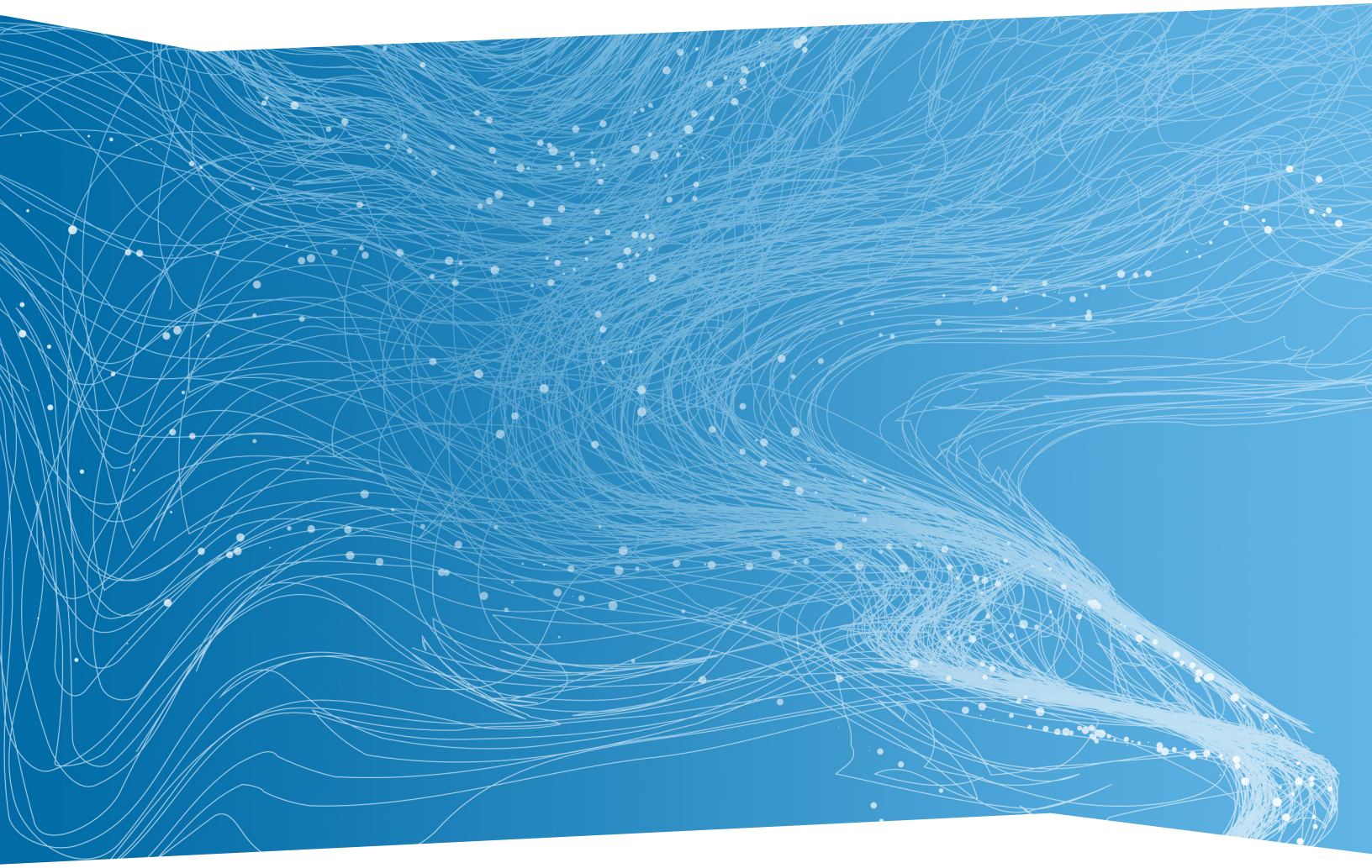
RSA



WHITE PAPER

RSA ARCHER® MATURITY MODEL: IT SECURITY RISK MANAGEMENT

RSA

OVERVIEW

Organizations face a litany of threats in the modern digital business world. Managing IT security today requires a combination of technology controls, effective and efficient processes, and skilled, informed people. The RSA Archer Maturity Model for IT Security Risk Management (ITSRM) outlines RSA Archer's role in the critical stages in a company's journey from reactive, compliance-driven processes to a risk-centric, opportunity-focused security program that is a competitive advantage to fuel the enterprise.

CONTENTS

RSA

WHY IT SECURITY RISK MANAGEMENT?

