Gartner IT 领导者

CISO 上任首个 100 天的行动指南

分析师：William Candrick、Sam Olyaei、Tom Scholtz

Gartner

CISO 上任首个 100 天的行动指南

发布日期：2021 年 5 月 24 日 - ID G00747118 - 阅读全文约需 20 分钟

分析师：William Candrick、Sam Olyaei、Tom Scholtz

项目：安全与风险管理领导者

> 担任首席信息安全官（或同等职务）的前 100 天，将决定你是否可以作为安全与风险管理领导者取得成功。为此，Gartner 将通过本研究提供相关的指导和支持，帮助新任 CISO 在这个关键的过渡阶段取得最大的成功。

概述

主要发现

- 成功的首席信息安全官（CISO）是领导者、管理者和沟通者，而不是技术人员。
- CISO 的成功取决于是否能够实现以下两个重要成就：（1）建立个人信誉和领导力品牌，以及（2）为防御安全项目奠定基础。
- 如果新任 CISO 不能理解领导层的期望或不能有效传达安全项目如何支持业务成果时，他们就会陷入困境。

建议

任期内的首个 100 天，CISO 应该：

- 将你的领导要务与业务成果及目标联系起来，加强网络安全项目与业务项目的关系。
- 在深入研究技术细节和进行技术决策之前，先制定一个安全战略。
- 确定你可以在 CISO 任期内前 100 天完成两到五个优先事项，这将最大限度地提高你的成功机会。
- 在不可预测的安全事件发生之前，为其留出更多处理时间，避免延误战略项目。
- 分享战略愿景，展示员工融入该愿景的方式并避免公开批评前任 CISO，从而赢得安全团队的支持。

导语

在担任 CISO 的前 100 天，你将有机会确定自己的角色和职业关系。你可以在这段短暂的“蜜月期”内制定战略、与其他高管建立关系、获得领导层的支持、与新团队建立信任以及展现你的领导风格。如果这时贵企业需要对网络风险治理开展重大改革，或者需要大幅提高安全项目的成熟度，那么这个机会就显得尤为宝贵。

本研究将主要探讨杰出的 CISO 充分利用这 100 天的具体方法。另外，我们将这 100 天分成了六个阶段，它们分别是：准备阶段、评估阶段、规划阶段、行动阶段、衡量阶段和沟通阶段（图 1）。

图 1：CISO 上任后首个 100 天的路线图

CISO 上任后首个 100 天的路线图

来源：Gartner
747118_C

Gartner

阶段	目标
准备	在上任前，对你的角色进行规划。
评估	了解安全部门的当前成熟度。
规划	为首个 100 天制定路线图。
行动	采取行动，大幅提高成熟度。
衡量	证明安全部门取得的进展。

首个 100 天计划

简而言之，成功的前 100 天计划安排应该：

- 建立你作为 CISO 的信誉，提升安全部门在企业中的内部品牌和形象。
- 确定安全部门当前的成熟度（见安全与风险管理 IT Score 评价模型）。
- 重点关注各战略项目下的细分项目，细分项目应通过合理的方法（如成熟度评估、风险评估等方法）选择并确定优先等级。
- 缩短卓越安全运营和业务价值（如高管的优先事项）之间的差距。
- 确定现实、可衡量、有时限的目标，并设定衡量标准来跟踪这些目标的进展。

下面，本研究将为实现这些目标提供易于操作的指导。

准备阶段（上任前）

在上任前，为你的新角色做好准备，制定好初步规划，从而为成功的开始奠定基础，并为你的 CISO 任期建立需要的职业关系。

准备阶段需要实现的目标成果

在准备阶段，你要以实现下列成果为目标：

- **大致了解**你的角色和你的员工、高层利益相关者和领导团队的期望。

- **制定基本的会面计划**，去认识领导层利益相关者和安全工作人员。

这个阶段的重点是倾听和学习，而不是做决定。在你担任 CISO 的前几周，你应该避免做出大范围的声明或决定。

准备阶段需要采取的行动

在上任之前，你要采取以下行动：

评估贵企业需要的 CISO 类型：在文化、行业、政治挑战和其他因素的影响下，不同的企业对 CISO 有不同的要求。有些企业需要运营型 CISO，有些企业则需要业务型 CISO。为此，Gartner 建议安全与风险管理领导者查阅“CISO 有效性指数”，并根据企业的需求来确定 CISO 类型。

