确的课程表、参训人员参与情况检查，并对学习内容的理解和掌握能力进行测试。培训内容由行业最佳实践和组织内部标准组成，包括对组织使用的特定系统进行培训。

除了与安全直接相关的问题外，组织在该培训计划中还应包括其他标准，如：代码复杂性、代码文档、命名规范以及其他与过程相关的内容。该培训最大程度地减少了因员工遵循组织外部的惯例而导致的问题，并确保了代码样式和技能的连续性。

为了促进监视进度和成功完成每个培训模块，组织应配备一个学习管理平台或一个具有类似功能的集中门户。即使员工完成了初始培训，员工也可以掌握他们自己的培训进度，并获得所有培训资源。

至少每年检查一次由于员工没有遵循既定标准、政策、程序或安全最佳实践而导致的问题，以评估培训的有效性，并确保培训涵盖与组织有关的所有问题。定期更新培训内容，并为员工提供有关最新安全缺陷和变更方面的培训课程。

问题

您是否配备了一个学习管理系统或类似系统来追踪员工的培训和认证过程？

质量标准

学习管理系统被用于追踪培训和认证过程；
培训基于内部标准、政策和程序；
使用认证计划或考勤记录来确定对开发系统和资源的访问。

回答

没有；
是的，对于一些培训；
是的，对于至少一半的培训；
是的，对于大多数或所有培训。

1.3.2 组织和文化

1.3.2.1 成熟度等级 1

收益

将安全基本嵌入在开发组织中。

活动

实施一个计划，其中，每个软件开发团队都有一个被视为“安全专家（Security Champion）”的成员，该成员是信息安全人员与开发人员之间的联络人。根据团队的规模和结构，“安全专家”可能是软件开发人员、测试人员或产品经理。“安全专家”每周有固定的工作小时数与信息安全相关实践相关。他们参加定期的情况介绍会，以提高对不同安全领域的认识和专业知识。“安全专家”需要接受额外的培训，以帮助他们发展作为软件安全主题专家。出于文化原因，您可能需要自定义创建和支持“安全专家”的方式。

该职位的目标是提高应用软件安全和合规的有效性和效率，并加强各个团队与信息安全团队之间的关系。为了实现这些目标，“安全专家”将协助研究、验证与安全性和合规相关的软件缺陷，并确定它们的优先级。“安全专家”参与所有的风险评估、威胁评估和架构审查工作，通过使应用软件架构更具弹性并减少攻击威胁面，来帮助确定消除安全缺陷的机会。

除了协助信息安全团队外，“安全专家”还为项目团队定期审查所有与安全相关的问题，以便每个人都知道问题所在以及当前和将来的补救措施。通过与整个开发团队合作，可以利用这些评论来为更复杂的问题集思广益。

问题

您是否为每个开发团队确定了“安全专家”？

质量标准

“安全专家”接受了适当的培训；
应用软件安全团队和开发团队会定期收到来自“安全专家”的简报，内容涉及安全计划和修复的总体状态；
“安全专家”在解决应用软件积压的问题之前，先审查外部测试的结果。

回答

没有；
是的，对于某些团队；
是的，对于至少一半的团队；
是的，对于大多数或所有团队。

1.3.2.2 成熟度等级 2

收益

针对组织量身定制的特定最佳安全实践。

活动

该组织实施了一个正式、卓越的安全编码中心，由架构师和高级开发人员代表不同的业务部门和技术堆栈。该团队有一份官方章程，并定义了改进软件开发实践的标准和最佳实践。目的是减轻由于技术、编程语言、开发框架和库的快速变化，使信息安全专业人员难以充分了解所有技术的细微差别对安全的影响。即使是开发人员，对于为了使软件开发更快、更好、更安全的发展变化和新工具，也常常难以跟上步伐。

这样可以确保当前进行的所有编程工作都遵循行业的最佳实践，并且组织的开发和实施标准包括所有关键配置设置。这有助于确定、培训和支持“产品专家（Product Champion）”，他们负责协助不同的团队使用工具，以实现 SDLC 各方面自动化、合理化或改进。它确定了 SDLC 中具有较高成熟度等级的开发团队，以及达到高成熟度等级的实践和工具，目的是将其复制给其他团队。

该小组提供了特定主题的专家，帮助信息安全团队评估工具和解决方案以提高应用软件安全性，确保这些工具不仅有用，而且与不同团队开发应用软件的方式兼容。希望对其软件进行重大架构变更的团队需与该小组联系，以避免对 SDLC 或已建立的安全控制产生不利影响。

问题

组织是否有一个卓越的安全软件中心（SSCE）？

质量标准

SSCE 有一个章程来定义其在组织中的角色；
开发团队与 SSCE 审查所有重要的架构变更；
SSCE 发布与应用软件安全相关的 SDLC 标准和指南；
产品专家负责促进特定安全工具的使用。

回答

没有；
是的，刚开始实施；
是的，作用于组织的一部分；
是的，作用于整个组织。

1.3.2.3 成熟度等级 3

收益

和所有产品团队共同开发安全知识。

活动

安全是所有员工的责任，而不仅仅是信息安全团队的责任。部署交流和知识共享平台，以帮助开发人员围绕不同的技术、工具和编程语言建立社区。在这些社区中，员工共享信息、与其他开发人员讨论遇到的技术问题，并能在知识库中搜索到先前讨论问题的回答。

围绕角色和职责形成社区，并使来自不同团队和业务部门的开发人员和工程师在社区中能够自由交流，并从彼此的专业知识中受益。鼓励大家参与，制定计划以促进那些帮助最多的人成为思想领袖，并使管理层认识他们。除了提高应用软件的安全性之外，该平台还可以根据人们的专业知识和帮助他人的意愿，帮助确定卓越安全软件中心或“安全专家”的未来成员。

卓越安全软件中心和应用软件安全团队会定期审查信息门户，以了解新的和即将到来的技术，以及通过新计划、新工具、新程序和新培训资源帮助社区的机会。使用门户网站向所有开发人员传播有关新标准、新工具和资源信息，以不断提高组织的 SDLC 成熟度和应用软件安全。

问题

是否有一个集中的门户网站，支持来自不同团队和业务部门的开发人员和应用软件安全专业人员交流和共享信息？

质量标准

组织为不同的团队和业务部门推广使用唯一的一个门户网站；
该门户网站用于及时信息发布，如：安全事件、工具更新、架构标准更改的通知，以及其他相关公告；
该门户网站被开发人员和架构师广泛认可为组织特定的应用软件安全信息集中存储库；
所有内容都被认为是可持久使用的和可搜索的；
该门户网站可访问特定于应用软件的安全指标。

回答

没有；
是的，刚开始实施；
是的，对于组织的一部分可用；
是的，对于整个组织可用。

2、 设计

设计，涉及到与组织如何定义目标和在开发项目中创建软件有关的过程和活动。通常，这将包括需求收集、高级架构规范和详细设计。

2.1 威胁评估

威胁评估（TA）实践的重点是基于正在开发的软件功能和运行时的环境特征，识别和理解项目级风险。通过分析每个项目威胁和潜在攻击的详细信息，对安全措施的优先级设置进行更好的决策，从而使整个组织更有效地运作。此外，对风险接受的决策更加明智，因此可以更好地与业务保持一致。

通过从简单的威胁模型开始，并构建应用软件风险的画像，组织随着时间的推移不断改进。最终，一个成熟的组织将不断维护此类信息，而维护的方式是与外部实体的补偿因素和传递风险紧密相连。这样可以更广泛地了解安全问题可能对下游产生的影响，同时可以密切关注组织当前在已知威胁下的运转情况。

成熟度等级		**活动流 A** **应用软件风险画像**	**活动流 B** **威胁建模**
1 级	在软件需求过程中明确考虑安全性。	对应用软件安全风险进行基本评估，以了解攻击的可能性和影响。	使用头脑风暴法和带有简单威胁列表清单的现有图表，尽力而为，执行基于风险的威胁建模。
2 级	提升源自业务逻辑和已知风险的安全需求颗粒度。	通过集中利益相关者的所有风险画像来了解组织中所有的应用软件安全风险。	标准化威胁建模的培训、流程和工具，以在整个组织范围内进行推广。
3 级	对所有的软件项目和第三方依赖项，要求安全需求过程。	定期审查应用软件风险画像，以确保准确性并反映了当前的状态。	不断优化和自动化威胁建模方法。

2.1.1 应用软件风险画像

2.1.1.1 成熟度等级 1

收益

能根据风险对应用软件进行分类。

活动

使用一种简单的方法来评估每个应用软件的安全风险，以评估其在遭受攻击时对组织业务造成的潜在影响。为此，评估破坏对数据或服务的机密性、完整性和可用性的影响。考虑使用一组 5 至 10 个问题来理解重要的应用软件特征，例如：应用软件是否处理财务数据、是否面向互联网、是否涉及隐私相关数据。应用软件风险画像会告诉您这些因素是否适用，以及它们是否会对组织产生重大影响。

接下来，根据风险，使用一个方案对应用软件进行分类。这个方案可以是简单、定性的（如：高、中、低），将风险特征转化为一个对应风险值，这通常是有效的。使用这些值表示和比较不同应用软件的风险非常重要。高度成熟的风险驱动型组织可能使用定量风险方案。如果您的组织已经有一个运作良好的风险方案，就不要发明一个新的风险方案。

问题

您是否使用一组简单且预定义的问题，并根据业务风险对应用软件进行分类？

质量标准

已有商定的风险分类方法；
应用团队了解风险分类；
风险分类涵盖组织面临业务风险的关键方面；
组织拥有范围内应用软件的清单。

回答

没有；
是的，有其中一些；
是的，有至少一半；
是的，有大多数或全部。

2.1.1.2 成熟度等级 2

收益

对您应用软件风险水平有深入的理解。

活动

该活动的目标是彻底了解组织内所有应用软件的风险级别，并在真正重要的方面集中精力进行软件保障活动。

从风险评估的角度来看，一组基本问题不足以彻底评估所有应用软件的风险。创建一个广泛且标准化的方法来评估应用软件的风险，以及通过其对信息安全（数据的保密性、完整性和可用性）的影响来评估。除了安全，您还希望评估应用软件的隐私风险。了解应用软件处理的数据以及与哪些潜在侵犯隐私行为是相关的。最后，研究此应用软件对组织内其他应用软件的影响（例如，该应用软件可能正在修改在另一上下文中被视为只读的数据）。评估组织内的所有应用软件，包括所有现有的和旧的应用软件。

利用业务影响分析来量化和分类应用软件风险。简单的定性方案（如：高、中、低）不足以在企业范围内有效地管理和比较应用软件。

基于此输入，安全官员利用分类来定义风险画像，以建立风险画像的集中清单并管理责任制。此清单为产品所有者、经理和其他组织涉众提供了应用软件风险级别的一致视图，以便为与安全相关的活动分配适当的优先级。

问题

您是否使用集中和量化的应用软件风险画像来评估业务风险？

质量标准

应用软件风险画像符合组织风险标准；
应用软件风险简介涵盖了对安全和隐私的影响；
您可以手动和/或自动验证风险画像的质量；
应用软件风险画像集中存储。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

2.1.1.3 成熟度等级 3

收益

当发生变更时，及时更新应用软件分类。

活动

组织的应用软件组合以及应用软件生存的条件和约束（如，受公司战略驱动）会发生变化。定期检查风险清单，以确保不同应用软件风险评估的正确性。

在企业范围内进行定期审查。另外，随着企业在软件保障方面的成熟，激发团队不断询问哪些条件变化可能会影响风险状况。例如，一个内部应用软件可能会由于业务决策而暴露于互联网。这应该触发团队重新执行风险评估，并相应地更新应用软件风险画像。

在此实践的成熟执行过程中，对团队进行培训并不断更新这些风险评估中的经验教训和最佳实践。这样，可以更好地执行应用软件并更准确地表述应用软件风险画像。

问题

您是否定期审查和更新应用软件的风险画像？

质量标准

组织的风险标准考虑了历史反馈，以不断改进评估方法；
应用软件或业务环境中的重大变化，会触发对相关风险画像的审查。

回答

没有；
是的，偶尔；
是的，当应用软件发生变更后；
是的，至少每年一次。

2.1.2 威胁建模

2.1.2.1 成熟度等级 1

收益

识别应用软件中的架构设计缺陷。

活动

威胁建模是一种结构化活动，用于识别、评估和管理系统威胁、架构设计缺陷和建议的安全缓解措施。它通常作为设计阶段或安全评估的一部分完成。

威胁建模是一个团队作业，包括产品所有者、架构师、安全专家和安全测试人员。在此成熟度级别上，使团队和涉众可以进行威胁建模，以提高安全意识并创建对系统安全性的共识。

在成熟度等级 1 上，可以对高风险应用软件临时执行威胁建模，并使用简单的威胁清单，例如 STRIDE。避免进行冗长的讨论会，并避免对低级别威胁进行过于详细的列出。迭代执行威胁建模，以适应更多的迭代开发范例。如果将新功能添加到现有应用软件中，则仅查看新添加的功能，而不尝试覆盖整个范围。一个很好的起点是您在讨论会上对现有图表进行注释。始终确保对威胁建模讨论的结果进行保留，以备后用。

启动威胁建模的最重要工具是白板、智能板或一张纸。争取与团队就安全意识、简单的过程和可行的结果达成共识。

问题

您是否通过威胁建模识别和管理架构设计缺陷？

质量标准

您对高风险应用软件执行威胁建模；
您使用简单的威胁清单，例如 STRIDE；
您将威胁模型的结果保留下来，以备后用。

回答

没有；
是的，使用了其中一些；
是的，使用了至少有一半；
是的，使用了大多数或全部。

2.1.2.2 成熟度等级 2

收益

对威胁建模活动的质量有明确的期望。

活动

为您的组织使用标准化的威胁建模方法，并将其与您的应用软件风险等级设置保持一致。考虑在整个组织内推广使用威胁模型。

培训您的架构师、安全专家和其他利益相关者如何进行实际的威胁建模。威胁建模需要相关的理解、清晰的操作手册和模板、特定于组织的示例、经验，而这些都很难实现自动化。

您的威胁建模方法论至少包括图表、威胁识别、设计缺陷缓解措施以及如何验证威胁模型的成果输出。您的威胁模型图可让您详细了解环境和应用软件的机制。您可以通过清单（例如：STRIDE）来发现对应用软件的威胁，或更多组织特定的威胁。对于已确定的设计缺陷（根据组织的风险进行排序），您可以添加缓解控制措施以支持利益相关者应对特定威胁。定义触发更新威胁模型的触发因素，例如：技术变更或在新环境中部署应用软件。

将威胁建模的输出反馈给缺陷管理过程，以进行适当的跟进。用应用软件团队使用的工具获得威胁建模的成果输出。

问题

您是否使用符合您应用软件风险级别的标准方法？

质量标准

培训您的架构师、安全专家和其他利益相关者如何进行实际威胁建模；
您的威胁建模方法论至少包括：图表、威胁识别、设计缺陷缓解措施以及如何验证威胁模型成果输出的方法；
应用软件或业务环境中的变化，会触发对相关威胁模型的审查；
用应用软件团队使用的工具获得威胁建模成果输出。

回答

没有；
是的，对于某些应用使用；
是的，对于至少一半的应用软件使用；
是的，对于大多数或所有应用软件使用。

2.1.2.3 成熟度等级 3

收益

确保持续改进威胁建模活动。

活动

威胁建模已集成到您的 SDLC 中，并已成为开发人员安全文化的一部分。根据组织的威胁模型，创建和改进了可重用的风险模式，包括相关的威胁库、设计缺陷和安全缓解措施。您定期（例如，每年一次）检查现有威胁模型，以验证应用软件与新的威胁无关。

您可以优化威胁建模方法。您从威胁模型中学到经验教训，并使用它们来改进威胁建模方法。您查看与组织相关的威胁类别，并适当地更新您的方法。您会不时地独立评估威胁模型的质量。

您可以使用威胁建模工具自动化执行威胁建模过程。您将威胁建模工具与其他安全工具集成在一起，例如：安全验证工具和风险跟踪工具。您考虑了“威胁建模作为代码”实践，以将威胁建模成果输出与应用软件代码集成在一起。

问题

您是否定期检查和更新了应用软件的威胁建模方法？

质量标准

威胁模型方法论考虑了历史反馈信息以进行改进；
您定期（例如，每年一次）审查现有的威胁模型，以验证应用软件与新的威胁无关；
使用威胁建模工具自动化执行威胁建模过程。

回答

没有；
是的，但是审查是临时的；
是的，我们会定期审查；
是的，我们至少每年审查一次。

2.2 安全需求

安全需求（SR）实践聚焦于对安全软件而言重要的安全需求。第一种类处理典型的与软件相关需求，以指定目标和期望，从而保护应用软件核心的服务和数据。第二种类涉及与供应商组织有关的需求，这些需求属于应用软件开发上下文的一部分，尤其是对于外包开发而言。重要的是简化安全开发方面的期望，因为外包开发可能会对应用软件的安全产生重大影响。第三方（技术）库的安全性是软件供应链的一部分（请参阅“安全构建”部分），本实践中没有包含。

成熟度等级		活动流 A 软件需求	活动流 B 供应商安全
1 级	在软件需求过程中明确考虑安全性。	高级别的应用软件安全目标已映射到功能需求。	根据组织的安全需求评估供应商。
2 级	提升源自业务逻辑和已知风险的安全需求颗粒度。	已形成结构化的安全需求，且开发人员团队可以使用。	将安全纳入供应商协议中，以确保符合组织要求。
3 级	对所有的软件项目和第三方依赖项，要求安全需求过程。	建立供产品团队使用的需求框架。	通过提供明确的目标来确保外部供应商的适当安全范围。

2.2.1 软件需求

2.2.1.1 成熟度等级 1

收益

了解开发过程中的关键安全需求。

活动

对软件项目的功能需求进行审查。通过推理软件项目提供服务或数据的机密性、完整性、可用性，确定此功能的相关安全需求（即，期望）。需求应陈述目标（如，“应该安全地传输和存储注册过程中的个人数据”），而不是达到目标的实际措施（如，“使用 TLSv1.2 进行安全传输”）。

