RSA® ARCHER® IT & SECURITY RISK MANAGEMENT

Solution Brief

INTRODUCTION

Organizations battle growing security challenges by building layer upon layer of defenses: firewalls, anti-virus, intrusion prevention systems, intrusion detection systems, vulnerability scanners, security policies, identity management, and physical access controls, and more. While these layers are necessary to provide fundamental defense and protect against today's threats, each layer also adds a level of complexity to the security infrastructure. This increased complexity makes it harder to clearly reconcile where security risks are emerging, and at what velocity threats could materialize.

Security functions are also challenged with growing security-related data created by these layers of defense, adding to the already crushing mountain of business data they are mandated to protect. Without a solid understanding what data is most important to the business, IT and security teams struggle to determine which security events are the most relevant.

Security is increasingly impacted by today's technology shifts, most notably, the transition of business elements to the cloud and external providers. As companies migrate more business critical processes and IT services outside the perimeter, security controls will rely heavily, if not completely, on outside parties. This shift to the third platform increases the challenge of both security and compliance requirements.

Today's constantly changing threats and incidents raise the interest of executives in how the organization deals with increased cyber risk. More than ever, executives are concerned about security risks – reputational damage, financial impacts and regulatory exposure, and the pure cost of investigation and resolution of a breach or other security event.

BRINGING INSIGHT TO IT & SECURITY

In order for IT risk and security functions to compile and render a complete picture of technology related risk, multiple operational groups must collaborate and coordinate efforts. Security policies must be aligned to regulatory and business requirements. Threat and vulnerability management processes must be agile to stay ahead of growing threats. Security operations must be active and diligent in order to swiftly identify active attacks against the organization and protect assets at risk. Security strategy must look beyond the immediate and tactical to bring innovative and cost-effective solutions to bear. Finally, security compliance must ensure the proper controls are designed and operating effectively.

THE RSA ARCHER IT & SECURITY RISK MANAGEMENT ADVANTAGE

With RSA® Archer® IT & Security Risk Management, your security function can benefit from enhanced visibility, analytics, action and metrics.

Connect Cybersecurity Risks in the Context of GRC

With today's interconnected business processes, organizations must be able to effectively address the complexity and cascading impact of rapidly changing cybersecurity risks. RSA Archer can connect your security processes and data with risk and compliance functions across the enterprise. The IT and security risk functions can then consider the relationship between business risk and IT risk in terms of business criticality to establish ownership and accountability; and connect IT and security risk to broader governance, risk and compliance programs.

Address IT & Security Risk Management through Multiple Dimensions

To effectively manage IT and security risk, you must organize your security program in such a way that you can manage the full spectrum of IT security risks. Your IT and security risk program must address risk management from multiple dimensions – from policies, standards, and compliance to threats, vulnerabilities and attacks. RSA Archer enables IT and security teams to centrally manage processes, prioritize cyber threats, and stay on top of the latest threats.

Bridge Business Context and Process Enablement

Managing IT and security risk today involves significantly more than just data speeds and feeds. IT risk must be understood in business terms because technology issues could put the entire organization at serious risk. By ensuring alignment between the business and IT, your IT and security risk management program can facilitate what needs to be addressed to keep the business secure. RSA Archer IT & Security Risk Management fills the gap between people and technology by establishing processes to identify and escalate risks effectively and efficiently.

RSA ARCHER IT & SECURITY RISK MANAGEMENT

New and emerging IT and security threats are pervasive in today's complex businesses. RSA Archer IT & Security Risk Management allows you to determine which assets are critical to your business, establish and communicate security policies and standards, detect and respond to attacks, identify and remediate security deficiencies, and establish clear IT risk management best practices.

RSA Archer IT & Security Risk Management provides a variety of use cases to meet your specific business needs on your risk management maturity journey.

Issues Management

RSA Archer Issues Management applies to any security, risk or compliance-related use case to capture and consolidate issues arising from security incidents; failed or deficient internal controls; and exceptions that require attention or escalation. Issues Management enables organizations to catalog internal and external audit findings, regulatory examination issues, and management self-identified issues; establish accountability for problem resolution; and track remediation plans against commitments and due dates. Robust reporting makes it easy for all levels of management and the Board to understand the full scope of outstanding issues, priorities, and remediation timelines.

IT & Security Policy Program Management

RSA Archer IT & Security Policy Program Management enables you to document external regulatory obligations and establish a systematic review and approval process for tracking changes to those obligations, understanding the business impact, and prioritizing a response.

IT Controls Assurance

RSA Archer IT Controls Assurance provides the ability to assess and report on the performance of controls across all IT assets, and automate control assessment and monitoring. You can implement a centralized system to catalog IT assets for compliance reporting and establish a system of record for documenting IT controls. Streamlined processes and workflow for testing of IT controls allow you to deploy standardized assessment processes for manual controls and integrate testing results from automated systems. Issues identified during compliance assessments are centralized, enabling you to track and report on compliance gaps. Remediation efforts for gaps can be

RSA

documented and monitored to ensure compliance variances are addressed in a timely manner.