了解贵企业的组织结构：获取组织结构图和运营文件（如流程图），了解安全部门、IT 部门和整个企业的结构，从而了解安全部门在企业中目前的管理和运营角色。

确定关键利益相关者：创建一个你将与之合作的领导层利益相关者名单。这份名单可包括（但不限于）首席执行官（CEO）、首席财务官（CFO）、首席信息官（CIO）、法律总顾问、人力资源（HR）主管、首席隐私官（CPO）和首席风险官（CRO）。

建立新的联系：最好是在你上任前，与领导层的利益相关者和安全人员接触，如发送面试后的感谢信和关注他们的 LinkedIn 账号（带有个性化备注）。

安排首次会议：与行政助理（或企业内部友好联系的人）合作，安排你的首轮会议：计划在第一天召开安全团队全体成员会议，并在第一周与整个企业的关键利益相关者开展一系列会见和会谈。最初几周是一个在企业内进行自我介绍和建立良好形象的好机会。

准备阶段需要开展的沟通

上任前，你的重点应该是了解企业的情况，准备与利益相关者和团队的沟通信息。可以说，最初几周的成功取决于有效的沟通，而不是决策。

上任前，以及上任后的最初几周，你应该关注以下内容：

了解其他高管的优先事项：杰出的 CISO 明白，他们是企业高管，而不仅仅是运营经理或技术专家。因此，要充分发挥你作为 CISO 的潜力，你需要了解企业业务以及高管和董事会最关心的优先事项。所以在上任前，请参考以下信息来源：

- 从企业官网“关于我们”页面上了解公司的使命宣言。
- 阅读最近的公开财务报告（例如，美国上市公司的季报或年报），了解领导层的优先事项和关注点。
- 阅读并观看领导层最近的报道和访谈（并可以关注领导层的社交媒体账户）。
- 确定高管内部的竞争要点，并做好准备带领安全部门应对这些复杂的领导层关系。

自我介绍：准备简短版的简历，涵盖你的个人背景、工作经验以及你对加入该企业的一些想法。然后在介绍和会面时使用这一简历，让所有人都能了解你是谁，来自哪里。但要注意，你在这个过程中，应避免宣布大胆且具有破坏性的决定。相反，你的首要目标应该是赢得同事和团队成员的欢迎。

讲故事：讲故事是改变人们观点、获得认同的一个有效方法。例如，新任 CISO 可以讲一个故事，说明安全部门如何帮助企业快速、安全地发展，而不会为了最大限度地降低风险而拖慢工作进展。另外，你还可以从过去的经验或新闻事件中举例，帮助利益相关者了解安全部门及其领导 CISO，是一种资源而不是障碍。

创建讨论指南：在第一轮见面会之前，准备好相关的问题和谈话要点。例如，你可以考虑使用以下内容：

- **与利益相关者的讨论：**对于这类会议，你的重点应该放在利益相关者对安全部门和 CISO 角色的看法上。在最初的 100 天里收集这些信息将有助于你计划要在未来几个月里实现的变化，包括改变领导层的观点和（重新）定义 CISO 的角色。可以提问的问题包括：
  - 你最紧迫的业务是什么？
  - 你目前对安全部门的看法是什么？
  - 你在与安全部门合作时的最大痛点是什么？
  - 你与安全部门的合作进展顺利吗？
- **与团队成员的讨论：**你可以准备一些问题，从而了解（1）安全治理和运营工作的现状，以及（2）团队成员对团队和工作环境的看法。可以提问的问题包括：
  - 你的大部分工作时间都在做什么？
  - 怎样才能使你的工作更容易完成？
  - 对你最有挑战性的事情是什么？
  - 我怎样才能更好地支持你和你的团队？
  - 你认为安全部门的首要优先事项应该是什么？
  - 你认为企业的首要目标是什么？