同时，从攻击者的角度检查功能，以了解该功能如何被滥用。这样，您可以为手里的软件项目确定额外的保护需求。

安全目标可能与您需要添加到应用软件中的特定安全功能（如，“始终标识应用软件的用户”）或整个应用软件的质量和行为（如，“确保在传输过程中正确保护个人数据”）相关，但不一定会带来新功能。遵循编写安全需求的良好做法。使它们具体、可测量、可操作、相关、有时间限制（SMART）。提防添加的需求过于通用（如，应用软件应防止 OWASP Top 10），以至于与手里的应用软件无关。尽管它们是正确的，但并不能增加讨论的价值。

问题

项目团队在开发过程中是否明确安全需求？

质量标准

团队从功能需求以及客户或组织的关注中得出安全需求；
安全需求是特定的、可测量的和合理的；
安全需求符合组织基线。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

2.2.1.2 成熟度等级 2

收益

使安全需求与其他类型的需求保持一致。

活动

安全需求可以源自其他来源，包括：策略和法规、应用软件中的已知问题、来自测量和反馈的情报资讯。在此级别上，必须通过分析安全需求的不同来源，来实现对安全需求更系统的启发。确保从这些来源获得适当的输入，以帮助确定需求。例如，组织访谈或头脑风暴会议（如，在政策和立法的情况下）、历史记录或漏洞系统分析。

对应用软件安全需求使用结构化表示方法，并为项目集成其他（功能）需求指定的方式。例如，扩展分析文档、编写用户故事等。

当明确了安全需求后，在产品开发过程中考虑这些安全需求就变得十分重要了。设置一种机制来刺激或强迫项目团队满足产品中的这些安全需求。例如，为安全需求设置优先级、强调安全需求处理的影响以增强足够的安全偏好（同时与其他非功能性需求保持平衡）。

问题

您是否在安全需求收集过程的成果输出中定义、结构化并包含安全需求的优先级？

质量标准

当策略和指南应用于产品开发时，安全需求考虑了特定领域的知识；
领域专家参与需求定义过程；
您已经就安全需求达成了一致的结构化表示法；
开发团队拥有一名安全专家，专门负责审查安全需求和结果。

回答

没有；
是的，有时候；
是的，至少有一半的时候；
是的，大部分或所有时候。

2.2.1.3 成熟度等级 3

收益

高效、有效地处理组织中的安全需求。

活动

设置安全需求框架，以帮助项目获得适当而完整的需求集。该框架考虑了不同类型的需求和需求来源。它应适应组织的习惯和文化，并在确定和形成需求时提供有效的方法和指导。

该框架可帮助项目团队提高需求工程的效率和有效性。它可以提供多类常见的需求和许多可重用的需求。请记住，尽管未经考虑的“拿来主义”通常效率低下，但对潜在的相关需求进行推理，通常则会产生效果。

该框架还对需求的质量给出了明确的指导，并规范了如何描述它们。对于用户故事，比如，具体的指导可以解释：完成的定义是什么、就绪的定义是什么、故事描述是什么、接受标准是什么。

问题

您是否使用标准需求框架来简化对安全需求的获取？

质量标准

安全需求框架对项目团队可用；
该框架按通用要求和基于标准的要求进行分类；
该框架为需求质量以及如何描述需求提供了明确的指导；
该框架可适应特定的业务需求。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

2.2.2 供应商安全

2.2.2.1 成熟度等级 1

收益

软件供应商的安全实践公开透明。

活动

参与软件开发的外部供应商，其安全能力和习惯可能会对最终产品的安全态势产生重大影响。因此，在此方面了解并评估您的供应商就非常重要了。

执行供应商评估以了解您供应商的优缺点。使用基本的检查清单或进行访谈以审查其典型实践和交付方式。这使您了解他们如何组织自己和元素，以评估您是否需要采取其他措施来消减潜在风险。理想情况下，与组织中的不同角色交流，甚至为此目的执行一次小规模的成熟度评估。能力强的供应商会执行他们自己的软件保障计划，并且能够回答您的大多数问题。如果供应商在软件安全方面的能力较弱，请与他们讨论如何以及在什么程度上计划进行此工作，并评估这对您的组织是否足够。软件供应商可能正在从事低风险的项目，但这可能会改变。

您的供应商必须了解并适应风险偏好，并能够满足您在该领域的要求，这一点很重要。明确表达您对他们的期望，并进行明确讨论。

问题

利益相关者是否审查与合作供应商的安全需求和方法？

质量标准

当创建第三方协议时，您考虑了包括特定的安全需求、活动和流程；
配备了供应商调查表，以评估供应商的优势和劣势。

回答

没有；
是的，有时候；
是的，至少有一半的时间；
是的，大部分或所有时间。

2.2.2.2 成熟度等级 2

收益

明确定义软件供应商的安全职责。

活动

提高您对供应商软件安全能力的信心。讨论您的供应商和您自己组织的具体责任和期望，并与供应商签订合同。职责可以是特定的质量要求或特定任务，并且最低服务可以在《服务级别协议（SLA）》中详细说明。质量要求示例：供应商将针对 OWASP Top 10 为软件提供保护，并且如果发现问题，将予以修复。任务示例：供应商必须在主要版本发布之前执行连续的静态代码分析，或执行独立的渗透测试。协议中规定了若发生重大问题时的债务要求和处罚上限。

一旦在为几个供应商实施了此协议，则将此协议作为谈判的基础和对供应商的标准协议。您可以逐案偏离此标准协议，但这将帮助您确保不会忽略重要主题内容。

问题

供应商是否满足组织定义《服务级别协议》中的安全责任和质量措施？

质量标准

当创建供应商协议时与供应商讨论安全需求；
供应商协议中约定：在商定时间期限内提供有关安全缺陷修复的特定指导；
针对关键供应商安全流程，组织配备有职责和服务等级的模板协议；
测量关键的绩效指标。

回答

没有；
是的，有时候满足；
是的，至少有一半的时候满足；
是的，大部分或所有时候满足。

2.2.2.3 成熟度等级 3

收益

使软件开发实践与供应商保持一致以限制安全风险。

活动

最小化软件中出现安全问题风险的最佳方法，是最大程度地各方保持一致并紧密融合在一起。从过程的角度来看，这意味着使用相似的开发范例并引入常规的里程碑，以确保适当的对齐和质量改进。从工具的角度来看，这可能意味着使用相似的构建、验证和部署环境，并共享其他的支持工具（如，需求、架构工具或代码存储库）。

如果供应商无法实现您设定的目标，则实施补偿性控制，以便总体上实现您的目标。执行额外的活动（如，在开始实际的实施周期之前进行威胁建模）或采用额外的工具（如，在解决方案获取时进行第三方库分析）。供应商偏离您的要求的越多，就需要进行更多的工作来弥补。

问题

供应商是否与组织使用的标准安全控制、软件开发工具和流程保持一致？

质量标准

供应商拥有一个安全的 SDLC，其中，与组织使用的安全构建、安全部署、缺陷管理和事件管理相一致；
在每个主要版本发布之前，您都要验证解决方案是否满足质量和安全性目标；
如果没有标准的验证流程，则使用补偿控制机制，例如：软件成分分析、独立的渗透测试。

回答

没有；
是的，有时候；
是的，至少有一半的时候；
是的，大部分或所有的时候。

2.3 安全架构

安全架构（SA）实践聚焦于与在软件架构设计期间要处理的组件和技术相关的安全。安全架构设计着眼于有关解决方案构成基础的组件选择和组成，并着重于其安全性。技术管理着眼于在开发、部署和运营过程中所使用支持技术的安全性，例如，开发堆栈和工具，部署工具以及操作系统和工具。

成熟度等级		活动流 A 架构设计	活动流 B 技术管理
1 级	在软件设计过程中插入对主动安全指导的考虑。	在设计过程中，团队接受了有关基本安全原则使用方面的培训。	在整个解决方案中采用有效的技术、框架和集成来识别风险。
2 级	将软件设计过程导向到已知的安全服务和默认安全设计。	建立通用的设计模式和安全解决方案以供采用。	标准化在不同应用软件中使用的技术和框架。
3 级	正式控制软件设计过程并验证安全组件的使用情况。	使用参考的架构，并不断对使用情况和适当性进行评估。	在所有软件开发中强加标准技术的使用。

2.3.1 架构设计

2.3.1.1 成熟度等级 1

收益

一组安全基本原则可以被产品团队使用。

活动

在设计过程中，产品团队的技术人员使用简短的安全原则清单。通常，安全原则包括：纵深防御、保护最薄弱的链接、使用安全默认设置、安全功能设计的简单性、安全故障、安全和可用性的平衡、最小特权运行、因模糊而避免安全，等。

对于外围接口，团队会在整个系统的上下文中考虑每个原则，并确定可添加的功能以增强每个此类接口的安全性。限制这些设计，以使产品团队仅需在执行功能需求的正常研发前以的少量额外投入进行工作。注意投入较大的工作，并将其安排在未来版本的计划中。

在执行前，对每个产品团队进行安全意识培训，并与更多精通安全知识的人员合作制定设计决策。

问题

团队在设计过程中是否使用安全原则？

质量标准

您有一个已达成一致的安全原则清单；
您将安全原则清单存储在可访问的位置；
相关利益相关者了解安全原则。

回答

没有；
是的，对于某些应用软件使用；
是的，对于至少一半的应用软件使用；
是的，对于大多数或所有应用软件使用。

2.3.1.2 成熟度等级 2

收益

可重复使用的安全服务可以被产品团队使用。

活动

识别具有安全功能的共享基础结构或服务。这些通常包括单点登录服务、访问控制或授权服务、日志记录、监控服务、应用软件级防火墙。收集和评估可重用的系统，以收集形成此类资源的列表，并通过它们实现的安全性机制对其进行分类。对于每种资源，考虑产品团队为何需要集成它，如，使用共享资源的好处。

如果每个类别中存在多个资源，请为每个类别选择一个或多个共享服务并对其进行标准化。由于将来的软件开发将依赖于这些服务，因此请彻底检查每个服务以确保了解基线安全状况。对于每个选定的服务，为产品团队创建设计指南，帮助了解如何与系统集成。通过培训、指导、准则和标准提供指导。

建立一套代表最佳实践安全功能方法的最佳实践。您可以研究或购买它们，并且如果对它们进行自定义，这样通常会更有效，以便它们更适合您的组织。模式示例包括单点登录子系统、跨层委派模型、职责分离授权模型、集中式日志记录模式等。

这些模式可以源自特定的项目或应用软件，但是请确保您在组织中不同团队之间共享它们，以高效、一致地应用适当的安全解决方案。

为了增加对这些模式的采用，可以将它们链接到共享的安全服务，或将它们实现为可以在开发过程中轻松集成到应用软件中的实际组件解决方案。支持组织内的关键技术，例如在不同的开发堆栈的情况下。如有问题或疑问，请在适当支持下将这些解决方案视为实际应用。

问题

您在设计过程中是否使用共享安全服务？

质量标准

您有一份记录的可重用安全服务列表，并可供相关利益相关者使用；
您已经查看了每个选定服务的基线安全状况；
您的设计师经过培训，可以按照可用的指导集成每个选定的服务。

回答

没有；
是的，对于某些应用软件使用；
是的，对于至少一半的应用软件使用；
是的，对于大多数或所有应用软件使用。

2.3.1.3 成熟度等级 3

收益

集中提供的安全解决方案，其质量和可用性完全公开透明。

活动

建立一组参考架构，这些架构选择并组合一组经过验证的安全组件，以确保安全的恰当设计。参考平台在缩短审计和与安全相关的审核、提高开发效率以及降低维护开销方面具有优势。基于组织和社区内的新见识，不断维护和改进参考架构。让架构师、高级开发人员和其他技术利益相关者参与参考平台的设计和创建。创建后，团队将持续支持和更新。

参考架构可以具体化为一组软件库和工具，项目团队可以在其上构建其软件。它们作为标准化配置驱动、默认安全方法的起点。您可以通过在生命周期的早期选择一个特定的项目并让精通安全的工作人员与他们一起以通用方式构建安全功能来引导框架，以便可以从项目中提取该安全功能并在组织中的其他地方使用。

在有关架构、开发或运营的讨论背景下，持续监视组织中可用安全解决方案的弱点或缺陷。这是改善现有参考架构适用性和有效性的输入。

问题

您的设计是否基于可用的参考架构？

质量标准

您已记录了一个或多个已批准的参考架构，可供利益相关者使用；
您基于深刻理解和最佳实践不断改进参考架构；
您提供了一组组件、库和工具来实现每个参考架构。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

2.3.2 技术管理

2.3.2.1 成熟度等级 1

收益

对引入安全风险的技术公开透明。

活动

人们通常会在开发、部署、运营软件解决方案时采取最小阻力的方法。当新技术可以促进或加快工作速度或使解决方案能够更好地扩展时，通常会包括在内。但是，这些新技术可能会给您管理的组织带来新的风险。

确定每个应用软件使用的重要技术、框架、工具和集成的组件。安排有经验的架构师来研究开发和运营环境以及成果输出，然后评估它们的安全质量，并提出需要管理的重要发现。

问题

您是否评估开发所使用重要技术的安全质量？

质量标准

您有一个包含所有应用软件使用和支持最重要技术的列表；
您识别并跟踪技术风险；
您确保这些技术的风险符合组织基线。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

2.3.2.2 成熟度等级 2

收益

具有适当安全级别的技术可供产品团队使用。

活动

确定组织中各个软件项目中使用的常用技术、框架和工具，从而使您专注于捕获高级技术。

创建列表并将其作为推荐技术在整个开发组织中共享。选择它们时，请考虑历史事件、脆弱点跟踪记录、组织功能的适用性、使用过于复杂的第三方组件、组织内的足够知识。

由高级开发人员和架构师创建此列表，并包含管理人员和安全审核员的意见。与开发组织共享此推荐列表。最终，目标是为项目团队提供众所周知的默认信息。定期检查这些技术的安全性和适用性。

问题

您是否有一个针对该组织的推荐技术列表？

质量标准

该列表基于软件中使用的技术；
由首席架构师和开发人员审查并批准该列表；
您在整个组织中共享列表；
您至少每年检查和更新一次列表。

回答

没有；
是的，对于某些技术领域；
是的，至少有一半的技术领域；
是的，对于大多数或所有技术领域。

2.3.2.3 成熟度等级 3

收益

由于使用经过审查的技术导致攻击面有限。

活动

对于所有专有开发（包括：内部开发或购置），都要强加并监视标准化技术的使用。根据您的组织，可以通过事后对应用软件成果输出（如：源代码、配置文件或部署）进行自动分析，或者将这些限制集中到构建或部署工具中，或定期检查框架是否正确使用了这些限制。

与项目团队一起验证几个因素。确定使用非推荐技术，以确定建议与组织需求之间是否存在差距。检查未使用或使用不当的设计模式和参考平台模块，以确定是否需要更新。此外，随着组织的发展和项目团队的需要，在参考平台中实现功能。

问题

您是否在组织内强制使用推荐的技术？

质量标准

您定期监视应用软件，以判断是否正确使用了推荐的技术；
您可以根据组织政策解决针对列表的违规问题；
如果违规数量超出年度目标，则应采取措施。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

3、 开发

开发聚焦于与组织如何构建和部署软件组件及相关缺陷有关的过程和活动。

开发中的活动对开发人员日常工作影响最大。共同的目标是交付具有最少缺陷的、可靠的、可正常运行的软件。

3.1 安全构建

安全构建（SB）实践强调以标准化、可重复的方式构建软件以及使用安全组件（包括第三方软件依赖项）进行构建的重要性。

活动流 A 聚焦于在构建过程中尽可能完全使用自动化来消除任何可能的主观错误。自动化构建管道可以包括其他自动化安全检查手段，例如 SAST 和 DAST，以通过构建失败来获得进一步的安全保障并及早标记出安全性下降。

活动流 B 关注现代应用软件中软件依赖性的普遍性。它旨在识别软件依赖并跟踪其安全状态，以控制其不安全性对本身安全的应用软件的影响。在高级形式中，它对应用软件本身的软件依赖项执行类似的安全检查。

成熟度等级		活动流 A 安全构建	活动流 B 软件依赖
1 级	构建过程是可重复且持续的。	建立一个构建过程的正式定义，使其变得持续且可重复。	创建您应用软件的物料清单记录，并找机会进行分析。
2 级	优化了构建过程并将其完全集成到工作流中。	使您的构建管道自动化并确保使用的工具安全。在构建管道中添加安全检查。	评估使用过的依赖项，并确保对可能给应用软件带来风险的情况做出及时反应。
3 级	构建过程有助于防止已知缺陷进入生产环境。	在构建过程中定义强制性安全检查，并确保在构建不合规的工件时失败。	采用代码分析相同的方式，为安全问题分析使用的软件依赖。

3.1.1 构建过程

3.1.1.1 成熟度等级 1

收益

在构建过程中发生人为错误的风险有限，从而将安全问题降至最低。

活动

定义构建过程，将其分解为一组清晰的指令，然后由人员或自动工具执行。构建过程定义以端到端的方式描述了整个过程，以便人员或工具每次都能始终如一地遵循它并产生相同的结果。该定义集中存储，任何工具或人员都可以访问。避免存储多份副本，因为它们可能会变得缺乏统一性，且过时。

流程定义不包括任何秘密信息（特别考虑构建过程中所需的秘密信息）。

审查所有的构建工具，以确保其得到了供应商积极的维护，并使用了最新的安全补丁程序。强化每个工具的配置，使其与供应商指南和行业最佳实践保持一致。

为每个生成的工件确定一个值，例如签名或哈希值，该值可在以后用于验证其完整性。保护此值，如果保护了工件，则保护私有签名证书。

确保定期对构建工具打补丁和适当加固。

问题

您的完整构建过程得到正式描述了吗？

质量标准

您有足够的信息来重新创建构建过程；
您的构建文档是最新的；
您的构建文档存储在可访问的位置；
生成的工件校验和是在构建期间创建的，以支持以后的验证；
对构建过程中使用的工具进行加固。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