Companies battle security threats by building layer upon layer of defenses – firewalls, anti-virus software, intrusion prevention systems, intrusion detection systems, vulnerability scanners, security policies, identity management, physical access controls, and more. Of course, these many layers are necessary – without them, a company would be completely defenseless against the security threats. However, each layer of defense challenges IT security functions with more data, a growing complex security infrastructure, and a constantly changing business and technology landscape.

Security functions are challenged first with additional data. Every layer of defense creates more security-related data. And every day, this business data is piling up and adding to the already crushing mountain of data that security teams are mandated to protect. What's more, all of this data clouds the real issues. Security isn't sure which security issues are the most relevant, and they struggle with understanding what data is most important to the business.

These factors are also impacted by changes in technology. Some defensive layers will be breached with the movement of business processes and services to the cloud and external providers. As companies move more business processes and IT services outside the company perimeter, protective barriers will fade or disappear completely, and security controls will rely heavily, if not completely, on an outside party. This shift affects both complexity challenges and data issues.

Finally, nearly every day, there is headline news about data breaches and their impact. Constantly changing threats and resulting incidents not only indicate increasing risk for many companies but also raise the executives' awareness, driving more and more scrutiny from the C-suite as to how the organization is dealing with increased cyber risk.

As a result, organizations not only become overwhelmed with the "noise" inundating their security teams, they can also lose sight of the strategic value security can bring to the business. With all of this increased complexity, it becomes more difficult to clearly see where security risks are, where they are emerging, and at what velocity threats are approaching.

KEY CAPABILITIES

All companies face similar security challenges which make IT security a significant "cost of doing business." Companies that can execute efficiently and effectively can use this "cost" as a competitive advantage simply by reducing efforts, reducing costs and approaching security with strategic enablers.

RSA Archer GRC Maturity Models focus on key capabilities enabled by the RSA Archer solution. As a technology enabler, RSA Archer provides the critical infrastructure to leverage processes, share data and establish common taxonomies and methodologies.

RSA

Many organizations have addressed IT security as a technology problem. However, layer upon layer of defenses is not the ultimate answer. Organizations must also mature their IT security processes in proportion to the business and technology. With better security processes in place, the business has the safety net to pursue and exploit new opportunities such as adopting new technologies, expanding markets and launching new products and services.

When a security function – namely the Chief Information Security Officer (CISO) – puts together the picture of IT security risk, it requires multiple dimensions and operational groups to collaborate and coordinate efforts:

- Security policies must be aligned to regulatory and business requirements.
- Threat and vulnerability management processes must be agile to adjust and evolve to stay ahead of the growing threats.
- Security operations must be active and diligent to swiftly identify active attacks against the organization and protect assets.
- Security strategies must be built to look beyond the immediate and tactical in order to bring innovative and cost-effective solutions to bear.
- And finally, security compliance efforts must ensure the proper controls are designed and operating effectively.

To achieve these goals, RSA Archer's IT & Security Risk Management solution focuses on the following key capabilities:

Establish business context for security --
Enabling the IT security function to understand the business and IT assets, relationships and criticality, establish ownership and accountability and lay the foundation for security reporting.

Establish security policies and standards --
Processes to build solid security practices driven by regulatory and business data protection requirements, leveraging best practices and laying the foundation for security technical and process controls.

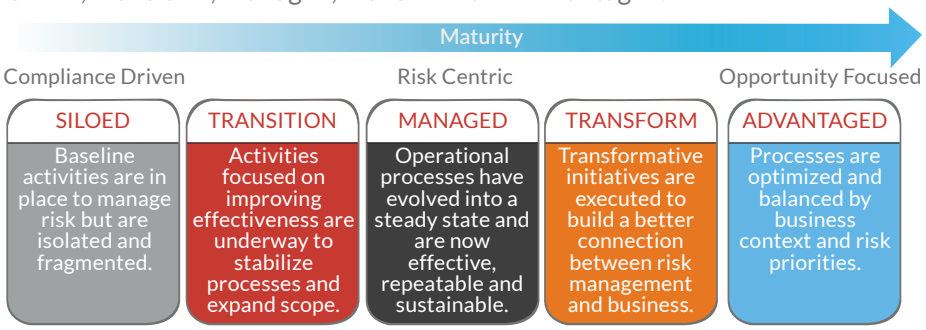
Identify and resolve security deficiencies --
Efficient methods to identify and manage security deficiencies and gaps ranging from control compliance issues to threats and vulnerabilities so the organization can respond appropriately and effectively.