准备阶段需要使用的资源

你可以从阅读以下 Gartner 资源开始。

Gartner 研究与工具

《CISO 有效性路线图》——根据杰出 CISO 所提供的经过验证的最佳实践来定制你的领导方法。

《培养当代 CISO 技能》——确定和培养技能，发展成为一位全面、有能力的 CISO。

《CISO 有效性：影响 CISO 有效性的行为和思维方式报告》——确定与 CISO 有效性最密切相关的行为和思维方式。

评估阶段（第 1-4 周）

评估安全项目当前的成熟度和表现。高质量的安全评估会展现出安全项目的差距，为战略规划提供信息。因此，成功的 CISO 应该依靠客观评估，而不是直觉，做出合理、可重复且经过验证的安全决策。

评估阶段需要实现的目标成果

评估阶段，你要以实现下列成果为目标：

- 找到一位帮助你深入了解企业文化的**高管导师**。
- 了解你的**可用资源**，包括资金、人员和技术。
- 开展正式的成熟度评估、团队对话和利益相关者互动，找出**一系列安全差距**。
- 确定**三到五个战略优先事项**，解决安全差距问题并与业务成果保持一致。

评估阶段需要采取的行动

在任职的第一个月，你要采取以下行动：

寻找一位高管导师：在这个阶段，你最珍贵的一份资产就是一位高级别的导师。这位导师需要深入了解企业高级管理人员的内部运作，但可以不必了解安全领域的相关知识。因为如果他/她对安全领域所知不多，那么他/她就能切实客观地评估你的提案和领导能否被接受，也就能更好地服务于你。

确定安全部门的角色和责任：你担任 CISO 的首要任务就是说明和确定安全部门的角色和责任。为此，你需要与你的经理进行讨论，全面了解安全部门以及你的角色。你可以考虑阐明在以下领域的角色和责任：

- 物理安全
- 业务连续性和灾难恢复（BC/DR）
- 隐私
- 合规
- IT 风险
- 风险治理
- 安全运营

对于安全职权范围以外的领域，你需要与其他高管和领导者（例如，企业风险管理主管、首席隐私官、法律总顾问）建立工作关系。

清点你的信息来源：迅速清点你管理的安全部门所需的信息来源。例如，找到任何现有的政策、组织结构图、战略计划、当前项目、技术路线图和指标。然后，你可以使用这些信息来说明你对安全部门的现状和近期计划的理解。

开展成熟度评估：为安全部门的工作人员创造一个安全的环境，让他们坦诚地评估本部门的成熟度。这些评估会展现出差距，为前瞻性的战略制定提供信息，且不会“秋后算账”。作为新任 CISO，你至少应该开展以下核心评估，如果可能的话，还可以考虑增加其他评估。

首个 100 天应该开展的核心评估：

- 职能部门成熟度评估：评估安全部门的能力和流程成熟度。为此，你可以使用 Gartner 安全与风险管理 IT Score 评价模型。
- 控制措施成熟度评估：评估安全控制措施的成熟度。为此，你可以使用 Gartner 控制措施成熟度基准服务。
- 风险评估：评估与整个企业的应用程序和基础设施相关的信息风险。风险评估应优先考虑风险最高的领域，在任何现有风险登记册中收集到的信息都有可能帮助你评估贵企业的风险状况。

其他评估：

- 审计结果
- 漏洞评估
- 威胁评估
- 人才评估
- 监管结果
- 渗透测试
- 网络钓鱼测试

确定你的首要战略要务：评估后将揭示安全项目中存在的差距。因此，你可以利用这些差距来确定能够在最初的 100 天里解决的三到五个战略要务。这些要务应解决基本的挑战，并给安全团队和高级领导层留下积极印象。

这些要务可以包括：

- 使安全项目成功所需的基本要求
- 与业务成果建立明确的联系
- 为长期的成熟度改进工作奠定基础
- 建立你作为高效 CISO 和公司管理者的可信度

评估阶段需要开展的沟通

评估安全部门的现状非常具有挑战性。例如，一些安全部门工作人员可能会把差距降到最低，因为他们处于戒备状态，或者喜欢以最好的方式呈现事情。还有一些安全部门工作人员可能会夸大差距，以便为他们所谓的重要任务获得投资和支持。但你要记住，这些都是人们的正常倾向行为，可以通过创造一个开放、安全和透明的沟通环境来防止其发生。

