RSA® ARCHER® IT & SECURITY RISK MANAGEMENT

解决方案概要

简介

组织通过构建一层又一层的防护来应对不断增长的安全挑战：防火墙、防病毒、入侵防护系统、入侵检测系统、漏洞扫描程序、安全策略、身份管理以及物理访问控制等等。虽然这些层对于针对当今威胁提供基本防御和保护必不可少，但是每个层也增加了安全基础架构的复杂性级别。由于复杂性不断增加，因此更加难以清楚地协调出现安全风险的地方以及威胁成形的速度。

除了必须要保护本来就已经不堪重负的海量业务数据，安全职能部门还面临着由于这些防御层产生的安全相关数据不断增长所带来的挑战。如果不能充分地了解哪些数据对于业务而言最重要，IT 和安全团队就很难确定哪些安全事件最相关。

当今技术转变对安全的影响日益加深，最显著的就是业务元素迁移到云中和外部提供商环境中。随着公司将更多业务关键型流程和 IT 服务迁移到公司外部，安全控制严重依赖外部相关方（即使不是完全依赖）。向第三平台的迁移提高了满足安全和法规遵从性要求的难度。

当今不断变化的威胁和事件让高管越来越关心组织如何应对日益增长的网络风险。高管比以往任何时候都更加关注安全风险 — 声誉受损、财务影响和违反法规以及调查和解决数据泄露或其他安全事件的净成本。

深入洞察 IT 和安全性

为了让 IT 风险和安全职能部门编制并呈现完整的技术相关风险视图，多个运营团队必须协作并协调工作。安全策略必须与法规和业务要求保持一致。威胁和漏洞管理流程必须足够敏捷，可以抢先应对不断增长的威胁。安全运营团队必须积极主动，辛勤工作，才能迅速识别针对组织的主动攻击并保护处于风险之中的资产。安全战略团队必须透过即时战术审视全局，引入经济高效的创新解决方案。最后，安全法规遵从性团队必须确保设计合适的控制措施并有效地执行。

RSA ARCHER IT & SECURITY RISK MANAGEMENT 的优势

借助 RSA® Archer® IT & Security Risk Management，您的安全职能部门可以从经过改进的可见性、分析、操作和指标中受益。

在 GRC 背景中关联网络安全风险

由于当今的业务流程彼此互连，组织必须能够有效地解决快速变化的网络安全风险的复杂性和一连串影响。RSA Archer 可以将您的安全流程和数据与企业内部的风险和法规遵从性职能部门相关联。之后，IT 和安全风险职能部门可以从业务关键性角度考虑业务风险与 IT 风险之间的关系，从而建立所有权和问责制并将 IT 和安全风险与更加广泛的治理、风险和法规遵从性计划相关联。

从多个维度进行 IT 和安全风险管理

要有效地管理 IT 和安全风险，您必须通过组织安全计划来管理一系列 IT 安全风险。您的 IT 和安全风险计划必须从多个维度— 从策略、标准和法规遵从性到威胁、漏洞和攻击 — 展开风险管理 。RSA Archer 支持 IT 和安全团队集中管理流程、划分网络威胁优先级并从容地应对最新威胁。

将业务背景与流程支持关联起来

如今，管理 IT 和安全风险涉及到的远不止数据速度和馈送。必须从业务的角度了解 IT 风险，因为技术问题可能会将整个组织置于严重的风险之中。通过确保业务与 IT 之间相一致，IT 和安全风险管理计划可以促进需要解决的问题，保持业务的安全性。RSA Archer IT & Security Risk Management 通过建立流程来有效且高效地识别和升级风险，填补了人员与技术之间的空白。

RSA ARCHER IT & SECURITY RISK MANAGEMENT

在如今复杂的业务环境下，新兴的 IT 和安全威胁无处不在。通过 RSA Archer IT & Security Risk Management，您可以确定哪些资产对您的业务至关重要，建立并传达安全策略和标准，检测并应对攻击，识别并修补安全缺陷以及制定清晰的 IT 风险管理最佳做法。

RSA Archer IT & Security Risk Management 提供了多种使用情形，可满足您在风险管理成熟之旅中的特定业务需求。

问题管理

RSA Archer Issues Management 适用于任何安全性、风险或法规遵从性相关使用情形，可捕获并整合源自安全事件的问题、失败或者缺少的内部控制措施以及需要关注或上报的例外情况。Issues Management 支持组织为内部和外部审核结果、法规检查问题和管理自我识别的问题编制目录；确立解决问题的问责制并根据承诺和到期日跟踪补救计划。强大的报告功能让所有级别的管理层和董事会可以轻松地全面了解未解决的问题、优先级和补救时间表。

IT 和安全策略计划管理

RSA Archer IT & Security Policy Program Management 可以帮助您记录外部法规义务并建立系统化审核和批准流程以跟踪对这些义务的变更，从而了解业务影响并确定响应的优先级。

IT 控制措施保证

RSA Archer IT Controls Assurance 支持评估和报告控制措施在所有 IT 资产之间的效果并自动执行控制措施评估和监控。您可以实施一个集中式系统，为 IT 资产编制目录以提供法规遵从性报告，并建立一个记录 IT 控制措施的记录系统。借助经过简化的 IT 控制措施测试流程和工作流，您可以为手动控制措施部署标准化评估流程，并整合来自自动化系统的测试结果。系统会集中管理在法规遵从性评估期间发现的问题，让您可以跟踪并报告法规遵从性差距。可以记录并监控针对差距所采取的补救措施，以确保及时地消除法规遵从性差异。