3.1.1.2 成熟度等级 2

收益

带有集成安全工具的高效构建过程。

活动

自动化构建过程，以便随时进行持续的构建。构建过程通常不需要任何干涉，从而进一步减少了人为错误的可能性。

自动化系统的使用增加了对构建工具的安全性的依赖，并使工具集的硬化和维护变得更加关键。要特别注意那些工具的界面，例如，基于 Web 的门户网站以及如何锁定它们。将构建工具暴露给网络可能会使恶意行为者篡改过程的完整性。例如，这可能允许将恶意代码内置到软件中。

自动化过程可能需要访问构建软件所需的凭据和秘密信息，例如，代码签名证书或对存储库的访问。需要小心处理。使用组织或业务部门的证书对生成的构件进行签名，以便您可以验证其完整性。

最后，在管道流程中添加适当的自动化安全检查工具（例如，SAST 工具），以利用自动化带来的安全利益。

问题

构建过程是否完全自动化？

质量标准

构建过程本身不需要任何人工干预
根据最佳实践和供应商指南对构建工具进行了强化
您可以加密构建工具所需的机密信息，并根据最小特权原则控制访问权限

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

3.1.1.3 成熟度等级 3

收益

确保您构建符合安全基线的软件。

活动

定义适合在构建过程中执行的安全检查，以及通过构建的最低标准。这些标准可能会根据各种应用软件的风险状况而有所不同。在构建中包括相应的安全检查，并在不满足预定义条件的情况下强制中断构建过程。触发低于阈值的问题的警告，并将其记录到集中式系统中以跟踪它们并采取措施。明智的话，如果已经接受或减轻了特定漏洞的风险，请实施异常机制来绕过此行为。但是，请确保首先明确批准这些案例，并记录其发生情况和理由。

如果技术方面的限制阻止了组织自动中断构建过程，则通过其他措施（如，明确的政策和定期审核）确保相同的效果。

在单独的集中式服务器上处理代码签名，该服务器不会将证书暴露给执行构建的系统。在可能的情况下，使用确定性方法输出逐个字节的可复制工件。

问题

您是否在构建过程中执行了自动安全检查？

质量标准

如果应用软件不符合预定义的安全基线，则构建失败；
您对脆弱点具有最高危的可接受程度；
您在集中式系统中记录警告和故障信息；
您选择并配置工具，以至少每年一次的方式对每个应用软件的安全需求进行评估。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

3.1.2 软件依赖

3.1.2.1 成熟度等级 1

收益

有关依赖项中已知安全问题的可用信息。

活动

记录整个目标生产环境中使用的所有依赖项。有时称其为物料清单（BOM）。考虑到应用软件的不同组件可能使用完全不同的依赖关系。例如，如果软件包是 Web 应用软件，则涵盖服务器端应用软件代码和客户端脚本。在构建这些记录时，请考虑可以指定依赖项的各个位置，例如，配置文件、磁盘上的项目目录、程序包管理工具或实际代码（例如，通过支持列出依赖项的 IDE）。

收集有关每个依赖项的以下信息：

- 使用或引用的地方；
- 使用的版本；
- 软件授权许可；
- 源信息（链接到资源库、作者姓名等）；
- 依赖项的支持和维护状态；

检查记录以发现具有已知漏洞的任何依赖项，并相应地更新或替换它们。

问题

您对所依赖的依赖项有扎实的知识吗？

质量标准

您有每个应用软件当前的物料清单（BOM）；
您可以快速找出哪些应用受特定 CVE 的影响；
在过去的三个月中，您至少分析、解决并记录了依赖项的发现情况。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

3.1.2.2 成熟度等级 2

收益

依赖项中已知的安全问题完全公开透明。

活动

评估已使用的依赖关系，并根据一组定义的标准建立和批准在项目、团队、组织中使用的可接受依赖关系列表。

引入一个可以从中构建所有软件依赖关系的中央存储库。

定期检查使用的依赖项，以确保：

- 它们保持正确的许可信息；
- 不存在影响您应用软件的已知漏洞和重大漏洞；
- 依赖关系仍然得到积极的支持和维护；
- 您正在使用当前最新主流版本；
- 有正当理由要包含依赖项。

通过将不合格品视为缺陷，及时、适当地应对不合格品。考虑使用自动化工具扫描易受攻击的依赖项，并将识别出的问题分配给各个开发团队。

问题

您是否通过正式程序处理第三者依赖风险？

质量标准

您保留符合预定义条件的已批准依赖项列表；
您可以自动评估新 CVE 的依赖关系并提醒负责人员；
您会自动检测许可证更改并发出警报，这可能会影响合法应用软件的使用；
您跟踪并提醒有关未维护依赖项的使用情况；
您可以可靠地检测并删除软件中不必要的依赖项。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

3.1.2.3 成熟度等级 3

收益

采用代码分析相同的方式，为安全问题分析使用的软件依赖。

活动

维护批准依赖项和版本的白名单，并确保在依赖项不在列表中时，构建过程失败。如果明智的话，需包括一个签发流程来处理此规则的例外情况。

以与目标应用软件本身类似的方式（尤其是使用 SAST 和分析可传递依赖关系）对白名单上的依赖关系执行安全验证活动。确保这些检查还旨在确定依赖项中可能存在的后门或其他未知安全缺陷。与依赖项的作者或开发者建立漏洞披露流程（包括用于解决问题的 SLA）。如果强制执行 SLA 不切实际（如，带有开源漏洞），确保可以预见的最可能情况，并且您能够及时实施补偿措施。对已发现问题的修复程序执行回归测试。

使用缺陷跟踪系统跟踪所有已识别的问题及其状态。将构建管道与此系统集成，以便在所包含的依赖项包含超出定义的关键性级别的问题时使构建失败。

问题

如果软件构建受依赖关系漏洞的影响，您是否会阻止软件构建？

质量标准

您的构建系统已连接至用于跟踪第三方依赖风险的系统，除非导致漏洞被评估为误报或明确接受了风险，否则将导致构建失败；
您使用静态分析工具扫描依赖关系；
您使用已建立负责任的披露流程将发现报告给依赖项作者；
使用未评估安全风险的新依赖项会导致构建失败。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

3.2 安全部署

交付安全软件的最后阶段之一是确保在部署过程中不损害已开发应用软件的安全性和完整性，安全部署（SD）实践就聚焦于此。为此，该实践的第一个活动流侧重于通过尽可能自动执行部署过程来消除人为错误，并使其成功取决于集成安全性验证检查的结果。它还使受过适当培训的非开发人员负责部署，从而促进职责分离。

第二活动流超出了部署机制，重点是保护应用软件在生产环境中运行所需敏感数据（如：密码、令牌和其他机密）和隐私数据的完整性。以最简单的形式，将合适的生产环境机密信息从存储库和配置文件移入经过恰当管理的数字保管库。在更高级的形式中，机密信息是在部署时动态生成的，并且常规过程可以检测并减轻环境中任何未受保护的机密信息存在。

成熟度等级		活动流 A 部署流程	活动流 B 机密信息管理
1 级	部署过程已完整记录。	正式制定部署流程并保护使用的工具和流程。	引入基本保护措施以限制对生产环境中机密信息的访问。
2 级	部署过程包含安全验证里程碑。	在所有阶段自动化部署过程，并引入明显的安全验证测试。	在部署过程中，从加固的存储中动态注入秘密，并审计所有对其的人工访问。
3 级	部署过程是完全自动化的，并结合了所有关键里程碑的自动化验证。	自动验证所有已部署软件的完整性，无论是内部开发还是外部开发。	通过定期生成并确保正确使用，来改进应用软件机密信息的生命周期。

3.2.1 部署过程

3.2.1.1 成熟度等级 1

收益

在部署过程中发生人为错误的风险有限，可最大程度地减少安全问题。

活动

在所有阶段定义部署过程，将其分解为一组清晰的说明，以供人员或自动工具遵循。部署过程定义应端到端描述整个过程，以便每次可以始终遵循该过程以产生相同的结果。该定义集中存储，所有相关人员均可访问。请勿存储或分发多份副本，因为其中某些副本可能应缺乏统一维护而过时。

使用自动化过程或由开发人员以外的人员手动将应用软件部署到生产中。确保开发人员不需要直接访问生产环境即可进行应用软件部署。

查看所有部署工具，以确保它们由供应商积极维护并提供最新的安全补丁。强化每个工具的配置，使其与供应商指南和行业最佳实践保持一致。鉴于大多数这些工具都需要访问生产环境，因此其安全性至关重要。确保工具本身及其遵循工作流程的完整性，并根据最小特权原则配置对这些工具的访问规则。

让具有生产环境访问权限的人员至少通过最低程度的培训或认证，以确保他们在此方面的能力。

问题

您是否使用可重复的部署过程？

质量标准

您有足够的信息来运行部署过程；
您的部署文档是最新的；
相关利益相关者可以访问您的部署文档；
您确保只有定义合格的人员才能触发部署；
您可以对部署过程中使用的工具进行加固。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

3.2.1.2 成熟度等级 2

收益

通过集成安全工具形成高效的部署过程。

活动

将部署过程自动化以涵盖各个阶段，因此不需要手动配置步骤，并且消除了孤立的人为错误风险。确保并验证部署在所有阶段都是一致的。

在部署过程中集成自动安全检查，例如，使用动态分析安全测试（DAST）和漏洞扫描工具。另外，在适当的地方验证已部署工作输出件的完整性。集中记录这些测试的结果，并采取任何必要的措施。如果发现任何缺陷，请确保自动通知相关人员。如果发现任何超出预定义关键程度的问题，请自动停止或撤消部署，或者引入单独的手动批准工作流程，以便记录此决策，其中包含对异常的解释。

解释并审核所有部署的所有阶段。有一个适当的系统来记录每个部署，包括：有关执行该部署的人员、部署的软件版本以及特定于部署的任何相关变量信息。

问题

部署过程是否自动化并采用安全检查？

质量标准

部署过程在所有阶段都是自动化的；
部署包括了自动化安全测试程序；
您提醒相关负责人员注意已发现的漏洞；
您在定义的时间内有可用于过去部署的日志。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

3.2.1.3 成熟度等级 3

收益

确保部署到生产环境中软件部件的完整性。

活动

利用在构建时进行签名的二进制文件，并通过对照受信任的证书检查签名来自动验证正在部署软件的完整性。这可能包括内部开发和构建的二进制文件以及第三方软件。如果无法验证其签名，包括那些带有无效或过期证书的签名，请不要部署它们。

如果受信任的证书列表中包含第三方开发人员，请定期检查它们，并使它们与组织治理范围的受信任第三方供应商保持一致。

在自动部署期间，至少要手动批准一次部署。在部署过程中，只要人工检查比自动检查准确得多，就选择此选项。

问题

您是否持续验证已部署软件部件的完整性？

质量标准

如果检测到完整性问题，则阻止或回退部署；
针对在构建期间所创建签名的验证工作已经完成；
如果无法检查签名（如，外部构建软件），则采取补偿措施。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

3.2.2 机密信息管理

3.2.2.1 成熟度等级 1

收益

定义和限制地访问生产环境的机密信息。

活动

开发人员不应访问生产环境的机密或凭据。拥有适当的机制保护生产环境中机密信息，例如：1、通过让特定人员在部署时将它们添加到相关的配置文件中（职责分离原则）；2、对配置文件中包含的生产环境机密信息进行加密。

不要在开发或测试环境的配置文件中使用生产环境机密信息，因为这样的环境可能会大大降低安全性。同样，请勿在代码存储库中存储的配置文件中使机密信息不受保护。

始终使用静态加密存储生产系统的敏感凭据和机密信息。考虑为此使用专用工具。认真处理密钥管理，以便只有负责生产部署的人员才能访问此数据。

问题

您是否按照最小特权原则限制对应用软件机密信息的访问？

质量标准

您将生产环境机密信息存储在安全的位置；
开发人员无法访问生产环境机密信息；
生产环境机密信息在非生产环境中不可用。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

3.2.2.2 成熟度等级 2

收益

检测生产环境机密信息的潜在泄漏。

活动

有一个自动化过程，可以在部署过程中各个阶段将凭据和机密信息添加到配置文件中。这样，开发人员和部署人员不会看到或处理这些敏感信息。

实施检查以检测代码存储库和文件中机密信息的存在，并定期运行它们。配置工具以查找已知字符串和未知高熵字符串。在有历史记录的系统（如，代码存储库）中，请在检查中包括版本。将发现的潜在机密标记为敏感值，并在适当的位置将其删除。例如，如果无法从代码存储库中的历史文件中删除它们，则可能需要刷新使用该机密信息在系统上的值。这样，如果攻击者发现了它们，也将对攻击者没有用。

从安全的角度来看，使用于存储和处理机密和凭据的系统更健壮。对静态和传输中的所有机密进行加密。配置此系统及其包含的机密的用户应遵循最小特权原则。例如，开发人员可能需要管理开发环境的机密，而不是用户验收测试或生产环境的机密。

问题

您是否在部署期间将生产环境机密信息注入到配置文件中？

质量标准

源代码文件不再包含使用的应用软件机密信息；
在正常情况下，部署过程中不会有人访问机密信息；
您记录并警告任何对机密信息的异常访问。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

3.2.2.3 成熟度等级 3

收益

最小化生产环境机密信息滥用的可能性，并及时发现滥用。

活动

对生产环境机密信息实施生命周期管理，并确保针对每个应用软件实例尽可能多地生成新机密。每个应用软件实例使用机密信息可确保可以追溯并正确分析意外的应用软件行为。工具可以在发生变更时，自动的、无缝的在所有相关位置更新机密信息。

确保所有对机密信息的访问（包括读写）都记录在中央基础架构中。定期查看这些日志以识别意外行为，并进行适当的分析以了解发生这种情况的原因。将问题和根本原因输入缺陷管理实践中，以确保组织能够解决任何不可接受的情况。

问题

您是否对应用软件机密信息实施了适当的生命周期管理？

质量标准

您可以使用经过审查的解决方案生成和同步机密信息；
不同的应用软件实例之间的机密信息是不同的；
机密信息会定期更新。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

3.3 缺陷管理

缺陷管理（DM）实践聚焦于收集、记录和分析软件安全缺陷，并用信息丰富它们，以驱动基于测量的决策。

该实践的第一个活动流是处理和管理缺陷的过程，以确保发布的软件具有给定的保障级别。第二个活动流集中于丰富有关缺陷的信息和派生指标，以指导有关项目和整个安全保障计划的安全性决策。

以一种复杂的形式，该实践需要正规的，独立的缺陷管理和实时，相关的信息，以检测趋势并影响安全策略。

成熟度等级		活动流 A 缺陷跟踪	活动流 B 指标和反馈
1 级	在每个项目中跟踪所有缺陷。	引入对安全缺陷的结构化跟踪，并基于此信息做出明智的决策。	定期检查以前记录的安全缺陷，并通过基本指标快速制胜。
2 级	缺陷跟踪用于影响部署过程。	对整个组织中的所有安全缺陷进行持续评估，并为特定的严重性等级定义 SLA。	收集标准化的缺陷管理指标，并将其用于集中驱动计划的优先级。
3 级	跨多个组件进行缺陷跟踪以帮助减少新缺陷的数量。	实施预定义的 SLA，并将缺陷管理系统与其他相关工具集成。	持续改进您的安全缺陷管理指标，并将其与其他来源相关联。

3.3.1 缺陷跟踪

3.3.1.1 成熟度等级 1

收益

影响特定应用软件的已知安全缺陷公开透明。

活动

引入对安全缺陷的通用定义和理解，并定义识别这些缺陷的最常用方法。这些通常包括但不限于：

- 威胁评估
- 渗透测试
- 静态和动态分析扫描工具的输出
- 负责任的披露程序或漏洞赏金

建立透明的文化，避免责怪任何团队引入或识别安全缺陷。在定义的位置记录和跟踪所有安全缺陷。该位置不一定要集中到整个组织，但是要确保您能够在任何时间点获得影响特定应用软件所有缺陷的概述。为跟踪的安全缺陷定义和应用访问规则，以减轻泄漏和滥用此信息的风险。

至少对安全缺陷进行基本的定性分类，以便您能够相应地优先确定修复工作。努力限制信息的重复和误报的出现，以提高流程的可信赖性。

问题

您是否在可访问的位置跟踪所有已知的安全缺陷？

质量标准

您可以轻松获得影响一个应用软件的所有安全缺陷的概述；
您至少有一个基本的分类方案；
该过程包括处理误报和重复条目的策略；
缺陷管理系统涵盖了来自不同来源和实践的缺陷。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

3.3.1.2 成熟度等级 2

收益

对安全缺陷进行一致的分类，并对它们的处理有明确的期望。

活动

根据被利用缺陷的可能性和预期影响，为整个组织引入并应用一套明确定义的安全缺陷评估方法。这将使您能够确定需要更多关注和投资的应用软件。万一您没有集中存储有关安全缺陷的信息，请确保您仍然能够轻松地从所有来源获取信息，并获得有关“热点”的概述，并需要引起您的注意。

引入 SLA 以便根据其严重性等级及时修复安全缺陷，并集中监视和定期报告 SLA 违规情况。针对在 SLA 定义时间内不能修复缺陷或需以高昂代价修复缺陷的情况，定义相关流程。这至少应确保所有利益相关者对所施加的风险有扎实的了解。如果合适，对这些情况采用补偿控制。

即使您没有用于修复低危缺陷的正式 SLA，也要确保负责的团队仍能定期获得有关影响其应用软件问题的概述，并了解特定问题如何相互影响或相互放大。

问题

您是否对整个组织的安全缺陷状态进行了概述？

质量标准

单一严重性方案适用于组织中的所有缺陷；
该方案包括用于修复特定严重等级的 SLA；
您定期报告 SLA 的遵守情况。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

3.3.1.3 成熟度等级 3

收益

确保在预定义的 SLA 中处理安全缺陷。

活动

如果修复时间违反了定义的 SLA，则对安全缺陷实施自动报警。确保将这些缺陷自动转移到风险管理流程中，并通过一致的定量方法进行评估。不仅在独立团队的层面上，而且在整个组织的层面上，评估特定缺陷如何相互影响/扩大。利用完整杀伤链的知识来确定优先级，引入和跟踪补偿控制，以减轻各自的业务风险。