Detect and respond to attacks --
Supporting an end-to-end solution for security operations to deal with the day to day security events while being prepared for serious incidents and data breaches.

RSA

THE MATURITY JOURNEY

RSA Archer Maturity Models are segmented into five major stages: Siloed, Transition, Managed, Transform and Advantaged.



The Maturity Model is designed to be pragmatic and implementable. Elimination of the "Level 0" that typical Maturity Models include avoids the unnecessary definition of a stage of maturity that will not meet today's security challenges.

- The **Siloed stage** focuses on baseline activities that all organizations need to manage risk.
- The **Managed stage** depicts the phase that organizations reach a coordinated, sustainable security program.
- The **Transition stage** and **Transform stage** help the organization "move to the next level" with initiatives that evolve critical capabilities setting the stage for advanced capabilities.
- Finally, the **Advantaged stage** is designed to be achievable for most organizations, allowing the organization to target an advanced stage of maturity that optimizes security programs.

The RSA Archer Maturity Model for IT Security Risk focuses on building the capabilities outlined above over time and implementing the broad strategy with tactical, intelligently designed processes.

FOUNDATIONS

Foundations are critical elements necessary for the overall success of the Maturity Journey for IT Security Risk Management. Without these foundations in place, the organization will face difficulties throughout the journey based on lack of focus, commitment, resources or strategy. Any organization looking to improve its maturity for IT Security Risk should discuss and address these foundations.

- **Management commitment** – The degree and level of leadership commitment to IT security risk management culture, strategy and priorities should be established as maturing security processes takes time and resources.

- **Performance and acceptable risk** – Defined levels of performance and acceptable risk for IT security need to be established to set the target state for the security program and ensure the business understands the level of risks involved.
- **Expectations and measurement** – Clear expectations and success criteria defined for the IT Security program must be communicated by management to guide strategies.
- **Stakeholder involvement** – Key business stakeholders and constituents need to agree on the importance of continuous improvement and maturity of IT security risk processes.
- **Budget and resources** – Sufficient resources for the IT security risk management program must be committed to achieve success.

THE SILOED STAGE: IMPLEMENTING THE BASICS

In the Siloed stage, the security organization orients reporting of security issues around major company units or divisional levels. Technical security reporting is oriented around technical attributes only (IP addresses, server names, etc.). Little to no detail of how the IT asset supports the business is used in managing, prioritizing or describing technical security issues. Because security reporting lacks a level of granularity making the issues relevant to line and business unit managers is difficult. Security issues are discussed and handled from a purely technical point of view.

Security policies are developed that generally align with the corporate objectives of the business. Policy owners (authors, contributors, approvers) are established and utilize an established process for managing policy lifecycle stages (authoring, approval, publication). Education processes utilize security policy content to promote employee awareness. The level of automation around policy management is minimal, as policies are managed and communicated through multiple mechanisms.

Vulnerabilities are identified with scanning performed on a regular basis for critical systems at a minimum or as required by regulatory obligations. Remediation of identified vulnerabilities are tracked and documented until closure of the security vulnerability. Requests for vulnerability scanning for operational purposes or ad-hoc scans of critical systems are tracked and documented.

Real-time collection, filtering and analysis of network packet and log data is implemented, at a minimum in critical segments of the network/infrastructure. An Incident Response framework is established with Level 1 (immediate triage) and Level 2 (detailed technical) analysis of security events. Analysis and details about the incident/investigation is documented and tracked in a central repository. Documentation of incident results and tracking of time to resolve the event is captured.

RSA

TRANSITION

Activities focused on improving effectiveness are underway to stabilize processes and expand scope.

THE TRANSITION STAGE: BUILDING CONTEXT FOR THE FUTURE

Within the Transition stage, the security organization gets more organized and granular in reporting security issues around business units and operational components of the organization. An understanding of business contacts has been established, allowing security issues to be aligned to line and business unit managers. Catalogs for key IT assets including applications and devices have been established and security issues are now reported with multiple dimensions and attributes to better define accountability around security.

Security standards are developed to support stated policy objectives. Review processes for policies, standards and procedures are executed to ensure security requirements remain aligned with business needs. Key stakeholders are assigned responsibility for security compliance processes. Regulatory obligations pertinent to the business are cataloged. Control activities that satisfy regulatory requirements are established. A process has been established to manage ad hoc changes required for security policies and standards.

Multiple vulnerability scanners are used to identify security deficiencies in infrastructure and applications. Vulnerability intelligence is gathered and tracked through the lifecycle of vulnerabilities with corresponding remediation and mitigation responses. Threat assessments are performed to identify possible security deficiencies. Issues and gaps are documented and tracked.