IT 安全漏洞计划

RSA Archer IT Security Vulnerabilities Program 采用大数据方法来帮助安全团队识别高风险威胁，并对这些威胁进行优先级排序。您可以通过综合运用资产业务环境、可作为行动依据的威胁情报、漏洞评估结果和全面的工作流来主动管理 IT 安全风险。可以结合全面的业务背景来为 IT 资产编制目录，从而更好地对扫描和评估活动进行优先级排序。这个经过整合的漏洞研究平台支持 IT 安全分析团队实施警报、浏览漏洞扫描结果并在出现问题时进行分析。功能强大且灵活的规则引擎会突出显示新的威胁、逾期未解决的问题和不断变化的业务需求。通过将已知漏洞风险与适用的业务背景相关联，有助于对响应和补救工作进行优先级排序，从而加快弥补重大差距的完成速度并降低成本。

IT 风险管理

借助 RSA Archer IT Risk Management，您可以为组织元素和 IT 资产编制目录，以便进行 IT 风险管理。该使用情形包括一个风险登记簿，用于为 IT 风险编制目录，为 IT 预先构建的风险评估、预先构建的威胁评估方法和一个用于记录 IT 控制措施的目录。还附带 RSA Archer Issues Management，以便管理通过风险评估发现的差距和结果。

通过清楚地了解 IT 风险，您可以简化评估流程，加速识别 IT 风险并及时制定报告。风险与内部控制措施之间的关联有助于轻松地沟通 IT 控制措施要求，从而缩小法规遵从性差距并完善风险缓解策略。这个敏捷的风险管理框架让您可以跟上企业内部不断变化的要求并将资源重点放在具有最大影响力的 IT 风险上。

PCI 管理

RSA Archer PCI Management 支持您简化 PCI（支付卡行业）法规遵从性流程，自动执行评估并减少遵守要求所需的工作量。您可以通过组织有序的项目管理方式快速启动 PCI 法规遵从性计划，高效地执行条件评估，生成结构化报告并获得管理和缓解风险所需的可见性。PCI Management 与其他 RSA Archer GRC 解决方案全面集成，支持客户实施有效且可持续的 PCI 法规遵从性计划，并轻松地汇总结果，为范围更广的企业风险和法规遵从性绩效指标提供依据。

安全事件管理

RSA Archer Security Incident Management 支持您处理大量安全警报并实施托管流程来上报、调查和解决安全事件。您可以利用集中式系统将 IT 资产目录与全面的业务背景层相结合，推动对安全活动进行优先级排序。量身定制的工作流、警报和报告有助于简化安全事件响应流程并支持团队采取果断的行动。

可以通过定义的程序跟踪和管理事件调查，确保正确地处理和补救。通过明确定义的工作流，安全分析团队可以更加有效地利用时间，从而更加快速地处理安全事件。这些集成的流程还有助于提高 SIEM/

RSA

日志/数据包捕获基础架构投资回报，并且支持安全团队集中精力处理影响最大的事件，从而高效地管理并减少总体安全风险。

安全运营和漏洞管理

借助 RSA Archer Security Operations & Breach Management，您可以建立一个集中式系统，为 IT 资产编制目录，从而划分事件优先级。此目录中的全面的业务背景可帮助您对事件进行优先级排序。工作流驱动的安全事件报告让安全经理可以从容应对最紧急的问题。有关事件处理程序的最佳做法内容可以帮助安全分析团队有效且高效地响应警报。此外，当发生漏洞时，量身定制的工作流可以帮助管理后续调查和补救活动。安全运营经理可以有效地监视关键绩效指标，衡量控制措施的有效性并管理整个 SOC（安全运营中心）团队。

可以将应对安全事件和其他事件的事件响应流程整合成一种更加广泛、更加成熟的安全运营管理方式。通过明确定义的工作流，SOC 经理可以更好地分配分析团队的时间和资源，从而更加快速地处理安全事件。这些集成的流程还有助于提高 SIEM/日志/数据包捕获基础架构投资回报，并支持安全团队迅速响应漏洞和其他事件，从而有效地管理和减少总体安全风险。

IT 法规管理

RSA Archer IT Regulatory Management 提供了记录影响您的 IT 和敏感数据环境的外部法规义务所必需的工具和功能。这为敏捷策略框架奠定了基础，支持您的组织跟上不断变化的业务和 IT 法规遵从性风险。您还可以建立系统化审核和批准流程，以便跟踪对法规义务的更改，了解业务影响并对响应进行优先级排序。之后，可以快速地向高级管理人员和 IT 组织提供有关法规和企业必须遵守的其他法规遵从性要求的指导。通过完善 IT 法规遵从性要求与内部控制措施之间的关联，不仅缩小了差距，而且高级管理人员可以更好地了解影响业务的 IT 相关问题。

信息安全管理体系

RSA Archer Information Security Management System 支持您快速地划定信息安全管理体系的范围，并记录适用性声明，以便进行报告和认证。您还可以为与 ISMS（信息安全管理体系）相关的各个资源编制目录，其中包括信息资产、应用程序、业务流程、设备和设施，并且您可以记录和维护相关策略、标准及风险。通过这个有关信息安全管理体系的集中式视图，您可以更加轻松地了解资产关系并管理对基础架构的更改。可以集中跟踪在评估期间发现的问题，确保统一记录、监控并有效地实施针对差距采取的补救措施。

结论

RSA Archer IT & Security Risk Management 提供了基于业务风险开展安全措施的方式，支持您减少当今安全威胁、不一致的安全做法和运营安全不合规所带来的风险。您不仅能确定安全措施的业务背景，记录和管理安全策略及标准，检测和响应攻击，还可以识别和修复安全漏洞。