将缺陷管理系统与其他实践引入的自动化工具集成在一起，例如：

- 构建和部署：除非高于特定严重性的安全缺陷影响最终工件，否则构建/部署过程将失败，除非有人明确签署了例外。
- 监视：如果可能，请确保识别并警告生产环境中安全缺陷的滥用。

问题

您是否执行 SLA 来修复安全缺陷？

质量标准

您会自动发出有关 SLA 违规的告警，并将相应的缺陷转移到风险管理流程中；
您将相关工具（例如，监视、构建、部署）与缺陷管理系统集成在一起。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

3.3.2 指标与反馈

3.3.2.1 成熟度等级 1

收益

从可用的缺陷信息中识别出能够快速制胜的信息。

活动

在每个定义的时间段内遍历一次每个团队中已解决的和仍未解决的安全缺陷记录，并从可用数据中提取基本指标。通常，至少每年执行一次。这些指标可能包括：

- 缺陷总数与验证活动总数的对比。这可以使您了解缺陷的密度和质量情况；
- 缺陷所在的软件组件。这表示可能最需要注意的地方，以及将来可能再次出现安全缺陷的地方；
- 缺陷的类型或类别，表明开发团队需要进一步培训的领域；
- 缺陷的严重性，可以帮助团队了解软件的风险。

识别并开展明智的活动，您可以从新获得的知识中汲取教训。这些可能包括诸如关于一种特定漏洞类型的知识共享会话或执行/自动化安全扫描之类的事情。

问题

您是否使用有关已记录安全缺陷的基本指标，来进行快速制胜的改进活动？

质量标准

您去年至少分析了一次记录的指标；
至少记录并提供了有关该计划的基本信息；
您已根据数据确定并进行了至少一项快速制胜活动。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

3.3.2.2 成熟度等级 2

收益

改善对组织中安全缺陷的学习。

活动

定义、收集和计算整个组织的统一指标。这些可能包括：

- 验证活动和已识别缺陷的总数；
- 已识别缺陷的类型和严重程度；
- 发现缺陷的时间和解决缺陷的时间；
- 对实时系统上存在缺陷暴露的时间窗口期；
- 漏洞的回归或重新开放的数量；
- 特定软件组件的验证活动范围；
- 可接受的风险值；
- 由于未知或未记录的安全缺陷而导致的安全事件比率。

为合适的受众定期生成报告（如，月报）。通常，这将覆盖诸如经理、安全官和工程师之类的受众。将报告中的信息用作安全策略的输入，例如，改进培训或安全验证活动。

修复安全缺陷后，例如在定期的知识共享会议上，与其他团队分享有关安全缺陷的最突出或最有趣的技术细节，包括修复策略。这将有助于将学习效果从缺陷扩展到整个组织，并限制将来发生的缺陷。

问题

您是否根据标准化指标改进了安全保障计划？

质量标准

您为缺陷的分类和活动流记录了指标，并保持指标最新；
执行管理层定期接收有关缺陷的信息，并在去年采取了措施；
您定期在团队之间共享有关安全缺陷的技术详细信息。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

3.3.2.3 成熟度等级 3

收益

基于缺陷信息的优化安全策略。

活动

定期（每年至少一次）重新访问您正在收集的缺陷管理指标，并比较收集和跟踪这些指标所需的工作量与预期结果。做出明智的决策，以删除那些无法提供整体预期价值的指标。尽可能包括并自动执行针对收集数据质量的验证活动，并确保在发现任何差异的情况下进行持续改进。

将数据与威胁情报和事件管理指标进行汇总，并将结果用作整个组织中其他计划的输入，例如：

- 规划各种人员的安全培训；
- 针对内部和外部开发收集的安全验证活动进行改进；
- 供应链管理，例如对合作伙伴组织进行安全审核；
- 对基础架构和应用软件的攻击进行监视；
- 对安全基础架构或补偿性控制进行投资；
- 为您的安全团队配备人员并设置安全预算。

问题

您是否定期评估安全指标的有效性，以便其输入有助于推动安全策略的信息？

质量标准

您去年至少分析过一次安全指标的效果；
在可能的情况下，您将自动验证数据的正确性；
指标与其他信息来源（如，威胁情报、事件管理）汇总；
您从去年的指标中衍生出至少一项战略活动。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

4、 验证

验证的重点是有关于组织如何检查和测试整个软件开发过程中产生成果输出的过程和活动。这通常包括质量保证工作，例如测试，但也可包括其他审核和评估活动。

4.1 架构评估

架构评估（AA）实践的可确保应用软件和基础架构充分满足所有相关的安全性和合规要求，并充分缓解已识别的安全威胁。第一个活动流针对系统中的每个接口，侧重于先临时性、再系统化的方式，验证是否满足“策略与合规”和“安全需要”实践中确定的安全性和合规要求。第二个活动流审查架构，首先是针对典型威胁的缓解措施，然后针对威胁评估实践中确定的特定威胁进行缓解。

该实践以更高级的形式使安全架构审查过程正式化，不断评估架构安全控件的有效性、可伸缩性和策略一致性。识别出的弱点和可能的改进将反馈给安全架构实践，以改进参考架构。

成熟度等级		活动流 A 架构验证	活动流 B 架构缓解
1 级	审核架构，以确保针对典型风险的基线缓解措施已到位。	识别应用软件和基础架构组件，并检查基本的安全配置情况。	对架构进行临时审查，以缓解安全隐患。
2 级	审查架构中安全机制的完整配置情况。	验证架构的安全机制。	分析架构中已知的威胁。
3 级	审查架构有效性和反馈结果以改进安全架构。	审查架构组件的有效性	将架构审查的结果反馈到企业架构、组织设计原则和模式、安全解决方案和参考架构中。

4.1.1 架构验证

4.1.1.1 成熟度等级 1

收益

对概要架构和合理安全措施的了解。

活动

创建总体架构视图，并检查其是否正确提供了常规安全机制，例如身份验证、授权、用户和权限管理、安全通信、数据保护、密钥管理和日志管理。同时考虑对隐私的支持。基于项目成果输出（例如架构或设计文档）或与企业主和技术人员的访谈来执行此操作。还应考虑基础架构组件。基础架构组件不是特定于应用软件的系统、组件和库（包括 SDK），而是为组织中使用或管理应用软件提供直接支持。

注意架构中与安全性相关的所有功能，并查看其正确配置。从匿名用户、授权用户和特定应用软件角色的角度出发，以临时方式执行此操作。

问题

您是否临时审查应用软件架构中的关键安全目标？

质量标准

您已经就整体软件架构达成了共识模型；
您将组件、接口和集成的组件包括在架构模型中；
您验证常规安全机制的正确提供情况；
您将缺失的安全控件记录为缺陷。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

4.1.1.2 成熟度等级 2

收益

整个组织内持续的架构审核过程。

活动

验证解决方案架构是否满足所有已确定的安全性和合规要求。对于应用软件中的每个接口，请遍历安全性和合规要求列表，并分析其提供的架构。并且，执行交互或数据流分析，以确保在不同组件上充分满足需求。详细分析以显示满足每个需求的设计级功能。

在两个内部接口（例如，层之间）以及外部接口（例如，构成攻击面的外部接口）上执行此类分析。还应确定并验证作为架构一部分做出的重要设计决策，尤其是当它们偏离组织中可用的共享安全解决方案时。最后，根据开发周期中所做的变更更新发现，并注意在设计中未明确提供的要求，将这些要求作为评估发现的结果。

问题

您是否定期审查架构的安全机制？

质量标准

您审查对内部和外部要求的合规情况；
您系统地审查系统中的每个接口；
您使用正式的审查方法和结构化验证；
您将缺失的安全机制记录为缺陷。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

4.1.1.3 成熟度等级 3

收益

确保架构控制的有效性。

活动

根据组织的整体策略，审查架构组件及其提供安全机制的有效性，并仔细检查所选安全解决方案的可用性、可伸缩性和企业就绪程度。尽管针对特定应用的战术选择在特定情况下是有意义的，但重要的是要保持全局，并确保所设计解决方案在将来可以使用。

将所有发现反馈到缺陷管理中，以触发对该架构的进一步改进。

问题

您是否定期审查安全控制的有效性？

质量标准

您评估安全控件的预防能力、检测能力和响应能力；
您评估安全控制的策略一致性、支持恰当性以及可伸缩性；
您至少每年评估一次效果；
您将识别的缺点记录为缺陷。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

4.1.2 架构缓解

4.1.2.1 成熟度等级 1

收益

确保该架构可以防御典型的安全威胁。

活动

查看架构以了解典型的安全威胁。精通安全的技术人员根将来自架构师、开发人员、经理和业务所有者的输入作为需要进行分析，以确保架构解决所有常见的威胁，而缺乏专业安全知识的开发团队可能会忽略这些常见的威胁。

架构中的典型威胁可能与对安全机制（例如身份验证、授权、用户和权限管理、安全通信、数据保护、密钥管理和日志管理）的错误假设或过度依赖有关。另一方面，威胁也可能与技术组件或框架的已知限制或问题有关，这些问题或解决方案是解决方案的一部分，而缓解措施不足。

问题

您是否会临时审查应用软件架构以缓解典型威胁？

质量标准

您已经就整体软件架构达成了共识模型；
由精通安全的人员进行审查；
您考虑各种类型的威胁，包括内部威胁和与数据相关的威胁。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

4.1.2.2 成熟度等级 2

收益

所有识别出对该应用软件的威胁均得到了妥善处理。

活动

系统地审查“威胁评估”活动中发现的每个威胁，并检查架构如何缓解它们。使用标准化的过程来分析系统架构及其中的数据流。通常将其链接到所使用的威胁模型（例如 STRIDE），以便识别解决每种威胁类型的相关安全目标。对于每种威胁，确定架构中设计层级的对应功能并评估其有效性。

在可用的地方，查看架构决策记录，以了解架构约束和设计过程中的权衡。将其影响以及系统安全操作所依赖的任何安全性假设都考虑在内，并对其进行重新评估。

丰富您先前创建的威胁模型，以使每个威胁及其估计的影响都与相应的对策相关联。生成映射文件或专用工具中的仪表板，以使相关利益相关者可以使用和看到信息。

问题

您是否定期评估对架构的威胁？

质量标准

您系统地审查了威胁评估中确定的每个威胁；
由受过训练或有经验的人审查实践情况；
您可每种已识别的威胁确定设计级别的缓解功能；
您将未处理的威胁记录为缺陷

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

4.1.2.3 成熟度等级 3

收益

基于架构审查的企业架构持续改进。

活动

作为一个组织，您可以通过了解软件架构中哪些威胁仍未解决，并调整策略来防止这种威胁，从而进一步改善软件安全状况。正式制定流程，并将在架构中反复出现的威胁作为触发点，以识别安全评估漏洞的原因并加以解决。通过创建或更新相关的参考架构、现有的安全解决方案或组织设计原则和模式，将发现的威胁反馈到设计阶段。

问题

您是否根据架构评估结果定期更新参考架构？

质量标准

您以标准化的书面形式评估架构；
您使用重复发现的威胁来触发对参考架构的审查；
您可以临时、独立审查架构评估的质量；
您以参考架构更新触发点，以基于风险的方式对相关共享解决方案进行审查。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

4.2 需求驱动的测试

需求驱动测试（RT）实践的目标是确保已实施的安全控制按预期运行，并满足项目规定的安全需求。它通过逐步构建一组安全测试和回归案例并定期执行来实现。

这种做法的一个关键方面是它同时关注正面和负面的测试。前者将验证应用软件的安全控件是否满足规定的安全需求，并验证其正确功能。这些要求通常本质上是功能性的。负面测试解决了安全控制实施的质量问题，旨在通过误用和滥用测试来检测意外的设计缺陷和实施错误。该实践以更高级的形式促进安全压力测试（例如，拒绝服务），并通过始终如一地自动化安全性单元测试并为所有已识别和修复的错误创建安全性回归测试，努力不断提高应用软件的安全性。

尽管需求驱动测试和安全测试实践都与安全测试有关，但前者着重于验证安全需求的正确实现，而后者则旨在发现应用软件中的技术实现弱点，而与需求无关。

成熟度等级		活动流 A 控制验证	活动流 B 误用/滥用测试
1 级	机会性地发现基本漏洞和其他安全问题。	测试软件的安全控制。	执行安全模糊测试。
2 级	执行实施审查，针对安全需求，发现特定于应用软件的风险。	根据已知的安全需求派生测试用例。	创建并测试滥用案例和业务逻辑缺陷测试。
3 级	在错误修复，更改或维护期间，维持应用软件的安全级别。	执行回归测试（使用安全单元测试）。	拒绝服务和安全压力测试。

4.2.1 控制验证

4.2.1.1 成熟度等级 1

收益

验证标准安全控制的有效性

活动

进行安全性测试，以验证标准软件安全性控件是否按预期运行。从高层次上讲，这意味着测试数据以及服务的机密性，完整性和可用性控制的正确功能。安全测试至少包括身份验证，访问控制，输入验证，编码以及数据和加密控制转义的测试。测试目标是验证安全控制措施是否正确实施。

安全测试将验证相关的软件安全控制。每次应用软件更改其控件使用方式时，请手动或使用工具执行控件验证安全性测试。当功能经过充分验证时，可以使用诸如功能切换和 A / B 测试之类的技术逐步向更广泛的受众展示功能。对于 SAMM 程序中的所有软件，必须进行软件控制验证。

题

您是否测试应用软件的标准安全控制功能是否正常？

质量标准

安全测试至少要验证身份验证，访问控制，输入验证，数据编码和转义以及加密控制的实现

每当应用软件更改其控件的使用时，都会执行安全性测试

回答

没有

是的，其中一些

是的，至少有一半

是的，大多数或全部

4.2.1.2 成熟度等级 2

收益

将安全需求集成到测试方案中

活动

根据安全需求，确定并实施一组安全测试用例，以检查软件的正确功能。要拥有成功的测试程序，您必须了解安全需求所指定的测试目标。

从作为“安全需求” SAMM 安全实践的一部分而创建的安全需求中派生适用于应用软件的安全测试用例。为了通过安全测试验证安全需求，安全需求是功能驱动的，并突出显示了预期的功能（功能是什么）以及隐含的实现方式（方法）。这些要求也称为“肯定要求”，因为它们规定了可以通过安全测试验证的预期功能。积极要求的示例包括“在六次失败的登录尝试后，应用软件将锁定用户”或“密码至少应为六个字母数字字符”。肯定需求的确认包括声明预期的功能。您可以重新创建测试条件并根据预定义的输入运行测试。将结果显示为失败或通过条件。

通常，最有效的方法是利用项目团队的时间来构建特定于应用软件的测试用例，并使用可公开获得的资源或购买的知识库来选择适用的通用测试用例以提高安全性。相关的开发，安全和质量保证人员检查候选测试用例的适用性，有效性和可行性。在功能的需求和/或设计阶段派生测试用例。测试安全需求是软件功能测试的一部分。

题

您是否始终如一地编写和执行测试脚本以验证安全需求的功能？

质量标准

您可以针对每个应用软件量身定制测试并声明预期的安全功能

您将测试结果捕获为通过或失败条件

测试使用标准化框架或 DSL

回答

没有

是的，其中一些

是的，至少有一半

是的，大多数或全部

4.2.1.3 成熟度等级 3

收益

及时，可靠地发现违反安全需求的情况

活动

为所有已识别（和已修复）的错误编写并自动执行回归测试，以确保它们成为测试工具，以防止在以后的发行版中引入类似的问题。安全单元测试应动态（即在运行时）验证组件是否按预期运行，并应验证是否正确实施了代码更改。

对于开发人员而言，一个好的实践是将安全测试用例构建为通用安全测试套件，这是现有单元测试框架的一部分。通用安全测试套件可能包括安全测试用例，以验证对安全控制（例如身份，身份验证和访问控制，输入验证和编码，用户和会话管理，错误和异常处理，加密以及审计和日志记录）的肯定和否定要求。尽早验证安全测试的正确执行。例如，如果可行，在允许新代码进入主代码库之前，将通过安全性测试作为合并要求的一部分。或者，考虑他们通过了验证构建的要求。

对于安全功能测试，请对软件组件级别的安全控件的功能（例如功能，方法或类）使用单元级别的测试。例如，测试用例可以通过断言组件的预期功能来检查输入和输出验证（例如，变量卫生）以及对变量进行边界检查。

题

您是否自动测试应用软件的安全性退化？

质量标准

您始终为所有已识别的错误编写测试（可能超过了预先定义的严重性阈值）

您在作为现有单元测试框架一部分的测试套件中收集安全测试

回答

没有

是的，对于某些应用

是的，对于至少一半的应用软件

是的，对于大多数或所有应用软件

4.2.2 滥用测试

4.2.2.1 成熟度等级 1

收益

在处理意外输入时洞察应用软件的行为

活动

执行模糊测试，向测试对象发送随机或格式错误的数据，以使其崩溃。模糊测试或模糊测试是一种黑盒软件测试技术，包括使用自动格式错误或半格式数据注入来查找实现错误。针对应用软件的主要输入参数，至少覆盖漏洞的最小模糊测试。

模糊测试的优势在于测试设计的简单性，以及对系统行为缺乏先入之见。随机方法会导致人眼或结构化测试经常遗漏的错误。它也是评估封闭系统（例如 SIP 电话）质量的几种方法之一。对目标进行模糊测试的简单性被准确检测和分类崩溃的难度所抵消。支持现有的模糊测试工具和框架以利用其支持工具。

题

您是否使用随机化或模糊测试技术来测试应用软件？

质量标准

测试涵盖了应用软件的大部分或全部主要输入参数

您会尽力记录并检查所有应用软件崩溃对安全性的影响

回答

没有

是的，对于某些应用

是的，对于至少一半的应用软件

是的，对于大多数或所有应用软件

4.2.2.2 成熟度等级 2

收益

检测应用软件业务逻辑缺陷

活动

滥用和滥用案例描述了应用软件的意外使用和恶意使用情况，并描述了攻击者如何执行此操作。创建滥用案例，以滥用或利用软件功能控件的弱点来攻击应用软件。对应用软件使用滥用案例模型，可以充当识别直接或间接利用滥用场景的具体安全测试的动力。