IT Security Vulnerabilities Program

RSA Archer IT Security Vulnerabilities Program takes a big data approach to helping security teams identify and prioritize high-risk threats. You can proactively manage IT security risks by combining asset business context, actionable threat intelligence, vulnerability assessment results, and comprehensive workflows. IT assets can be cataloged with a full business context overlay, allowing you to better prioritize scanning and assessment activities. This consolidated vulnerability research platform enables IT security analysts to implement alerts, explore vulnerability scan results, and analyze issues as they arise. A powerful and flexible rules engine highlights new threats, overdue issues, and changing business needs. This ability to correlate known vulnerability risks with an applied business context helps prioritize response and remediation efforts, to speed the rate of closure of significant gaps and reduce costs.

IT Risk Management

With RSA Archer IT Risk Management, you can catalog organizational elements and IT assets for IT risk management purposes. This use case includes a risk register to catalog IT risks, pre-built risk assessments for IT, a pre-built threat assessment methodology, and a catalog to document IT controls. RSA Archer Issues Management is also included for managing gaps and findings generated from risk assessments.

Gaining clear visibility into IT risk enables you to streamline the assessment process, accelerate the identification of IT risks, and establish timely reporting. The linkage between risks and internal controls eases communication and correlation of IT control requirements to reduce compliance gaps and improve risk mitigation strategies. This agile risk management framework enables you to keep up with changing requirements within the business and focus resources on the most impactful IT risks.

PCI Management

RSA Archer PCI Management allows you to streamline the Payment Card Industry (PCI) compliance process, automate assessments, and reduce the effort required to comply. You can jump start your PCI compliance program with an organized project management approach, efficiently conduct continuous assessments, produce structured reports, and gain the visibility needed to manage and mitigate risk. PCI Management fully integrates with other RSA Archer GRC solutions, allowing customers to implement an efficient, sustainable PCI compliance program and easily roll up results to inform broader enterprise risk and compliance performance metrics.

Security Incident Management

RSA Archer Security Incident Management enables you to address the flood of security alerts and implement a managed process to escalate, investigate and resolve security incidents. You can leverage a centralized system to combine IT asset catalogs with a full business context overlay to drive prioritized security activities. Tailored workflows, alerts, and reporting help streamline the security incident response process and enable teams to take decisive action.

Incident investigations can be tracked and managed through defined procedures to ensure proper handling and remediation. With clearly defined workflows, security analysts can utilize their time more effectively to achieve faster closure rates for security incidents. These integrated processes also help to increase the return on SIEM/ log / packet capture infrastructure investments, and enable security teams to focus on the most impactful incidents to effectively manage and reduce overall security exposure risk.

Security Operations & Breach Management

With RSA Archer Security Operations & Breach Management, you can centralize a system to catalog IT assets for incident prioritization. A full business context overlay within this catalog allows you to prioritize events. Workflow-driven reporting for security incidents allows security managers to stay on top of the most pressing issues. Best practice content for incident handling procedures helps your security analysts respond to alerts effectively and efficiently. In addition, when a breach occurs, tailored workflows help to manage followup investigation and remediation activities. The security operations manager can effectively monitor key performance indicators, measure control efficacy, and manage the overall SOC (security operations center) team.

RSA

The incident response process to address security events and incidents is integrated into a broader, more mature approach to managing security operations. With clearly defined workflows, the SOC manager can better allocate analysts' time and resources to achieve faster closure rates for security incidents. These integrated processes also help to increase the return on SIEM / log / packet capture infrastructure investments and enable security teams to swiftly react to breaches and other incidents to effectively manage and reduce overall security exposure risk.

IT Regulatory Management

RSA Archer IT Regulatory Management provides the necessary tools and capabilities to document external regulatory obligations that impact your IT and sensitive data environments. This forms the basis for an agile policy framework that allows your organization to keep pace with changing business and IT compliance risk. You can establish a systematic review and approval process for tracking changes to regulatory obligations, understand the business impact, and prioritize a response. Accurate guidance can then be quickly delivered to senior management and the IT organization on regulatory and other compliance requirements to which the business must adhere. By improving the linkage between IT compliance requirements and internal controls, gaps are reduced and senior management gains better insight into IT related issues that impact the business.

Information Security Management System

The RSA Archer Information Security Management System allows you to quickly scope your information security management system and document your Statement of Applicability for reporting and certification purposes. You can also catalog individual resources related to your information security management system (ISMS), including information assets, applications, business processes, devices and facilities, and you can document and maintain related policies, standards, and risks. This centralized view of your information security management system makes it easier to understand asset relationships and manage changes to the infrastructure. Issues identified during assessments can be centrally tracked to ensure remediation efforts for gaps are consistently documented, monitored, and effectively addressed.

CONCLUSION

RSA Archer IT & Security Risk Management provides a business risk-based approach to security, enabling you to reduce the risk of today’s security threats, misaligned security practices, and operational security compliance failures. You can establish business context for security, document and manage security policies and standards, detect and respond to attacks, and identify and remediate security vulnerabilities.