因此，你要重点关注以下沟通机会：

- **团队领导会议：**与安全团队领导者举行一对一会议。了解他们对安全项目现状的意见，并明确每个领导者在制定未来几周、几个月和几年的安全执行战略中起到关键性的作用。
- **利益相关者访谈：**采访利益相关者，了解他们对安全部门的看法。这些利益相关者可以包括法律总顾问、首席隐私官、首席信息官、首席审计官和人力资源主管。
- **确定意见领袖：**在你与整个企业的领导人会面时，请注意那些能够推动安全要务、给你个人授权，并帮助你与高层和董事会沟通的高级意见领袖。

评估阶段需要使用的资源

你可以从阅读以下 Gartner 资源开始。

Gartner 研究与工具

安全与风险管理 IT Score 评价模型——评估安全部门的流程和能力成熟度。

控制措施成熟度基准服务——与你的同行进行技术控制措施成熟度的比较。

规划阶段（第 3-6 周）

规划阶段可汇总你的评估信息，并制定成行动蓝图。你的初步规划为你的前 100 天制定了路线图，指导你在第一年的工作中取得安全方面的成功。

规划阶段需要实现的目标成果

规划阶段，你要以实现下列成果为目标：

- 制定**书面战略计划**，为第一个 100 天确定两到三个重要的安全项目，并为第一年任期制定一个大概的路线图。

- 制定**运营预算**，确保有足够的资源来实现这些重要任务。如果资源缺乏，你应该相应调整战略计划，促使其实现。

规划阶段需要采取的行动

在规划阶段，你要采取以下行动：

选择几个首要任务：查看你的首要任务，并选择在未来三个月内需要重点关注的两到三个事项。为此，你可以使用以下标准来筛选出首要任务：

- 该项目能否在三个月内实现？
- 你是否有相应的行政支持、资源和预算？
- 该项目是否与降低网络风险有关？
- 失败的风险是否相对较低？

当你选定后，你就可以帮助业务领导者了解这些安全要务对业务成果的支持作用。越早让他们了解安全要务对业务成果的支持作用，那么在战略要务实现时，你和安全部门就能获得越高的信誉度。

设计或完善安全部门：你需要根据你的任务、首要任务和企业文化来构建安全部门。但遗憾的是，在安全部门的设计问题上并没有万能的方法。在设计安全部门时，你需要明确角色和职责，为管理人员授权并划分相应的责任，并与其他部门（例如，IT、隐私、法律部门）建立明确的关系。

制定运营预算：你对安全预算的控制程度取决于你加入企业的时间（财年初、财年中或财年末）和当前的预算编制程序。虽然在最初的 100 天里，预算编制的某些方面可能并不灵活，但你应该确保运营预算能够支持你的战略要务。你也可以考虑重新分配资源以支持首要任务。

规划阶段需要开展的沟通

制定书面安全战略计划：首个 100 天战略计划应包括三个部分：

1. 项目愿景（“我们想要实现的目标”）。

2. 成熟度评估结果（“我们目前的位置”）。

3. 差距分析和战略要务（“我们将如何达到目标”）。

建立安全项目愿景：信息安全项目需要一个清晰、简明的愿景声明，阐述安全部门的高级别任务和目标，并且应该与你的团队、管理层和相关利益相关者分享。

规划阶段需要使用的资源

你可以从阅读以下 Gartner 资源开始。

Gartner 研究与工具

《信息安全战略规划启动指南》——根据我们的详细指导创建一个战略计划。

《安全策略规划最佳实践》——制定一个可操作、能够建立信誉并获得支持的战略计划。

《安全投资组合优先次序：为安全投资决策增加严谨性》——设计一个可重复的合理方法，以确定内部安全项目的优先次序。

《工具包：一页纸信息安全战略——解构》——创建能够引起高管共鸣的单页战略文件。

行动阶段（第 5-12 周）

行动阶段应提高企业的安全能力。因此在最初的 100 天里，你的行动应该集中在可量化的显著成就上，从而建立你个人的信誉并提高安全部门在企业中的地位。最初的成功可以确保获得更多支持，为更多成功奠定基础，从而为你和你的团队创造一个改进和成功的良性循环。