功能的滥用（有时称为“业务逻辑攻击”）取决于应用软件功能和特性的设计和实现。一个示例是使用密码重置流程来枚举帐户。作为业务逻辑测试的一部分，请确定对应用软件重要的业务规则，并将其转变为实验，以验证应用软件是否正确执行了业务规则。例如，在股票交易应用软件上，是否允许攻击者在一天之初开始交易并锁定价格，将交易保持到一天结束，然后在股票价格上涨时完成交易还是取消价格下跌？

题

您是否根据功能需求创建滥用案例并使用它们来进行安全性测试？

质量标准

重要业务功能有相应的滥用案例

您以明确的动机和特征围绕相关角色构建虐待故事

您将已识别的弱点捕获为安全需求

回答

没有

是的，有时候

是的，至少有一半的时间

是的，大部分或所有时间

4.2.2.3 成熟度等级 3

收益

抵御拒绝服务攻击的弹性透明

活动

应用软件特别容易遭到拒绝服务攻击。在受控条件下（最好在应用软件接受环境中）对它们执行拒绝服务和安全压力测试。

负载测试工具会生成综合流量，使您可以在重负载下测试应用软件的性能。一个重要的测试是应用软件每秒可以处理多少个请求，同时又保持其性能要求。从单个 IP 地址进行测试仍然很有用，因为它可以表明攻击者必须生成多少请求才能影响应用软件。

拒绝服务攻击通常会导致应用软件资源匮乏或耗尽。要确定是否可以使用任何资源来创建拒绝服务，请分析每个应用软件资源以了解如何耗尽资源。优先处理未经身份验证的用户可以执行的操作。使用安全压力测试来补充整体拒绝服务测试，以执行操作或创建导致被测应用软件延迟，中断或失败的条件。

题

您是否执行拒绝服务和安全压力测试？

质量标准

压力测试针对特定的应用软件资源（例如，通过将大量数据保存到用户会话中来耗尽内存）

您可以使用定义明确的功能（知识，资源）围绕相关角色设计测试

您将结果反馈给设计实践

回答

没有

是的，有时候

是的，至少有一半的时间

是的，大部分或所有时间

4.3 安全测试

安全测试（ST）实践利用了以下事实：尽管自动化安全测试快速且可以很好地扩展到众多应用软件，但是有关应用软件及其业务逻辑深入知识的深度测试通常只能通过较慢的人工专家安全测试来执行。因此，每个活动流的核心都是一种方法。

第一个活动流侧重于建立通用的安全基线，以自动检测容易实现的目标。逐步为每个应用软件定制自动化测试，并提高其执行频率，以尽早发现更多的错误和回归。自动化流程可以检测到的错误越多，专家就必须花费更多的时间来利用他们的知识和创造力来专注于更复杂的攻击媒介，并确保在第二个活动流中进行深入的应用软件测试。由于手动审核缓慢且难以测量，因此审核人员会根据其风险、最近的相关变更或即将发布的主要版本来确定测试组件的优先级。例如，组织还可以通过参与漏洞赏金计划来获取外部专业知识。

与以需求为导向的测试实践（其侧重于验证应用软件是否正确满足需求）不同，此实践的目标是发现应用软件中的技术和业务逻辑弱点，并使它们对于管理和业务涉众可见，而与需求无关。

成熟度等级		活动流 A 可测量的基线	活动流 B 深入理解
1 级	执行安全测试（包括人工的和基于工具的）以发现安全缺陷。	利用自动化安全测试工具。	对高风险组件执行人工安全测试。
2 级	通过自动化以及常规的手动安全渗透测试，可以使开发过程中的安全测试更加完整和高效。	采用特定于应用软件的自动化安全测试。	执行人工渗透测试。
3 级	将安全测试嵌入到开发和部署过程中。	将自动化安全测试集成到构建和部署过程中。	将安全测试集成到开发过程中。

4.3.1 可测量的基线

4.3.1.1 成熟度等级 1

收益

检测常见的、易发现的脆弱点。

活动

对软件使用自动化的静态和动态安全测试工具，可以提高安全测试的效率和质量。逐渐增加安全测试的频率并扩展代码覆盖范围。

可以通过在不运行应用软件的情况下检查应用软件的源代，以静态地执行应用软件安全测试，也可以仅通过观察各种输入条件下的应用软件行为来动态地执行应用软件安全测试。前一种方法通常称为“静态应用软件安全测试（SAST）”，后一种称为“动态应用软件安全测试（DAST）”。称为“交互式应用软件安全测试（IAST）”的混合方法通过动态测试的方式自动检测的应用软件，并结合了这两种方法的优势（以额外的投入为代价），从而可以响应外部的输入而准确监视应用软件的内部状态。

如果不仔细检查源代码，很难检测到许多安全漏洞。理想情况下，这是由专家或同行评审完成的，但这是一项缓慢而昂贵的任务。尽管“自动”SAST 工具存在很多误报和错报，且通常不如专家主导的审查准确，但它比人类更经济、更快速、更方便。许多商业和免费工具都可以有效地检测大型代码库中足够重要的错误和漏洞。

动态测试不需要应用软件源代码，因此非常适合没有源代码的情况。它还确定了漏洞的具体实例。由于其“黑盒”方法，无需在应用软件中安装插入一个代理程序，它更有可能发现浅层错误。动态测试工具需要大量的测试数据源，而手动生成测试数据是令人望而却步的。现有许多工具可以自动生成合适的测试数据，从而更有效的执行安全测试、获得更高质量的结果。

根据几个因素选择合适的工具，包括检查的深度和准确性、安全测试用例的鲁棒性和准确性、与其他工具的可用集成情况、使用情况和成本模型等。在选择工具时，参考精通安全技术人员、开发人员和开发经理的意见，并与利益相关者一起审查结果。

问题

您是否使用自动化安全测试工具扫描应用软件？

质量标准

您可以使用自动化工具动态生成用于安全测试的输入；
您选择适合组织架构和技术堆栈的安全测试工具，并在检查的深度和准确性、结果对组织的可用性之间取得平衡。

回答

没有；
是的，使用了其中一些；
是的，使用了至少有一半；
是的，使用了大多数或全部。

4.3.1.2 成熟度等级 2

收益

检测特定于组织的、易于发现的脆弱点。

活动

通过对特定技术堆栈和应用软件进行调整和自定义，提高自动化安全测试工具的效率。自动化安全测试工具具有两个重要特征：假阳性错误率（FP），即，对不存在 bug 和脆弱点的不正确报告；假阴性错误率（FN），即，对存在 bug 和脆弱点的检测缺失。随着您对自动化测试工具的使用日趋成熟，您将努力降低其假阳性错误率和假阴性错误率。这样可以最大程度地延长开发团队用于审查和解决应用软件中实际安全问题的时间，并减少通常与使用未经调整的自动化安全分析工具相关的摩擦。

首先禁用对您不使用的技术和框架的工具支持，并在可能的情况下针对特定版本。这将提高执行速度，并减少报告虚假结果的数量。依靠安全工具的拥护者或共享的安全团队，与一群积极主动的开发团队协作来试用工具。这将识别出可能忽略或从工具输出中删除的假阳性结果。确定特定的安全问题和反模式，并倾向于使用最好的工具来检测它们。

利用可用的工具功能来考虑特定于应用软件和组织的编码样式以及技术标准。许多自动化的静态分析工具允许用户编写自己的规则或自定义默认分析规则到被测项目中的特定软件界面，以提高准确性和覆盖范围。例如，潜在危险输入（又名被污染的输入）在经过指定的自定义净化方法后可以标记为安全。

从策略上讲，与尝试立即检测所有已知问题相比，通过自动化工具可靠地检测安全问题的有限子集并逐步扩展覆盖范围，是更好的办法。一旦对工具进行了充分的调整，便可以将其提供给更多的开发团队。重要的是要持续监视开发团队之间的感知效力。在更高级的形式中，可以采用机器学习技术来识别并自动过滤出可能的误报。

问题

您是否为应用软件和技术堆栈自定义了自动化安全工具？

质量标准

您可以调整和选择与您的应用软件或技术堆栈相匹配的工具功能；
通过沉默或自动过滤无关的警告或低概率的发现，可以最大程度地减少假阳性误报；
通过利用工具扩展或 DSL 为应用软件或组织标准定制工具，可以最大程度地减少假阴性误报。

回答

没有；
是的，自定义了其中一些；
是的，自定义了至少有一半；
是的，自定义了大多数或全部。

4.3.1.3 成熟度等级 3

收益

在尽可能早的阶段识别可自动识别的漏洞。

活动

组织内的项目通常会运行自动化的安全测试，并在开发过程中检查结果。将安全测试工具配置为在构建和部署过程中自动运行，以使其具有较低的开销而可扩展。检查发现的结果。

尽早在需求或设计阶段进行安全测试将是有益的。尽管传统上使用功能测试用例，但这种类型的测试驱动开发方法涉及在开发周期的早期识别并运行相关的安全测试用例。随着安全测试用例的自动执行，项目进入实施阶段，并针对不存在的功能进行了许多失败的测试。所有测试通过后，实施完成。这为开发人员在开发周期的早期提供了明确的前期目标，降低了由于安全问题或在项目截止日期之前强制接受风险而导致发布延迟的风险。

通过仪表板显示自动和手动安全性测试的结果，并定期将其呈现给管理和业务涉众（例如，在每个版本之前）以供审核。如果在版本发布时仍有未解决的发现（作为可接受的风险），则利益相关者和开发经理将共同努力制定解决这些问题的具体时间表。不断检查并提高安全测试的质量。

考虑并实施安全测试相关工具，自动化的将来自动态测试、静态测试和交互式测试的测试结果匹配和合并到一个中央仪表板中，从而直接向“缺陷管理”提供输入。在开发团队中传播所创建的安全测试和结果的相关知识，以提高组织内部的安全知识和意识。

问题

您是否将自动化安全测试集成到构建和部署过程中？

质量标准

管理层和业务利益相关者在整个开发周期中跟踪和审查测试结果；
您可以将测试结果合并到中央仪表板中，并将其输入到缺陷管理中。

回答

没有；
是的，集成了其中一些；
是的，集成了至少一半；
是的，集成了大部分或全部。

4.3.2 深刻的理解

4.3.2.1 成熟度等级 1

收益

对关键组件检测可手动识别的漏洞。

活动

执行选择性的手动安全测试，可组合使用静态和动态分析工具来指导或重点聚焦于审查工作，以便能以攻击者的视角更全面地分析应用软件的各个部分。自动化工具可以有效地发现各种类型的漏洞，但永远无法取代专家的人工审核。

软件安全关键部分中的代码级漏洞可能会大大增加影响，因此项目团队将审查高风险模块中的常见漏洞。高风险功能的常见示例包括：身份验证模块、访问控制执行点、会话管理方案、外部接口以及输入验证器和数据解析器。团队，可以将代码级指标和针对性的自动扫描结合起来，以确定将精力集中在哪些方面。在实践中，该活动可以采取多种形式，包括配对编程和对等审查，涉及整个开发团队带时间限制的安全“推送”，或由专门安全小组成员进行的自发独立审查。

在变更和审查高风险代码的开发周期中，开发经理对结果进行分类，并根据其他项目利益相关者的意见适当地对修复工作进行优先级排序。

问题

您是否对选定高风险组件的安全质量进行人工查看？

质量标准

存在可帮助审核者将重点放在高风险组件上的标准；
由合格的人员按照文档指南进行审核工作；
您根据组织的缺陷管理策略处理发现的问题。

回答

没有；
是的，对于某些组件；
是的，对于至少一半的组件；
是的，对于大多数或所有组件。

4.3.2.2 成熟度等级 2

收益

从黑盒的视角了解应用软件的韧性。

活动

使用为每个项目标识的一组安全测试用例，进行人工渗透测试，以针对每个用例评估系统的性能。通常，这发生在发布之前的测试阶段，包括静态和动态人工渗透测试。如果无法在生产环境之外对软件进行实际测试，则使用诸如“蓝绿部署”或“A/B 测试”之类的技术在生产环境中进行严格的安全测试。

渗透测试案例包括：特定于应用软件的测试以检查是否业务逻辑健全；常规的脆弱点测试以检查设计和实现的效果。一旦指定，精通安全的质量保障或开发人员就可以执行安全测试用例。中央软件安全小组对项目团队安全测试用例的首次执行进行监视，以协助和指导团队的安全专家。

许多组织提供“漏洞赏金”计划，邀请安全研究人员查找应用软件中的漏洞并负责任地报告漏洞，以换取奖励。该方法使组织可以使用更大的人才库，尤其是那些缺乏足够内部能力或需要额外保障的组织。

在发布或大规模部署之前，利益相关者会检查安全测试的结果并接受发布时安全测试失败所带来的风险。建立具体的时间表以解决随着时间的推移而出现的差距。在整个开发团队中传播手动安全测试知识和结果，以提高组织内部的安全知识和意识。

问题

您是否定期对应用软件执行渗透测试？

质量标准

渗透测试使用特定于应用软件的安全测试用例来评估安全状况；
渗透测试在应用软件中查找技术和逻辑问题；
利益相关者审查测试结果并根据组织的风险管理进行处理；
由合格的人员执行渗透测试。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

4.3.2.3 成熟度等级 3

收益

在尽可能早的阶段里识别可人工识别的安全问题。

活动

与所有其他开发活动（包括：需求分析、软件设计和构建）并行集成安全测试。

由于在开发的每个阶段都运行着多种安全工具，因此，不再适合或不希望在指定的阶段修复安全问题（例如，发布前的测试）。必须对安全问题进行快速分类，并在风险和修复成本之间进行权衡取舍，并制定修复计划。通过将特定的、低摩擦的自动化测试集成到开发工具和构建过程中，以持续在开发生命周期的早期阶段检测问题，从而降低了修复成本、增加了迅速解决问题的可能性。

通过充分传播其他安全测试活动的结果，积极改进集成到开发过程中的安全测试工作。例如，如果安全渗透测试确定了会话管理的问题，则对会话管理的任何更改都应在将更改推送到生产环境之前触发专门的安全测试。

安全专家和中央安全软件小组在开发过程中不断审查自动和人工安全测试的结果，包括将这些结果作为对开发团队安全意识培训的一部分。将学习到的经验教训整合到整体手册中，以改进安全测试，作为组织发展的一部分。对于发布版本，如果仍有未解决的安全检测结果作为接受的风险，则利益相关者和开发经理应共同努力，确定解决这些问题的具体时间表。

问题

您是否使用安全测试的结果来改进开发生命周期？

质量标准

您使用其他安全活动的结果来改进开发过程中的集成安全测试；
您审查测试结果，并将其纳入安全意识培训和安全测试手册中；
利益相关者审查测试结果并根据组织的风险管理进行处理。

回答

没有；
是的，但我们会临时改进；
是的，我们会定期改进；
是的，我们至少每年改进一次。

5、 运营

运营业务功能包括那些确保在应用软件及其关联数据在整个生命周期内维护机密性、完整性和可用性所必需的活动。此业务功能的成熟度提高，可以更好地保障组织在面对运营中断时具有的韧性，并对运营范围内的变化进行响应。

5.1 事件管理

一旦组织的应用软件进入到运营阶段，您很可能会遇到安全事件。在此模型中，我们将安全事件定义为至少一项资产的安全目标受到破坏或迫在眉睫的威胁，无论是由于恶意行为还是过失行为。安全事件的示例可能包括：对云应用软件的成功拒绝服务（DoS）攻击、应用软件用户通过滥用安全漏洞访问另一用户的私有数据、攻击者修改应用软件源代码。事件管理（IM）实践聚焦于在组织中处理这些事件。

从历史上看，许多安全事件是在首次发生的数月甚至数年后才发现的。在检测到事件之前的“停留时间”内，可能会发生重大损坏，从而增加恢复的难度。我们的第一个活动流“事件检测”就着重于减少停留时间。

一旦确定自己遭受安全事件困扰，就必须以有纪律的、彻底的方式做出响应，以限制损失，并尽可能有效地恢复正常运行。这是我们第二个活动流的重点。

成熟度等级		活动流 A 事件检测	活动流 B 事件响应
1 级	尽力而为的事件检测和处理。	使用可用的日志数据对可能的安全事件执行尽力而为的检测。	确定事件响应的角色和责任。
2 级	正式的事件管理流程到位。	遵循已建立的、有据可查的、用于事件检测的过程，重点是自动日志评估。	建立正式的事件响应流程，并确保员工接受适当的培训以执行职责。
3 级	成熟的事件管理。	使用主动管理的过程来检测事件。	聘请一支专门的、训练有素的事件响应团队。

5.1.1 事件检测

5.1.1.1 成熟度等级 1

收益

检测到最明显安全事件的能力。

活动

分析可用的日志数据（如，访问日志、应用软件日志、基础架构日志），以根据已知的保留日志数据来检测可能的安全事件。

在小型设置中，您可以在常见命令行工具的帮助下手动执行此操作。对于较大的日志量，则使用自动化技术。即使是 cron 执行简单脚本来查找可疑事件的工作，也是向前迈出的重要一步！

如果将日志从其他来源发送到专用日志聚合系统，请在此处分析日志并采用基本的日志关联原则。

即使你没有一个 7*24 事件检测过程，确保有关负责人在无法工作时（如，休假或生病）不会显著影响事件检测的速度或质量。

建立并共享事件联系人，以正式创建安全事件。

问题

您是否定期分析日志数据中的安全事件？

质量标准

您有一个用于创建安全事件的联系点；
您根据日志数据的保留时段来分析数据；
事件分析的频率与您应用软件的关键程度相一致。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

5.1.1.2 成熟度等级 2

收益

及时、持续地检测预期发生的安全事件。

活动

为事件检测过程设置专门的负责人，编制清晰描述的文档，使所有过程中的涉众都可以访问，并确保对其进行定期检查和更新（如有必要）。确保负责事件检测的员工遵循此过程（如，使用培训）。

该过程通常依赖于高度的自动化，可以从不同的来源收集日志数据并将它们关联起来，包括应用软件日志。如果合适，您可以将日志汇总在一个中央位置。定期验证分析数据的完整性。如果添加新应用软件，请确保该过程在合理的时间内覆盖了该应用软件。

