Gartner

Gartner IT领导者

使用信息安全项目成熟路线图，保护企业商业资产

提高信息安全项目安全能力和有效性所必需的关键组成部分有哪些？

越来越多的企业高管都开始意识到，信息安全问题可能会对企业造成不可修复的损害，因此信息安全的重要性也随之迅速提升。到2023年，30%的首席信息安全官 (CISO) 将以“为业务部门创造的价值”作为其业务绩效的直接评估标准。

因此，安全与风险管理领导者必须制定和实施信息安全愿景，而该愿景需要既能大规模创造数字价值，又能切实管理安全风险。然而，提高信息安全能力及其有效性的关键在于成熟的框架，且该框架能够根据内外部各种因素来计划、建立、报告和修改信息安全活动。

如果企业机构缺乏信息安全项目，那么其信息安全活动将不过是众多技术性实践的单纯集合，不能系统地解决信息安全风险和施以相应的对策。

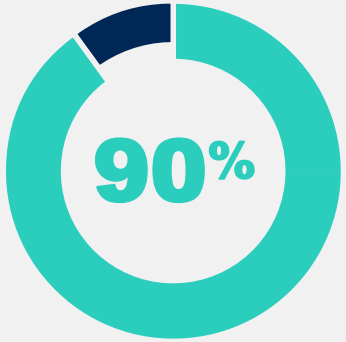
成熟的信息安全项目由七个部分组成，可高效满足企业机构的目标。

如何调整信息安全项目以应对新一代威胁？

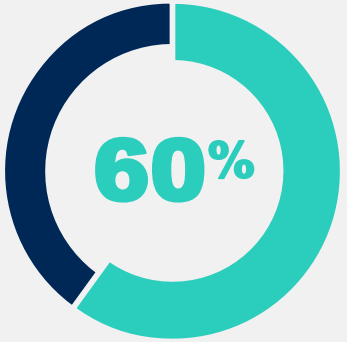
成熟的信息安全项目是由政策、流程和架构实践组成的强大的治理集合，它提供了：

- 用户、系统和配置活动的边界
- 针对设计、实施和运营的指导

成熟的信息安全项目必须能够适应新一代威胁及其给企业机构带来的风险，并满足业务部门的需求和要求。信息安全项目的开发需要时间，需要具备可高度演进，能够针对变化进行自我调整的特性。而达到这种成熟度水平的信息安全项目需要整个团队的共同努力。首席信息安全官（CISO）必须意识到，作为具体技能的使用者，销售、市场和其他业务部门的负责人都是其重要的合作伙伴。而且，安全风险往往大规模发生在IT之外的部门。



董事会对安全和风险管理的关注度越来越稿，90%的安全和风险管理领导者在过去一年中至少向其董事会汇报过一次信息安全问题。



到2024年，60%的CISO将与销售、财务和市场等关键部门的领导者建立重要的伙伴关系。

来源：Gartner

成熟的信息安全项目需要解决的一些重要问题：

1 实施和维护信息安全项目的流程是怎样的？

2 信息安全项目的组成部分有哪些？

3 如何使用商业语言传达信息安全的价值？

主要包括哪些关键步骤？

通过与已成功实施信息安全项目的客户的沟通互动，Gartner从中整理出了最佳实践洞察。路线图则展示了实现目标和预期成果的优先顺序，可用于协调所有利益相关方。

下面将重点介绍一些关键步骤和相关的Gartner资源样本，更多细节请参阅完整版路线图。

战略计划

确定信息安全计划和预期的关键成果

措施：

- 了解关键业务重点，确定项目的使命、愿景；明晰业务、技术和威胁的驱动因素。
- 明确项目的目标和价值，确定关键利益相关方的角色和职责。
- 根据企业机构战略制定安全控制措施，并映射到标准化的安全框架中。

+ 更多

Gartner提供的资源包括：

- 研究报告：2021年领导力前瞻：安全与风险管理
- 研究报告：安全与风险管理IT Score评价模型
- 研究报告：信息安全控制映射工具
- 分析师问询：确定项目的目标和价值，以及关键利益相关方的角色和职责

+ 更多

评估项目

评估项目的当前状态和创建路线图

任务：

- 评估现有系统、员工、流程、工具、技术、用户意识、以及与第三方的互动情况。
- 进行当前项目的成熟度基线评估，确定目标状态和进行差距分析。
- 利用审计结果，制定与项目目标一致的战略草案和设计各重要阶段；获得利益相关方的反馈。

+ 更多

Gartner提供的资源包括：

- 电话咨询：介绍GartnerBuySmart™流程，审查战略、财务和技术要求，确定需要支出管理的领域
- 分析师问询：设计安全架构、政策框架和解决方案层，并讨论出更多的安全功能性评估方法

+ 更多

制定战略

制定战略文件并开始初步实施

任务：

- 明确信息安全团队所需的角色及其职责，如承担责任、提供咨询和发出通知。
- 培养与信息安全相关的重要能力，以及需要和当下缺少的技能。
- 使用衡量指标和激励措施来推动各利益相关方共同承担相关责任。