行动阶段需要实现的目标成果

行动阶段，你要以实现下列成果为目标：

- 与安全管理人员、工作人员和团队举行一系列会议。
- 为每个安全要务指定一个项目负责人。
- 制定安全预算，确保有足够的资源来实现这些战略要务。
- 制定一份有形、可衡量的项目结果清单，展示你的战略目标进展。

行动阶段需要采取的行动

在行动阶段，你要采取以下行动：

完善角色和责任：首先，你要确保所有安全管理人员都有明确的角色和责任。明确每个安全管理人员的职责，以及评估其表现的方法。其次，你要确保所有级别的安全人员都有明确的工作描述和职责，清楚表明每个员工的实际工作。请注意，工作描述和绩效管理指标往往与工作实际完成情况不同，这一点应该在你的领导下得到纠正。

记住，安全管理人员可以帮助他们自己和他们的团队明确角色和责任。而作为 CISO，你应该监督这项工作，但不要觉得你必须自己完成所有的管理任务。

指派项目负责人：你的每一个战略重点都应该有一个正式的项目负责人。为此，你要为每个项目都设立明确的计划、期望和结果，并与各位项目负责人说明相关内容。尽可能降低项目失败风险的一个方法是建立多个项目目标，避免非黑即白的结果（成功或失败）。

确保获得领导层的支持：利用你的战略计划和安全愿景，让领导层参与进来，为你的首要任务争取支持。领导层的支持将给你和你的团队提供权限，从而确保你获得相应的资金，影响利益相关者和激励安全团队。

建立安全治理流程和论坛：开始在整个企业内建立有效的信息风险治理。这需要确定风险决策权、风险问责制和企业利益相关者的信息风险责任。作为新任 CISO，你最大的一个挑战可能就是培养正确的风险责任意识和决策方法。

调整必要的预算：如有必要，你可以调整预算，支持你的战略要务。你现在的首要任务是确保在未来三到六个月内有足够的资金和资源。当然，现在也是开始规划下一财年预算的好时机。作为新任 CISO，你可能会获得相当大的善意和余地来重新分配资金，甚至获得更多资源。但是请记住，你的初始预算可能会成为未来几年的比较基准，所以要确保你的预算结构能够支持长期路线图。

行动阶段需要开展的沟通

宣传你的战略计划和愿景：向企业领导层和利益相关者介绍你的战略计划和愿景。在宣传你的计划时，你需要根据听众来定制信息，比如将你的计划与利益相关者的首要任务联系起来，展现信息安全与企业领导者的首要任务和目标之间的联系。

安排团队和经理检查会议：人员管理是 CISO 职责的一个重要方面。因此，作为管理团队的第一步，你需要在整个安全团队中设立定期会议。特别是要考虑设置以下会议：

- 每周与每个安全经理进行一对一的检查会议。利用这些会议来计划和跟踪项目。经理会议也是一个指导机会，特别是在将业务意识和部门背景知识灌输到日常的安全运营方面。
- 每月或每季度与安全工作人员进行“跨级别”一对一会谈。你可以滚动安排这些会议，这样你就可以每周与多个工作人员会面。这些会议是一个你与员工直接沟通，收集意见并衡量士气的机会。

- 每月安排一次全体员工会议。你应以 CISO 的身份宣布重大事项，表彰表现出色的员工，并向全体成员介绍重要的最新信息。你还可将其作为一个培养机会，选择经理和员工在会议上发言。
- 鼓励设置团队日常会议。安全经理应每天与各自的团队召开会。这些简短的会议（例如在 30 分钟内）可以确定当天的安排，进行问答，促进合作。每日例会对于虚拟团队来说尤其重要，因为这类会议可以取代面对面团队之间的非正式对话。

行动阶段需要使用的资源

你可以从阅读以下 Gartner 资源开始。

Gartner 研究与工具

信息安全演示支持中心——使用“下载并使用”模板来加强你向企业领导层和利益相关者传达的信息。

使用相关工具和模板来提高流程成熟度：

- 《制定安全事件响应计划的启动指南》
- 《设计和启动安全用户计划的启动指南》
- 《信息安全战略规划启动指南》
- 《创建信息安全功能健康仪表盘的启动指南》
- 《建立网络危机测试项目的启动指南》