使用可用的清单检测可能的安全事件。该清单应涵盖预期的攻击媒介以及已知或预期的杀伤链。定期评估和更新。

当您确定某个事件是安全事件（具有足够高的可信度）时，即使在工作时间以外，也应立即通知负责人员。进行适当的进一步分析，然后开始升级过程。

问题

您是否遵循文件记录的事件检测流程？

质量标准

该过程有专门的负责人；
您将过程文档存储在可访问的位置；
该过程考虑了需进一步分析时的响应升级路径；
您在此过程中培训了负责事件检测的员工；
您有一份潜在攻击清单，以简化事件检测。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

5.1.1.3 成熟度等级 3

收益

及时检测安全事件的能力。

活动

确保过程文档中包含用于持续改进过程的措施。检查过程改进的连续性（如，通过跟踪更改）。

确保用于可疑事件检测的清单至少与这些关联：（1）来自公司外部的源信息和知识（如，影响所使用技术的新漏洞公告），（2）过去的安全事件，（3）威胁模型结果。

对所有合理攻击场景的事件检测使用关联日志。如果没有用于事件检测的日志数据，则将其记录为一个缺陷，并根据已建立的缺陷管理流程对其进行分类和处理。

事件检测的质量不取决于事件的时间或日期。如果未在指定的时间内（如，20 分钟）确认和解决安全事件，则确保根据已建立的响应升级路径生成进一步的通知。

问题

您是否定期检查和更新事件检测过程？

质量标准

您至少每年执行一次评论；
您可以使用内部和外部数据更新潜在攻击的列表清单。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

5.1.2 事件响应

5.1.2.1 成熟度等级 1

收益

能够有效解决最常见的安全事件。

活动

第一步是识别事件响应的能力，并定义一位负责人。为他们提供所需的时间和资源，以跟上当前事件处理的最佳实践和取证工具的最新状态。

在这种成熟度下，您可能尚未建立专门的事件响应团队，但已定义了流程的参与者（通常是不同的角色）。为流程分配一个单一的联系点，并让所有相关的利益相关者都知道。确保联系点知道如何联系每个参与者，并为参与的人员定义相应的职责。

当发生安全事件时，请记录所有已采取的措施。保护此信息，防止未经授权的访问。

问题

您是否对检测到的事件做出响应？

质量标准

您已为事件处理定义了一个人员或角色；
您记录了安全事件。

回答

没有；
是的，对于某些事件；
是的，至少有一半的事件；
是的，对于大多数或所有事件。

5.1.2.2 成熟度等级 2

收益

了解并有效处理大多数安全事件。

活动

建立并记录正式的安全事件响应过程。确保文档中包含以下信息：

- 对于最可能或最常见的安全事件场景，提供处理这些事件的概要说明；对于此类情况，还需使用有关第三方事件的相关公开知识；
- 对每个事件进行分类的规则；
- 不同利益相关者参与的规则，包括：高级管理层、公共关系、法律、隐私、人力资源、外部（执法）机构和客户；指定必要的时间表，如果需要的话；
- 进行根本原因分析和结果记录的过程。

确保在工作时间之内和之外都配备知识渊博且训练有素的事件响应团队。定义行动时间表和作战室。使硬件设备和软件工具保持最新状态，并随时可以使用。

问题

您对事件处理是否使用可重复的过程？

质量标准

您已对事件分类规则达成共识；
该过程针对高危事件考虑了根本原因分析；
在此过程中负责事件响应的人员接受了培训；
提供了可用的取证分析工具。

回答

没有；
是的，对于某些事件类型；
是的，至少有一半的事件类型；
是的，对于大多数或所有事件类型。

5.1.2.3 成熟度等级 3

收益

高效的事件响应，而与事件发生的时间、位置或类型无关。

活动

建立一个专门的事件响应团队，该团队可以持续提供服务，并能在常规根本原因分析的支持下持续改进流程。对于分布式组织，为所有相关位置定义并记录运筹规则（如果适用）。

记录详细的事件响应程序并保持最新。在适当的地方使过程自动化。准备使用这些过程所需的所有资源（例如，单独的沟通基础设施或可靠外部资源的位置）。及时检测并纠正这些资源的不可用性。

定期进行安全事件和突发事件的应急演练，并将结果用于流程改进。

定义、收集、评估事件响应过程中的指标，并对其采取行动，包括对其进行持续改进。

问题

您有一支专门的事件响应团队且可用吗？

质量标准

该团队针对所有安全事件执行根本原因分析，除非有特定原因不这样做；
您至少每年检查并更新响应流程。

回答

没有；
是的，有时可用；
是的，至少有一半的时间可用；
是的，大部分或所有时间可用。

5.2 环境管理

一旦应用软件开始运行，组织在应用软件安全方面的工作就不会结束。您所使用技术堆栈中的各个元素会定期发布新的安全功能和补丁，直到它们被废弃或不再受到支持。

默认情况下，任何应用软件堆栈中的大多数技术都不安全。这通常是有意的，以增强向后兼容性或易于安装。因此，要确保组织技术堆栈的安全运行，就需要对所有组件始终应用安全基线配置。环境管理（EM）实践聚焦于保持环境的干净和安全。

在组织所依赖技术的整个生命周期中都会发现脆弱点，并且解决这些脆弱点的新版本会按各种时间表发布。这使得监视漏洞报告非常重要，并能及时、有序的修补所有受影响的系统。

成熟度等级		活动流 A 配置加固	活动流 B 补丁与更新
1 级	尽最大努力做好修补和加固。	根据随时可用的信息，尽最大努力加强配置。	对系统和应用软件组件执行最大努力的修补。
2 级	具有基线的正式流程已就位。	按照既定的基线和指南，对配置进行持续的加固。	对整个堆栈执行系统和应用软件组件的常规修补。确保及时将补丁交付给客户。
3 级	符合不断改进的流程。	主动监视配置是否与基线不符，并将检测到的事件作为安全缺陷进行处理。	主动监视更新状态，并将缺失的补丁管理为安全缺陷。主动获取组件的脆弱点并更新信息。

5.2.1 配置加固

5.2.1.1 成熟度等级 1

收益

对组件基本配置设置加固。

活动

了解保护您使用技术堆栈的重要性后，根据已备好可用的指南（如，开源项目、供应商文档、博客文章）将安全配置应用于堆栈元素。当您的团队根据反复试验和团队成员收集的信息为其应用软件开发配置指南时，鼓励他们在整个组织中分享他们的经验。

根据团队的实际经验，确定常见技术堆栈的关键元素，并为它们建立配置标准。

在这种成熟度下，您还没有一个正式的流程来管理配置基线。配置可能无法在应用软件和部署之间一致地应用，并且可能没有一致性的监视。

问题

您是否加强了技术堆栈关键组件的配置？

质量标准

您已确定所使用的每个技术栈中的关键组件；
您已经为每个关键组件建立了配置标准。

回答

没有；
是的，对于某些组件；
是的，对于至少一半的组件；
是的，对于大多数或所有组件。

5.2.1.2 成熟度等级 2

收益

持续加固组织中的技术堆栈组件。

活动

针对所使用每个技术堆栈中的所有组件，建立配置加固的基线。为了协助持续加固应用软件的基线，为组件开发配置指南。要求产品团队在可行时将配置基线应用于所有新系统以及现有系统。

将加固基线和配置指南放在变更管理下，并为每个基线和指南分配负责人。根据不断发展的最佳实践或对相关组件的变更（如，版本更新、新功能），负责人负责使它们不断保持最新。

在较大的环境中，从本地维护的主服务器派生实例的配置，并应用相关的配置基线。使用自动化工具来强化配置。

问题

您是否有针对组件的加固基线？

质量标准

您已为每个基线分配了负责人；
负责人保持对其分配的基线最新；
您将基线存储在可访问的位置；
您对负责配置的员工在这些基线中提供培训。

回答

没有；
是的，对于某些组件；
是的，对于至少一半的组件；
是的，对于大多数或所有组件。

5.2.1.3 成熟度等级 3

收益

清晰查看组件配置，以避免不符合项。

活动

主动监视已部署技术堆栈的安全配置，并根据已建立的基线进行定期检查。通过发布的报告和仪表板，确保可以随时获得配置检查的结果。

当您检测到不符合要求的配置时，请将每次出现的不符合项都视为安全发现，并在已建立的缺陷管理实践中管理纠正措施。

使用自动化措施可以实现进一步的收益，例如，“自我修复”配置、安全信息和事件管理（SIEM）告警。

作为更新组件过程的一部分（如，新版本、供应商补丁），审查相应的基线和配置指南，并根据需要对其进行更新以保持其相关性和准确性。至少每年审查一次其他基线和配置指南。

定期审查您的基线管理过程，并与从应用和维护配置基线和配置指南的团队中获得的反馈和经验教训相结合。

问题

您是否监视并强制执行基线加固？

质量标准

您定期执行符合性检查，最好使用自动化手段；
您将合格性检查结果存储在可访问的位置；
您遵循已建立的流程来解决报告的不符合项；
您至少每年检查一次每个基线，并在需要时进行更新。

回答

没有；
是的，对于某些组件；
是的，对于至少一半的组件；
是的，对于大多数或所有组件。

5.2.2 补丁与更新

5.2.2.1 成熟度等级 1

收益

缓解第三方组件中众所周知的问题。

活动

确定需要更新或打补丁的应用软件和第三方组件，包括：底层操作系统、应用软件服务器和第三方代码库。

在这个成熟度等级上，识别和修补活动是尽力而为且临时性的，没有一个托管过程以跟踪组件版本、可用更新和补丁状态。但是，可能存在对补丁活动的概要要求（如，在投入生产之前测试补丁程序），并且产品团队正在尽最大努力达到这些要求。

除了重要的安全更新外（如，已公开发布针对第三方组件的漏洞利用），团队可利用为其他目的而建立的维护窗口期来执行组件补丁更新。对于组织开发的软件，组件修补程序仅作为向客户和组织托管解决方案所提供功能发布的一部分。

团队会临时共享他们对可用软件更新的了解情况以及修补经验。确保团队可以确定正在使用所有组件的版本，以评估其产品是否在受到通知时受到安全漏洞的影响。但是，生成和维护组件列表的过程可能需要大量分析人员的努力。

问题

您是否识别并修补易受攻击的组件？

质量标准

您具有组件的最新列表，包括版本信息；
您定期查看公开资源中与组件相关的脆弱点信息。

回答

没有；
是的，对于某些组件；
是的，对于至少一半的组件；
是的，对于大多数或所有组件。

5.2.2.2 成熟度等级 2

收益

持续且主动地修复技术堆栈组件。

活动

开发并遵循定义明确的过程，来管理使用技术堆栈中应用软件组件的补丁。确保流程包括与供应商更新时间（如，Microsoft Patch Tuesday）相一致的供应商更新常规计划。对于组织开发的软件，无论您是否包括新功能，都应向客户和组织托管的解决方案定期（如，每月）发布相关信息。

为优先考虑组件修补创建指南，以反映您的风险承受能力和管理目标。在确定测试和应用补丁程序的优先级时，请考虑操作因素（例如，应用软件的重要性、已解决漏洞的严重性）。

如果收到有关组件中严重漏洞的通知，而尚无补丁可用，则将其分类并作为风险管理问题进行处理（例如，实施补偿性控制、获得客户风险接受或禁用受影响的应用软件/功能） 。

问题

您是否遵循既定流程来更新技术堆栈的组件？

质量标准

该过程包括第三方修补程序的供应商信息；
该过程考虑了外部来源以收集有关零日攻击的信息，并包括适当的风险缓解步骤；
该过程包括有关确定组件更新优先级的指南。

回答

没有；
是的，对于某些组件；
是的，对于至少一半的组件；
是的，对于大多数或所有组件。

5.2.2.3 成熟度等级 3

收益

清晰查看组件补丁程序状态，以避免不符合项。

活动

开发和使用管理仪表板或报告来跟踪整个产品组合中补丁程序和 SLA 的合规状态。确保依赖项管理和应用软件打包过程可以随时支持应用的组件级补丁，以满足所需的 SLA。

将缺失的更新视为与安全相关的产品缺陷，并根据您已建立的缺陷管理实践管理它们的分类和更正。

不要依靠组件供应商的例行通知来了解漏洞和相关补丁。监视各种外部威胁情报源，以了解零日漏洞；处理那些对您应用软件造成影响的风险问题。

问题

您是否定期评估组件并审查补丁的状态？

质量标准

您更新组件和版本的列表；
您根据现有的 SLA 识别并更新缺失的更新；
您根据执行修补程序人员的反馈意见来审查和更新流程。

回答

没有；
是的，对于某些组件；
是的，对于至少一半的组件；
是的，对于大多数或所有组件。

5.3 运营管理

运营管理（OM）实践聚焦于在整个运营支持功能中确保安全性得到维护的活动。尽管这些功能不是由应用软件直接执行的，但应用软件及其数据的整体安全取决于它们的适当性能。在不支持补丁程序的漏洞，不受支持的操作系统上部署应用软件，或者无法安全地存储备份介质，可能会使该应用软件内置的保护不起作用。

该实践涵盖的功能包括但不限于：系统的供应、管理、退役；数据库的供应和管理；以及数据备份、还原和存档。

成熟度等级		活动流 A 数据保护	活动流 B 系统退役和旧版本管理
1 级	基础实践。	实施基本的数据保护实践。	退役已确定未使用的应用软件和服务。单独管理每个客户的升级和迁移。
2 级	托管的响应流程。	建立数据目录并建立数据保护策略。	为未使用的系统或/服务以及对从遗留依赖项的迁移过程，开发可重复使用的退役过程。为客户管理旧版迁移路线图。
3 级	主动监视和响应。	自动检测策略的不合规情况，并定期审核合规情况。定期检查和更新数据目录和数据保护策略。	针对不再受支持的报废依赖项和交付软件的旧版本，主动管理迁移路线图。

5.3.1 数据保护

5.3.1.1 成熟度等级 1

收益

通过实施快速见效的措施，以了解处理数据的敏感性。

活动

了解您应用软件存储和处理数据的类型和敏感性，并保持对处理后数据情况的了解（如，备份、与外部合作伙伴共享）。在此成熟度等级下，收集到的信息可能会以不同的形式和不同的位置被捕获，并假定不存在组织范围内的数据目录。根据对最敏感数据存储和处理的保护要求，保护和处理与给定应用软件关联的所有数据。

实施基本控制，以防止将未经净化的敏感数据从生产环境传播到较低安全保护等级的环境中。通过确保未经净化的生产数据不会传播到较低的（非生产）环境，您可以将数据保护策略和活动集中在生产环境上。

问题

您是否根据对在每个应用软件上存储和处理数据的保护要求来保护和处理信息？

质量标准

您知道每个应用软件处理和存储的数据元素；
您知道每个已识别数据元素的类型和敏感性级别；
您可以进行控制以防止未经净化的敏感数据从生产传播到较低的环境。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

5.3.1.2 成熟度等级 2

收益

标准化处理不同类别的敏感数据。

活动

在此成熟度等级，数据保护活动聚焦于主动对数据进行管理。建立技术和管理控制措施，以保护敏感数据的机密性，以及您关心所有数据的完整性和可用性，从最初的创建或接收到保留期结束时销毁备份。

识别应用软件存储、处理和传输的数据，并捕获有关其类型、敏感度（分类）级别、数据目录中的存储位置信息。明确标识受特定法规约束的记录或数据元素。建立与您使用数据有关的唯一事实来源，以支持对控件进行更细粒度的选择以保护它们。收集这类信息可以提高您对数据相关查询（如，来自审核员、事件响应团队或客户）时响应的准确性、及时性和效率，并支持威胁建模和合规活动。

根据您的数据保护策略，建立保护和保留数据整个生命周期的过程和程序，无论是静止的、正在处理的、还是在传输过程中。特别注意对处理系统之外敏感数据的处理和保护，包括但不限于：备份的存储、保留和销毁；以及离线存储媒介的标识、加密和物理保护。您的流程和过程涵盖了所有控制措施的实施，这些控制措施均需遵守有关存储所在位置、人员访问和其他因素的法规、合同或其他限制。

问题

您是否维护数据目录，包括：类型、敏感度等级、及处理和存储的位置？

质量标准

数据目录存储在可访问的位置；
您知道哪些数据元素受特定法规约束；
您具有在整个生命周期内保护和保留数据的控制机制；
您对数据有保留要求，并在相关保留期结束后及时销毁备份。

回答

没有；
是的，对于我们的一些数据；
是的，对于我们至少一半的数据；
是的，对于我们的大部分或全部数据。

5.3.1.3 成熟度等级 3

收益

从技术上强制遵守您的数据保护政策。

活动

此成熟度等级的活动着重于自动化的数据保护，从而减少了您对评估和管理策略遵从性时的人力投入。重点放在反馈机制和主动审查上，以识别流程改进机会并采取行动。

实施技术控制以强制遵守您的数据保护策略，并监视和检测任何企图或实际的违规行为。您可以使用各种可用的工具来防止数据丢失、访问控制和跟踪或异常行为检测。

定期审计已建立管理控制措施的合规情况，并密切监视自动化机制的性能和运行情况，包括备份和记录删除。监视工具可自动化的快速检测并报告故障，从而使您能够及时采取纠正措施。

定期检查和更新数据目录，以保持其对数据格局的准确反映。定期流程和程序进行审查和更新，以使其与您的策略和优先级保持一致。

问题

您是否定期审查和更新数据目录以及您的数据保护策略和过程？

质量标准

您具有自动监视功能，可以检测出企图或实际违反数据保护政策的情况；
您具有用于防止数据丢失、访问控制和跟踪、异常行为检测的工具；
您定期审计自动化机制的运行情况，包括备份和记录删除。

回答

没有；
是的，我们会根据要求执行；
是的，我们每隔几年执行一次；
是的，我们至少每年执行一次。

5.3.2 系统退役和旧版本管理

5.3.2.1 成熟度等级 1

收益

识别未使用的软件资产或组件。

活动

通过偶然观察或偶尔执行检查来临时标识未使用的应用软件。当您确定未使用的应用软件时，请处理这些发现以采取进一步的措施。如果您已经建立了让未使用的应用软件退役的正式流程，请确保团队知道并使用它。