+ 更多

Gartner提供的资源包括：

- 研究报告：向董事会提交状况报告的规则
- 分析师问询：确定和建立战略伙伴关系，明确供应商，并讨论出更实用的安全评估方法

+ 更多

进行沟通

通过沟通，获得利益相关方的支持

任务：

- 获得执行决策权、资源支持以及执行董事会的认可。
- 升级现有报告方法和应对措施；制定发生网络漏洞后的沟通计划。
- 对照关键指标评估项目进展情况；传达项目迄今为止所产生的价值。

+ 更多

Gartner提供的资源包括：

- 电话咨询：制定企业机构和董事会关于价值交付的沟通计划
- 现场研讨会：向员工灌输安全行为文化；定制相关的培训和意识提高活动
- Gartner IT Symposium/Xpo™会议

+ 更多

再次评估、优化改进

再次评估项目，进行跟踪和优化

任务：

- 确定项目结构，监测和对抗高级威胁
- 建立逆向恶意软件工程、搜寻原因和来源确定等方面的能力；确定威胁发生的原因和来源
- 再次进行项目成熟度评估，并进一步优化

+ 更多

Gartner提供的资源包括：

- 电话咨询：讨论有助于进一步优化企业机构网络安全就绪程度的关键问题
- 分析师问询：培养逆向恶意软件工程、搜寻原因和来源确定等方面的能力；确定威胁发生的原因和来源
- 研究报告：如何有效搭建网络安全和技术风险演示模型

+ 更多

涉及哪些利益相关方？

数字化业务最成功的企业组建了现代化项目跨部门团队。下图为Gartner建议应参与进信息安全项目的职能部门和角色，可有助于企业顺利完成项目各阶段的目标。

CISO

领导网络安全战略和项目的制定，并确保其与业务战略和目标保持一致。指导进行项目评估、制定项目行动计划和执行项目，并在整个企业机构内沟通战略和项目进展，与关键利益相关方合作实施项目。

CIO

与企业机构领导者合作，指导设立信息安全项目和培养数字能力。确保信息安全项目与业务战略和目标保持一致。在整个企业机构内传达任务、战略和目标。

技术专家团队

评估企业业务环境中的运营、战术和技术情况，在运营层面设计、实施和执行信息安全政策和治理。根据需求提高技能。

应用和软件工程领导者及其团队

CISO的关键合作伙伴。协助实施和操作信息安全计划和业务中的关键内容。

企业架构和技术创新领导者及其团队

与CISO和关键利益相关方合作，确保尽早了解信息安全要求。

基础设施和运营领导者及其团队

CISO的关键合作伙伴。协助实施和操作信息安全计划和业务中的关键内容。

安全和风险管理领导者及其团队

与CISO合作，将网络安全纳入企业机构内所有的治理、风险和合规项目与流程中。

项目和组合管理/PMO领导者及其团队

利用战略伙伴关系，进行适应性的项目协调和交付、资源管理、风险缓释和有效的组织管理，从而满足CISO的要求。

客户成功案例：提高安全风险管理水平，实现数字化增长

关键任务

客户的目标是培养更成熟的信息安全能力，以保护业务安全并实现数字增长，同时在风险管理、运营精简和成本效益之间取得适当的平衡。

Gartner服务

Gartner专家提供了一种方法和参与策略，可帮助风险团队更深入地了解业务的驱动因素，传达网络风险带来的业务影响。与此同时，在整个企业机构内就信息安全的商业价值达成一致。

Gartner专家还利用了Gartner风险管理框架，重点关注业务方面和建立综合风险管理战略的关键绩效指标。

项目成果

在Gartner的支持下，该客户能够：

- 大大提升业务部门对信息安全项目投资如何支持实现关键业务目标的理解
- 将业务风险和绩效管理项目与信息安全风险管理项目联系起来
- 提高业务部门对安全治理的持续参与度
- 将执行层面的安全指标从纯粹的运营指标转化为战略业务成果指标

可行的客观洞察

探索其他的网络安全免费资源和工具：

路线图

网络安全IT路线图

遵循最佳实践，制定弹性敏捷、可扩展的网络安全战略。

电子书

2022年领导力前瞻—安全风险管理领导者

了解2021年安全与风险管理领导者应该关注的新兴趋势、预期挑战和后续措施。

电子书

新兴风险应对工具包：网络风险

评估您的网络安全风险状态，您可使用该工具包加快风险处理的速度。

网络研讨会

中国云安全的最佳实践

安全与风险管理主管获得企业机构对其安全意识项目的支持的三种方法。

访问本系列中的其他路线图：

《云迁移IT路线图》

优化路线图以提高数据治理的有效性

已经是Gartner客户？
您可在客户门户网站上获得更多的资源。登录

了解更多。

获得可行的客观洞察，以实现您最关键的优先事项。Gartner专家指南和工具使您能够做出更快、更明智的决策并获得更优的业绩表现。联系我们成为客户：

成为客户

点击了解更多关于Gartner IT领导者的相关信息
https://www.gartner.com/cn

您可扫描以下二维码，关注Gartner官方微信公众号：

Gartner