衡量阶段（第 11-14 周）

衡量阶段能够证明你给安全部门和企业带来的影响。衡量和沟通是一名成功 CISO 的标志，因此应该在你的任期内尽量实现这个目标。

衡量阶段需要实现的目标成果

衡量阶段，你要以实现下列成果为目标：

- **设定一套明确的运营指标**，跟踪安全项目的绩效表现和进展。
- 向利益相关者和领导团队报告**初期进展并提交相关证据**。

- 为各方利益相关者，包括 CIO、风险指导委员会、高管和董事会，**设立会议和报告程序**。

衡量阶段需要采取的行动

确立一套安全指标：创建一组运营关键绩效指标，然后根据业务相关指标调整这些运营指标，从而获得领导层和董事会的认可。最好的业务相关指标包括业务背景指标，以及从技术细节中提取出来的指标。

制定执行报告流程：设定报告频率并确定报告对象，如指导委员会，高管简报和董事会报告（全体董事会和风险委员会）。一旦设定了报告的期望值，你就要花时间了解每个报告对象的期望和首要任务。然后，你要创建与每个报告对象相关的指标和报告，并为安全工作人员建立流程、确定职责，以便定期维护和更新这些仪表盘。

衡量阶段需要开展的沟通

监测计划和项目的进展：跟踪安全项目进展和项目成熟度的变化。向领导层报告进展情况，并趁势制定商业案例，以继续获得（或获得更多）所需的资金和支持。指导安全经理和项目负责人用与业务相关的术语来说明安全项目。你的领导团队应该能够简明扼要地解释安全项目的优先级是如何划定的，以及它如何支持业务目标。

强调初期成功和挑战：交流成功经验，并在挑战出现时制定解决方案，以此来保持你的成功势头。请记住，大多数安全项目都应设有多个目标（有些较小，有些较大），即使有些目标被推迟或错过，其他目标也有实现的可能。

衡量阶段需要使用的资源

你可以从阅读以下 Gartner 资源开始。

Gartner 研究与工具

《为什么要为安全与风险管理开发平衡计分卡》——使用平衡计分卡，向领导层传达与业务相关的指标。

《工具包：开发安全平衡计分卡》——该工具下载即可使用，可快速创建安全平衡计分卡。

《安全衡量标准的五个必要特征》——设计满足最佳实践的衡量标准。

《工具：简单的 NIST CSF 管理仪表盘》——开发一个安全管理仪表盘，反映行业标准（如 NIST 网络安全框架），并获得企业高级领导者的认可。

作者推荐

根据您当前的订阅情况，部分文件可能无法查看。

《CISO 有效性路线图》

《安全策略规划最佳实践》

《安全与风险管理 IT Score 评价模型》

《安全与风险领导者必须回答的五个董事会问题》

阶段	目标
准备	在上任前，对你的角色进行规划。
评估	了解安全部门的当前成熟度。
规划	为首个 100 天制定路线图。
采取行动	采取行动，大幅提高成熟度。
衡量	证明安全部门取得的进展。

可信赖的洞察

确保网络安全职能部门获得成功所需要的准备，了解以下为安全与风险领导者提供的其他免费资源和工具：

信息图

《使用信息安全项目成熟路线图，保护企业商业资产》

确保你的安全部门能够应对当前新挑战。

下载信息图

电子书

《响应网络安全事件的3个必备工具》

立即制定一个网络安全响应计划。

即刻下载

电子书

《高效能CISO领导力的四大使命》

了解优秀的网络安全领导者如何应对职责范围扩大所带来的挑战。

即刻下载

网络研讨会

中国数据安全治理解析

为 CISO 和数据安全领导者提供有关数据安全治理实施的见解和指导。

报名观看

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

Gartner

联系我们

获得容易操作的客观洞察，实现您的关键任务。Gartner 专家指南和工具使您能够做出更快速、更明智的决策，并获得更优业绩表现。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

gartner.com/cn

您可扫描以下二维码，关注 Gartner 官方微信公众号：

Gartner