针对每个产品和客户用户组，管理相关客户和客户用户组从旧版本产品的迁移情况。当任何客户用户组不再使用某个产品版本时，请停止对该版本的支持。但是，在当前成熟度等级，您可能拥有大量客户与用户正在使用的产品版本，这需要开发人员花大力气在后续版本中植入产品的修复程序。

问题

您是否标识并删除不再使用的、已达到使用寿命的、不再被积极开发或支持的系统、应用软件、应用软件依赖项或服务？

质量标准

您不使用不受支持的应用软件或依赖项；
您对每个产品和客户用户组，管理相关客户和客户用户组从旧版本产品的迁移情况。

回答

没有；
是的，对于某些应用软件；
是的，对于至少一半的应用软件；
是的，对于大多数或所有应用软件。

5.3.2.2 成熟度等级 2

收益

标准化的停用废除过程，以降低某些组件被遗忘的风险。

活动

作为停用废除系统、应用软件或服务的一部分，遵循既定流程从运行环境中删除所有相关的帐户、防火墙规则、数据等。通过从配置文件中删除这些未使用的元素，可以提高基础架构代码资源的可维护性。

遵循一致的流程，及时更换或升级已到期的第三方应用软件或应用软件依赖项（如，操作系统、专用的应用软件、库文件）。

在产品寿命即将到期时，与您产品的客户和用户群体互动，以将其及时迁移到提供支持的版本。

问题

在停用未使用的系统、应用软件、应用软件依赖项或服务时，您是否遵循既定流程以删除所有相关资源？

质量标准

您在可访问的位置记录对产品所有发行版本的支持状态；
该过程包括对已到期的第三方应用软件或应用软件依赖项的替换或升级；
运行环境中不再包含被遗弃的帐户、防火墙规则或其他配置文件。

回答

没有；
是的，有时候；
是的，至少有一半的时间；
是的，大部分或所有时间。

5.3.2.3 成熟度等级 3

收益

全面了解所有软件资产的生命周期。

活动

定期评估每个软件资产和基础架构组件的生命周期状态和支持状态，并估计其使用寿命。遵循定义明确的流程，以主动缓解由于资产或组件接近其使用寿命而产生的安全风险。定期检查和更新您的流程，以反映所汲取的教训。

制定产品支持计划，对即将废除的较旧产品版本停止支持提供明确的时间表。将有效使用的产品版本号限制为小的编号（例如，仅为 N.x.x 和 N-1.x.x）。建立并公开时间表，以中止对先前版本的支持，并与客户和用户群体积极互动，防止服务或支持受到干扰。

问题

您是否定期评估每个软件资产和基础架构组件的生命周期状态和支持状态，并估计其使用寿命？

质量标准

您的“使用寿命终止管理流程”已达成共识；
您将产品时间表通知客户和用户组，以防止服务或支持的中断；
您至少每年检查一次该过程。

回答

没有；
是的，对于某些资产；
是的，对于至少一半的资产；
是的，对于大多数或全部资产。

访谈记录表

说明
根据以下问题，根据 SAMM 业务功能和安全实践组织面试。
从“答案”列中的多项选择下拉选择中选择最佳答案。
在“面试笔记”栏中记录其他信息，如如何和为什么。
隐藏列 F-H 中的公式将计算分数，并根据需要更新评分框和其他工作表。
面试结束后，转到“记分卡”表并按照说明进行操作。

组织机构:	
团队/应用程序:	
访谈日期:	
团队领导:	
贡献者:	

治理					
活动流	**等级**	**战略与指标**	**回答**	**访谈记录**	**评级**
创建与推广	**1**	**您了解您的应用软件在整个企业范围内的风险偏好吗？**			**0.00**
		您把握了组织高管领导层的风险偏好。 组织的领导层审查并批准了一系列风险。 您为您的资产和数据识别了主要业务和技术威胁。 您记录风险并将其存储在可访问的位置。			
	2	**您是否有针对应用软件安全的战略计划，并用来制定决策？**			

		该计划反映了组织的业务重点和风险承受能力。 该计划包括可衡量的里程碑和预算。 该计划与组织的业务驱动因素和风险相一致。 该计划为战略和战术计划制定了路线图。 您获得了利益相关者的支持，包括开发团队。		
	3	**您是否经常审查和更新应用软件安全战略计划？**		
		您可以根据业务环境、组织或其风险偏好的重大变化来审查和更新计划。 计划的更新步骤包括与所有利益相关者一起审查计划，以及更新业务驱动因素和策略。 您可以根据从已完成的路线图活动中获得的经验教训，来调整计划和路线图。 您发布有关路线图活动的进度信息，以确保所有利益相关者都可以使用它们。		
测量与改进	**1**	**您是否使用一组指标来衡量应用软件安全计划的有效性和效率？**		
		您记录每个指标，包括来源描述、测量范围，以及有关如何使用它来解释应用软件安全趋势； 指标包括投入工作量、结果和环境三个类别； 大多数测量标准经常被测量，且数据收集方法方便、经济，并表示为基数或百分比； 由应用软件安全和开发团队发布指标。		
	2	**您定义的关键性能指标（KPI）是否来自于可用的应用软件安全指标？**		
		您在收集了足够的信息后，才定义了 KPI、建立了切合实际的目标； 您是由负责应用软件安全的领导层和团队来开发 KPI 的； 应用软件团队可以使用 KPI，其中包括可接受性的阈值和指南，以防团队需		

		要采取行动； 根据已定义的 KPI，可以清楚地看到应用软件安全计划的成功。			
	3	**您是否根据应用软件安全指标和 KPI 更新了应用软件安全战略和路线图？**			
		您每年至少审查一次 KPI 的效率和有效性； KPI 和应用软件安全指标触发了对应用软件安全战略的大部分更改。			
策略与合规			**回答**	**面试笔记**	**评级**
策略与标准	1	**您在整个组织中是否拥有并应用一套通用的策略和标准？**			**0.00**
		您已经采用了适合于组织所在行业的现有标准，以解决特定域的问题； 您的标准与策略保持一致，并纳入特定于技术的实施指南。			
	2	**您是否以测试脚本或运行手册的形式发布组织的策略，以方便开发团队进行解释？**			
		您创建了验证清单列表和测试脚本，并与策略要求和相关标准中的实施指南保持一致； 您创建了适用于组织所使用每种开发方法和技术的版本信息。			
	3	**您是否定期报告策略和标准的合规情况，并使用该信息指导合规工作的改进？**			
		您具有定期生成合规报告的过程（如果可能的话，以自动的形式生成报告）； 您将合规报告提供给所有相关的利益相关者； 利益相关者使用报告的合规状态信息来确定需要改进的地方。			
合规管理	1	**您对外部合规义务有完整的了解吗？**			

		您已确定外部合规义务的所有来源； 您已从所有来源捕获并协调了合规义务			
	2	**您是否有一套标准的安全需求和验证程序来解决组织的外部合规义务？**			
		您将每个外部合规义务映射到一组定义明确的应用软件需求； 您定义验证程序（包括自动测试），以验证是否符合相关要求。			
	3	**您是否定期报告外部合规义务的遵守情况，并使用这些信息来指导有关缩小合规差距的工作？**			
		您已经建立了明确定义的合规指标； 您定期测量和报告应用软件的合规指标； 利益相关者使用报告的合规状态信息来识别合规差距，并确定差距补救工作的优先级。			
教育与指导			**回答**	**面试笔记**	**评级**
培训和意识	**1**	**您是否要求涉及应用软件开发的员工接受 SDLC 培训？**			**0.00**
		培训是可重复的、持续的，并且对任何参与软件开发生命周期的人员都可用。 培训在适当的情况下包括最新的 OWASP Top 10，并包括诸如最低权限、纵深防御、安全故障保护、完全消减、会话管理，开放式设计和心理接受性的概念。 培训需要参加者的签字或确认。 您在最近 12 个月内更新了培训。 在员工入职过程中提供了培训。			
	2	**培训是否对不同角色（如：开发人员、测试人员或安全专家）进行量身定制？**			

		培训包括“成熟度等级 1”中的所有培训主题，并增加了其他特定的工具、技术和演示； 所有员工和承包商都必须参加培训； 培训包括组织内部专家和受训人员的输入信息； 培训包括组织内部开发的工具和技术演示； 使用培训反馈信息对培训进行优化。		
	3	**您是否配备了一个学习管理系统或类似系统来追踪员工的培训和认证过程？**		
		学习管理系统被用于追踪培训和认证过程； 培训基于内部标准、政策和程序； 使用认证计划或考勤记录来确定对开发系统和资源的访问。		
组织和文化	**1**	**您是否为每个开发团队确定了“安全专家”？**		
		“安全专家”接受了适当的培训； 应用软件安全团队和开发团队会定期收到来自“安全专家”的简报，内容涉及安全计划和修复的总体状态； “安全专家”在解决应用软件积压的问题之前，先审查外部测试的结果。		
	2	**组织是否有一个卓越的安全软件中心（SSCE）？**		
		SSCE 有一个章程来定义其在组织中的角色； 开发团队与 SSCE 审查所有重要的架构变更； SSCE 发布与应用软件安全相关的 SDLC 标准和指南； 产品专家负责促进特定安全工具的使用。		
	3	**是否有一个集中的门户网站，支持来自不同团队和业务部门的开发人员和应用软件安全专业人员交流和共享信息？**		

		组织为不同的团队和业务部门推广使用唯一的一个门户网站； 该门户网站用于及时信息发布，如：安全事件、工具更新、架构标准更改的通知，以及其他相关公告； 该门户网站被开发人员和架构师广泛认可为组织特定的应用软件安全信息集中存储库； 所有内容都被认为是可持久使用的和可搜索的； 该门户网站可访问特定于应用软件的安全指标。		
设计				
威胁评估			**回答**	**面试笔记**	**评级**
应用软件风险画像	**1**	**您是否使用一组简单且预定义的问题，并根据业务风险对应用软件进行分类？**			**0.00**
		已有商定的风险分类方法； 应用团队了解风险分类； 风险分类涵盖组织面临业务风险的关键方面； 组织拥有范围内应用软件的清单。			
	2	**您是否使用集中和量化的应用软件风险画像来评估业务风险？**			
		应用软件风险画像符合组织风险标准； 应用软件风险简介涵盖了对安全和隐私的影响； 您可以手动和/或自动验证风险画像的质量； 应用软件风险画像集中存储。			
	3	**您是否定期审查和更新应用软件的风险画像？**			
		组织的风险标准考虑了历史反馈，以不断改进评估方法； 应用软件或业务环境中的重大变化，会触发对相关风险画像的审查。			
威胁建模	**1**	**您是否通过威胁建模识别和管理架构设计缺陷？**			

		您对高风险应用软件执行威胁建模； 您使用简单的威胁清单，例如 STRIDE； 您将威胁模型的结果保留下来，以备后用。			
	2	**您是否使用符合您应用软件风险级别的标准方法？**			
		培训您的架构师、安全专家和其他利益相关者如何进行实际威胁建模； 您的威胁建模方法论至少包括：图表、威胁识别、设计缺陷缓解措施以及如何验证威胁模型成果输出的方法； 应用软件或业务环境中的变化，会触发对相关威胁模型的审查； 用应用软件团队使用的工具获得威胁建模成果输出。			
	3	**您是否定期检查和更新了应用软件的威胁建模方法？**			
		威胁模型方法论考虑了历史反馈信息以进行改进； 您定期（例如，每年一次）审查现有的威胁模型，以验证应用软件与新的威胁无关； 使用威胁建模工具自动化执行威胁建模过程。			
安全需求			**回答**	**面试笔记**	**评级**
软件需求	**1**	**项目团队在开发过程中是否明确安全需求？**			**0.00**
		团队从功能需求以及客户或组织的关注中得出安全需求； 安全需求是特定的、可测量的和合理的； 安全需求符合组织基线。			
	2	**您是否在安全需求收集过程的成果输出中定义、结构化并包含安全需求的优先级？**			
		当策略和指南应用于产品开发时，安全需求考虑了特定领域的知识； 领域专家参与需求定义过程； 您已经就安全需求达成了一致的结构化表示法； 开发团队拥有一名安全专家，专门负责审查安全需求和结果。			
	3	**您是否使用标准需求框架来简化对安全需求的获取？**			

		安全需求框架对项目团队可用； 该框架按通用要求和基于标准的要求进行分类； 该框架为需求质量以及如何描述需求提供了明确的指导； 该框架可适应特定的业务需求。			
供应商安全	1	**利益相关者是否审查与合作供应商的安全需求和方法？**			
		当创建第三方协议时，您考虑了包括特定的安全需求、活动和流程； 配备了供应商调查表，以评估供应商的优势和劣势。			
	2	**供应商是否满足组织定义《服务级别协议》中的安全责任和质量措施？**			
		当创建供应商协议时与供应商讨论安全需求； 供应商协议中约定：在商定时间期限内提供有关安全缺陷修复的特定指导； 针对关键供应商安全流程，组织配备有职责和服务等级的模板协议； 测量关键的绩效指标。			
	3	**供应商是否与组织使用的标准安全控制、软件开发工具和流程保持一致？**			
		供应商拥有一个安全的 SDLC，其中，与组织使用的安全构建、安全部署、缺陷管理和事件管理相一致； 在每个主要版本发布之前，您都要验证解决方案是否满足质量和安全性目标； 如果没有标准的验证流程，则使用补偿控制机制，例如：软件成分分析、独立的渗透测试。			
安全架构			**回答**	**面试笔记**	**评级**
架构设计	1	**团队在设计过程中是否使用安全原则？**			**0.00**
		您有一个已达成一致的安全原则清单； 您将安全原则清单存储在可访问的位置； 相关利益相关者了解安全原则。			

	2	**您在设计过程中是否使用共享安全服务？**			
		您有一份记录的可重用安全服务列表，并可供相关利益相关者使用； 您已经查看了每个选定服务的基线安全状况； 您的设计师经过培训，可以按照可用的指导集成每个选定的服务。			
	3	**您的设计是否基于可用的参考架构？**			
		您已记录了一个或多个已批准的参考架构，可供利益相关者使用； 您基于深刻理解和最佳实践不断改进参考架构； 您提供了一组组件、库和工具来实现每个参考架构。			
技术管理	1	**您是否评估开发所使用重要技术的安全质量？**			
		您有一个包含所有应用软件使用和支持最重要技术的列表； 您识别并跟踪技术风险； 您确保这些技术的风险符合组织基线。			
	2	**您是否有一个针对该组织的推荐技术列表？**			
		该列表基于软件中使用的技术； 由首席架构师和开发人员审查并批准该列表； 您在整个组织中共享列表； 您至少每年检查和更新一次列表。			
	3	**您是否在组织内强制使用推荐的技术？**			
		您定期监视应用软件，以判断是否正确使用了推荐的技术； 您可以根据组织政策解决针对列表的违规问题； 如果违规数量超出年度目标，则应采取措施。			
开发					
安全构建			**回答**	**面试笔记**	**评级**
构建过程	1	**您的完整构建过程得到正式描述了吗？**			

		您有足够的信息来重新创建构建过程； 您的构建文档是最新的； 您的构建文档存储在可访问的位置； 生成的工件校验和是在构建期间创建的，以支持以后的验证； 对构建过程中使用的工具进行加固。			0.00
	2	**构建过程是否完全自动化？**			
		构建过程本身不需要任何人工干预 根据最佳实践和供应商指南对构建工具进行了强化 您可以加密构建工具所需的机密信息，并根据最小特权原则控制访问权限			
	3	**您是否在构建过程中执行了自动安全检查？**			
		如果应用软件不符合预定义的安全基线，则构建失败； 您对脆弱点具有最高危的可接受程度； 您在集中式系统中记录警告和故障信息； 您选择并配置工具，以至少每年一次的方式对每个应用软件的安全需求进行评估。			
软件依赖	**1**	**您对所依赖的依赖项有扎实的知识吗？**			
		您有每个应用软件当前的物料清单（BOM）； 您可以快速找出哪些应用受特定 CVE 的影响； 在过去的三个月中，您至少分析、解决并记录了依赖项的发现情况。			
	2	**您是否通过正式程序处理第三者依赖风险？**			
		您保留符合预定义条件的已批准依赖项列表； 您可以自动评估新 CVE 的依赖关系并提醒负责人员； 您会自动检测许可证更改并发出警报，这可能会影响合法应用软件的使用；			

		您跟踪并提醒有关未维护依赖项的使用情况； 您可以可靠地检测并删除软件中不必要的依赖项。			
	3	**如果软件构建受依赖关系漏洞的影响，您是否会阻止软件构建？**			
		您的构建系统已连接至用于跟踪第三方依赖风险的系统，除非导致漏洞被评估为误报或明确接受了风险，否则将导致构建失败； 您使用静态分析工具扫描依赖关系； 您使用已建立负责任的披露流程将发现报告给依赖项作者； 使用未评估安全风险的新依赖项会导致构建失败。			
安全部署			**回答**	**面试笔记**	**评级**
部署过程	1	**您是否使用可重复的部署过程？**			**0.00**
		您有足够的信息来运行部署过程； 您的部署文档是最新的； 相关利益相关者可以访问您的部署文档； 您确保只有定义合格的人员才能触发部署； 您可以对部署过程中使用的工具进行加固。			
	2	**部署过程是否自动化并采用安全检查？**			
		部署过程在所有阶段都是自动化的； 部署包括了自动化安全测试程序； 您提醒相关负责人员注意已发现的漏洞； 您在定义的时间内有可用于过去部署的日志。			
	3	**您是否持续验证已部署软件部件的完整性？**			

		如果检测到完整性问题，则阻止或回退部署； 针对在构建期间所创建签名的验证工作已经完成； 如果无法检查签名（如，外部构建软件），则采取补偿措施。			
机密信息管理	1	**您是否按照最小特权原则限制对应用软件机密信息的访问？**			
		您将生产环境机密信息存储在安全的位置； 开发人员无法访问生产环境机密信息； 生产环境机密信息在非生产环境中不可用。			
	2	**您是否在部署期间将生产环境机密信息注入到配置文件中？**			
		源代码文件不再包含使用的应用软件机密信息； 在正常情况下，部署过程中不会有人访问机密信息； 您记录并警告任何对机密信息的异常访问。			
	3	**您是否对应用软件机密信息实施了适当的生命周期管理？**			
		您可以使用经过审查的解决方案生成和同步机密信息； 不同的应用软件实例之间的机密信息是不同的； 机密信息会定期更新。			
缺陷管理			**回答**	**面试笔记**	**评级**
缺陷跟踪	1	**您是否在可访问的位置跟踪所有已知的安全缺陷？**			**0.00**
		您可以轻松获得影响一个应用软件的所有安全缺陷的概述； 您至少有一个基本的分类方案； 该过程包括处理误报和重复条目的策略； 缺陷管理系统涵盖了来自不同来源和实践的缺陷。			
	2	**您是否对整个组织的安全缺陷状态进行了概述？**			

		单一严重性方案适用于组织中的所有缺陷； 该方案包括用于修复特定严重等级的 SLA； 您定期报告 SLA 的遵守情况。		
	3	**您是否执行 SLA 来修复安全缺陷？**		
		您会自动发出有关 SLA 违规的告警，并将相应的缺陷转移到风险管理流程中； 您将相关工具（例如，监视、构建、部署）与缺陷管理系统集成在一起。		
指标与反馈	**1**	**您是否使用有关已记录安全缺陷的基本指标，来进行快速制胜的改进活动？**		
		您去年至少分析了一次记录的指标； 至少记录并提供了有关该计划的基本信息； 您已根据数据确定并进行了至少一项快速制胜活动。		
	2	**您是否根据标准化指标改进了安全保障计划？**		
		您为缺陷的分类和活动流记录了指标，并保持指标最新； 执行管理层定期接收有关缺陷的信息，并在去年采取了措施； 您定期在团队之间共享有关安全缺陷的技术详细信息。		
	3	**您是否定期评估安全指标的有效性，以便其输入有助于推动安全策略的信息？**		
		您去年至少分析过一次安全指标的效果； 在可能的情况下，您将自动验证数据的正确性； 指标与其他信息来源（如，威胁情报、事件管理）汇总； 您从去年的指标中衍生出至少一项战略活动。		
验证				
架构评估			**回答**	**面试笔记**	**评级**

架构验证	1	**您是否临时审查应用软件架构中的关键安全目标？**			0.00
		您已经就整体软件架构达成了共识模型； 您将组件、接口和集成的组件包括在架构模型中； 您验证常规安全机制的正确提供情况； 您将缺失的安全控件记录为缺陷。			
	2	**您是否定期审查架构的安全机制？**			
		您审查对内部和外部要求的合规情况； 您系统地审查系统中的每个接口； 您使用正式的审查方法和结构化验证； 您将缺失的安全机制记录为缺陷。			
	3	**您是否定期审查安全控制的有效性？**			
		您评估安全控件的预防能力、检测能力和响应能力； 您评估安全控制的策略一致性、支持恰当性以及可伸缩性； 您至少每年评估一次效果； 您将识别的缺点记录为缺陷。			
架构缓解	1	**您是否会临时审查应用软件架构以缓解典型威胁？**			
		您已经就整体软件架构达成了共识模型； 由精通安全的人员进行审查； 您考虑各种类型的威胁，包括内部威胁和与数据相关的威胁。			
	2	**您是否定期评估对架构的威胁？**			
		您系统地审查了威胁评估中确定的每个威胁； 由受过训练或有经验的人审查实践情况； 您可每种已识别的威胁确定设计级别的缓解功能； 您将未处理的威胁记录为缺陷			
	3	**您是否根据架构评估结果定期更新参考架构？**			

		您以标准化的书面形式评估架构； 您使用重复发现的威胁来触发对参考架构的审查； 您可以临时、独立审查架构评估的质量； 您以参考架构更新触发点，以基于风险的方式对相关共享解决方案进行审查。			
需求驱动测试			**回答**	**面试笔记**	**评级**
控制验证	**1**	**您是否测试应用软件的标准安全控制功能是否正常？**			**0.00**
		安全测试至少要验证身份验证，访问控制，输入验证，数据编码和转义以及加密控制的实现 每当应用软件更改其控件的使用时，都会执行安全性测试			
	2	**您是否始终如一地编写和执行测试脚本以验证安全需求的功能？**			
		您可以针对每个应用软件量身定制测试并声明预期的安全功能 您将测试结果捕获为通过或失败条件 测试使用标准化框架或 DSL			
	3	**您是否自动测试应用软件的安全性退化？**			
		您始终为所有已识别的错误编写测试（可能超过了预先定义的严重性阈值） 您在作为现有单元测试框架一部分的测试套件中收集安全测试			
滥用测试	**1**	**您是否使用随机化或模糊测试技术来测试应用软件？**			
		测试涵盖了应用软件的大部分或全部主要输入参数 您会尽力记录并检查所有应用软件崩溃对安全性的影响			
	2	**您是否根据功能需求创建滥用案例并使用它们来进行安全性测试？**			
		重要业务功能有相应的滥用案例 您以明确的动机和特征围绕相关角色构建虐待故事 您将已识别的弱点捕获为安全需求			

	3	**您是否执行拒绝服务和安全压力测试？**			
		压力测试针对特定的应用软件资源（例如，通过将大量数据保存到用户会话中来耗尽内存） 您可以使用定义明确的功能（知识，资源）围绕相关角色设计测试 您将结果反馈给设计实践			
安全测试			**回答**	**面试笔记**	**评级**
可测量的基线	1	**您是否使用自动化安全测试工具扫描应用软件？**			**0.00**
		您可以使用自动化工具动态生成用于安全测试的输入； 您选择适合组织架构和技术堆栈的安全测试工具，并在检查的深度和准确性、结果对组织的可用性之间取得平衡。			
	2	**您是否为应用软件和技术堆栈自定义了自动化安全工具？**			
		您可以调整和选择与您的应用软件或技术堆栈相匹配的工具功能； 通过沉默或自动过滤无关的警告或低概率的发现，可以最大程度地减少假阳性误报； 通过利用工具扩展或 DSL 为应用软件或组织标准定制工具，可以最大程度地减少假阴性误报。			
	3	**您是否将自动化安全测试集成到构建和部署过程中？**			
		管理层和业务利益相关者在整个开发周期中跟踪和审查测试结果； 您可以将测试结果合并到中央仪表板中，并将其输入到缺陷管理中。			
深刻的理解	1	**您是否对选定高风险组件的安全质量进行人工查看？**			
		存在可帮助审核者将重点放在高风险组件上的标准； 由合格的人员按照文档指南进行审核工作； 您根据组织的缺陷管理策略处理发现的问题。			
	2	**您是否定期对应用软件执行渗透测试？**			

		渗透测试使用特定于应用软件的安全测试用例来评估安全状况； 渗透测试在应用软件中查找技术和逻辑问题； 利益相关者审查测试结果并根据组织的风险管理进行处理； 由合格的人员执行渗透测试。			
	3	**您是否使用安全测试的结果来改进开发生命周期？**			
		您使用其他安全活动的结果来改进开发过程中的集成安全测试； 您审查测试结果，并将其纳入安全意识培训和安全测试手册中； 利益相关者审查测试结果并根据组织的风险管理进行处理。			
运营					
事件管理			**回答**	**面试笔记**	**评级**
事件检测	1	**您是否定期分析日志数据中的安全事件？**			**0.00**
		您有一个用于创建安全事件的联系点； 您根据日志数据的保留时段来分析数据； 事件分析的频率与您应用软件的关键程度相一致。			
	2	**您是否遵循文件记录的事件检测流程？**			
		该过程有专门的负责人； 您将过程文档存储在可访问的位置； 该过程考虑了需进一步分析时的响应升级路径； 您在此过程中培训了负责事件检测的员工； 您有一份潜在攻击清单，以简化事件检测。			
	3	**您是否定期检查和更新事件检测过程？**			
		您至少每年执行一次评论； 您可以使用内部和外部数据更新潜在攻击的列表清单。			
事件响应	1	**您是否对检测到的事件做出响应？**			

		您已为事件处理定义了一个人员或角色； 您记录了安全事件。			
	2	**您对事件处理是否使用可重复的过程？**			
		您已对事件分类规则达成共识； 该过程针对高危事件考虑了根本原因分析； 在此过程中负责事件响应的人员接受了培训； 提供了可用的取证分析工具。			
	3	**您有一支专门的事件响应团队且可用吗？**			
		该团队针对所有安全事件执行根本原因分析，除非有特定原因不这样做； 您至少每年检查并更新响应流程。			
环境管理			**回答**	**面试笔记**	**评级**
配置加固	1	**您是否加强了技术堆栈关键组件的配置？**			**0.00**
		您已确定所使用的每个技术栈中的关键组件； 您已经为每个关键组件建立了配置标准。			
	2	**您是否有针对组件的加固基线？**			
		您已为每个基线分配了负责人； 负责人保持对其分配的基线最新； 您将基线存储在可访问的位置； 您对负责配置的员工在这些基线中提供培训。			
	3	**您是否监视并强制执行基线加固？**			
		您定期执行符合性检查，最好使用自动化手段； 您将合格性检查结果存储在可访问的位置； 您遵循已建立的流程来解决报告的不符合项； 您至少每年检查一次每个基线，并在需要时进行更新。			

补丁与更新	1	**您是否识别并修补易受攻击的组件？**			
		您具有组件的最新列表，包括版本信息； 您定期查看公开资源中与组件相关的脆弱点信息。			
	2	**您是否遵循既定流程来更新技术堆栈的组件？**			
		该过程包括第三方修补程序的供应商信息； 该过程考虑了外部来源以收集有关零日攻击的信息，并包括适当的风险缓解步骤； 该过程包括有关确定组件更新优先级的指南。			
	3	**您是否定期评估组件并审查补丁的状态？**			
		您更新组件和版本的列表； 您根据现有的 SLA 识别并更新缺失的更新； 您根据执行修补程序人员的反馈意见来审查和更新流程。			
运营管理			**回答**	**面试笔记**	**评级**
数据保护	1	**您是否根据对在每个应用软件上存储和处理数据的保护要求来保护和处理信息？**			**0.00**
		您知道每个应用软件处理和存储的数据元素； 您知道每个已识别数据元素的类型和敏感性级别； 您可以进行控制以防止未经净化的敏感数据从生产传播到较低的环境。			
	2	**您是否维护数据目录，包括：类型、敏感度等级、及处理和存储的位置？**			
		数据目录存储在可访问的位置； 您知道哪些数据元素受特定法规约束； 您具有在整个生命周期内保护和保留数据的控制机制； 您对数据有保留要求，并在相关保留期结束后及时销毁备份。			
	3	**您是否定期审查和更新数据目录以及您的数据保护策略和过程？**			

		您具有自动监视功能，可以检测出企图或实际违反数据保护政策的情况； 您具有用于防止数据丢失、访问控制和跟踪、异常行为检测的工具； 您定期审计自动化机制的运行情况，包括备份和记录删除。		
系统退役和旧版本管理	1	**您是否标识并删除不再使用的、已达到使用寿命的、不再被积极开发或支持的系统、应用软件、应用软件依赖项或服务？**		
		您不使用不受支持的应用软件或依赖项； 您对每个产品和客户用户组，管理相关客户和客户用户组从旧版本产品的迁移情况。		
	2	**在停用未使用的系统、应用软件、应用软件依赖项或服务时，您是否遵循既定流程以删除所有相关资源？**		
		您在可访问的位置记录对产品所有发行版本的支持状态； 该过程包括对已到期的第三方应用软件或应用软件依赖项的替换或升级； 运行环境中不再包含被遗弃的帐户、防火墙规则或其他配置文件。		
	3	**您是否定期评估每个软件资产和基础架构组件的生命周期状态和支持状态，并估计其使用寿命？**		
		您的“使用寿命终止管理流程”已达成共识； 您将产品时间表通知客户和用户组，以防止服务或支持的中断； 您至少每年检查一次该过程。		

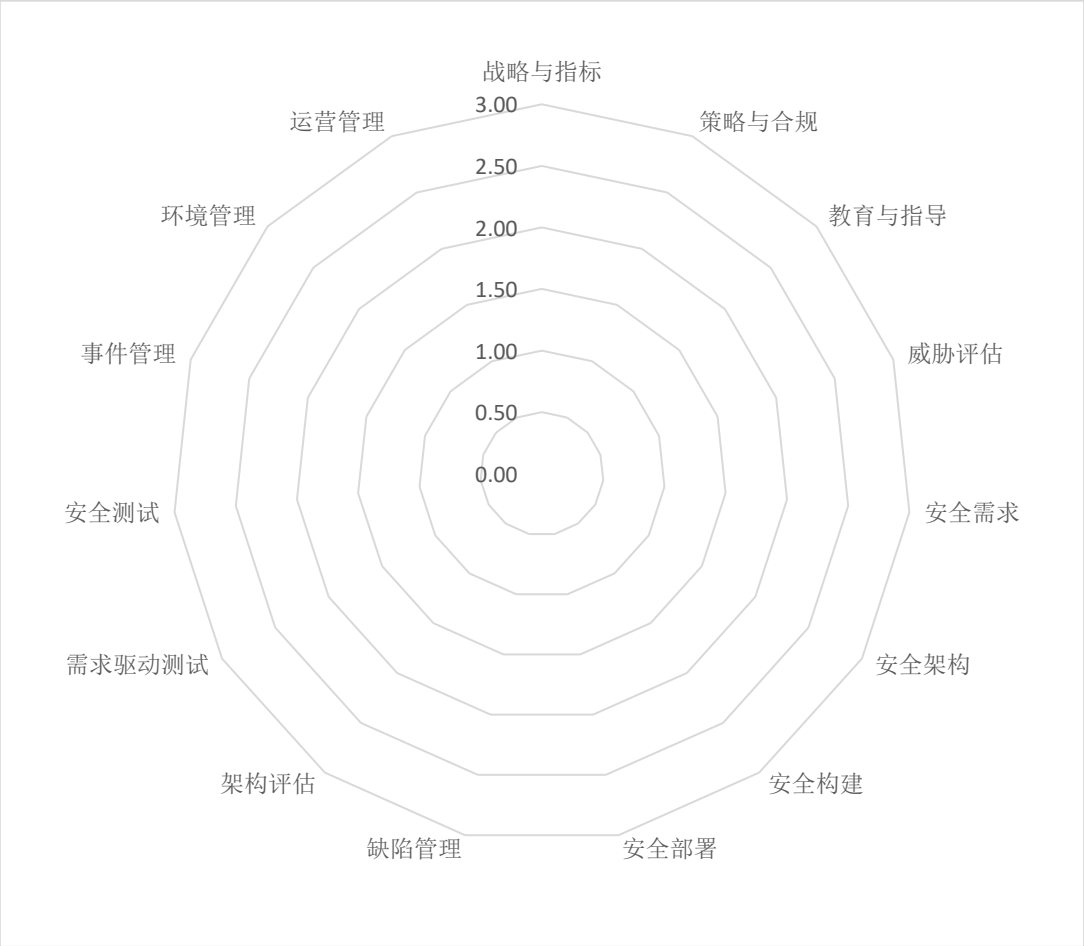
访谈记分卡

下述记分卡用于组织在执行访谈工作时记录得分情况。一般而言，组织在 SAMM 执行过程中分成 4 个阶段，即，在一段时间内执行 4 次访谈，以评估组织的成熟度发展情况，最后获得组织的成熟度发展路线图。

成熟度得分					
			成熟度		
业务功能	安全措施	当前	1	2	3
治理	战略与指标	0.00	0.00	0.00	0.00
治理	策略与合规	0.00	0.00	0.00	0.00
治理	教育与指导	0.00	0.00	0.00	0.00
设计	威胁评估	0.00	0.00	0.00	0.00
设计	安全需求	0.00	0.00	0.00	0.00
设计	安全架构	0.00	0.00	0.00	0.00
开发	安全构建	0.00	0.00	0.00	0.00
开发	安全部署	0.00	0.00	0.00	0.00
开发	缺陷管理	0.00	0.00	0.00	0.00
验证	架构评估	0.00	0.00	0.00	0.00
验证	需求驱动测试	0.00	0.00	0.00	0.00
验证	安全测试	0.00	0.00	0.00	0.00
运营	事件管理	0.00	0.00	0.00	0.00
运营	环境管理	0.00	0.00	0.00	0.00
运营	运营管理	0.00	0.00	0.00	0.00

业务功能	当前
治理	0.00
设计	0.00
开发	0.00
验证	0.00
运营	0.00

成熟度得分



成熟度得分

		治理	设计	开发	验证	运营
治理	**战略与指标**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
治理	**策略与合规**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
治理	**教育与指导**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
设计	**威胁评估**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
设计	**安全需求**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
设计	**安全架构**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**

开发	安全构建	0.00	0.00	0.00	0.00	0.00
开发	安全部署	0.00	0.00	0.00	0.00	0.00
开发	缺陷管理	0.00	0.00	0.00	0.00	0.00
验证	架构评估	0.00	0.00	0.00	0.00	0.00
验证	需求驱动测试	0.00	0.00	0.00	0.00	0.00
验证	安全测试	0.00	0.00	0.00	0.00	0.00
运营	事件管理	0.00	0.00	0.00	0.00	0.00
运营	环境管理	0.00	0.00	0.00	0.00	0.00
运营	运营管理	0.00	0.00	0.00	0.00	0.00

成熟度路线图

受篇幅影响，本文档不提供成熟度路线图的模板。读者可访问 OWASP 中国网站的 OWASP SAMM 项目站点下载模板文档（含：《访谈记录表》、《访谈记分卡》、《成熟度路线图》等）。

致谢

1. 全球项目领导团队

感谢 OWASP SAMM 项目负责人对《OWASP SAMM 2.0》文档编制工作的领导：

- Seba Deleersnyder
- Bart De Win

2. 中文项目翻译人员

感谢 OWASP 中国成员对《OWASP SAMM 2.0》中文版文档翻译和编制工作的开展：

- 王颉

由于中文项目翻译人员水平有限，存在的错误敬请指正。如有任何意见或建议，可联系我们。邮箱：project@owasp.org.cn

3. 中文项目赞助

开源网安 SECZONE GROUP

扫一扫
关注 OWASP 中国