Scalability and flexibility across network topologies and geographies is supported for log/event/packet capture and analysis across the organization beyond critical segments of infrastructure. Remediation of issues and gaps arising from security incidents is captured, tracked and reported. Exceptions resulting from issues arising from security incidents are cataloged via the security policy process. Any policy changes needed resulting from issues arising from security incidents are passed to the security policy processes and addressed.

MANAGED

Operational processes have evolved into a steady state and are now effective, repeatable and sustainable.

THE MANAGED STAGE: OPERATIONALLY SOUND

In the Managed stage, a Business Asset catalog has been established for use by security. This catalog includes Facilities, key Information Assets (types/locations) and Business Processes. Attributes (owners, managers, business usage, etc.) have been established for these business assets and are in an active, managed catalog. The Business Hierarchy (organizational structure) has been mapped into the Business Asset and IT Asset catalogs. Additionally, mappings between IT assets and Business assets are managed. Security issues are now reported with business context (business usage) and IT context (technical information).

RSA

Key controls are connected to relevant enterprise assets and regulatory requirements to establish a clearly defined operational system of compliance. Content is developed for use in risk and compliance assessments related to policies, standards and controls that is harmonized and rationalized to reduce testing processes. Compliance testing is consistently executed to ensure controls are operating effectively. There is a process to manage Exceptions for risk issues where the risk being accepted by the business is defined and operational, including a risk analysis and sign-off from appropriate authorized delegated authorities for risk.

Business context (relationship between IT and Business assets) is added to vulnerability scan data to provide IT administrators with prioritization guidance. Escalation of vulnerabilities for critical/severe situations is enabled. An internal criticality rating system for vulnerabilities has been established and is utilized to escalate security deficiencies. Control assessment results are aggregated to inform compliance and risk performance metrics of security processes. A lifecycle (recurring, periodic, consistent) approach to performing threat and risk assessments across business and IT scopes is implemented. Policy changes and remediation resulting from issues arising from these assessments are documented and tracked. Operational and management reports on vulnerability risks and security gaps are provided on a regular, recurring basis with appropriate oversight for remediation and closure.

Event stream analytics on security events is enabled allowing for deeper inspection and investigation of active or potential attacks. Business context (relationship between IT and business assets) is added to event data to aid in triage and prioritization. All response activities are tracked and reported on until closure of security incident. Escalation of incidents and investigations is enabled using business impact prioritization and threat intelligence added to event data. Issues and gaps arising from security incidents are tracked and analyzed to identify systemic issues or correlate events indicating possibly larger attack scenarios. Standard response procedures are developed and implemented per incident type to streamline first and second line response activities. Security operations (analysis and response) is at an advanced stage based on business and technology requirements, e.g. 24X7 level with managed Shift Turnovers. Incidents resulting in data compromise or release are treated as data breaches and receive additional response handling. Data breaches are tracked until closure including any regulatory obligations associated to data compromised.

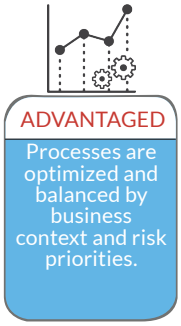
THE TRANSFORM STAGE: PRIORITIZATION AND CONTROL

The Business Asset catalog has been extended to account for organizational Products and Services connecting end customer facing products to internal processes and IT infrastructure. A common, extensible Business Impact Analysis process has been established and is being consistently executed on business processes to understand criticality to the business. This process is being used to feed business criticality of assets within security processes and technologies.

A system of record for managing enterprise control activities has been established. The Control Catalog has been mapped to internal policies and standards, external regulatory obligations and associated risks. The design of controls is assessed in addition to operating effectiveness to ensure they are tailored effectively to satisfy the control objectives. Compliance processes utilize a standardized approach to evaluate control compliance for assets (products/services, business processes, IT applications, facilities, etc.). Exceptions to policy are periodically reviewed and reaffirmed. Policy changes needed resulting from issues arising from control testing and assessments are documented and remediated.

Historical data from vulnerability scans is stored and managed in an archive with the ability to run complex queries for advanced analysis of emerging or changing risks. The criticality of vulnerability results is calculated to drive prioritization using both vulnerability and asset attributes including the business criticality of devices and applications and related business processes. Multiple feeds of vulnerability intelligence from outside sources are used to inform security threat risks. Threat assessments are proactively executed identifying exceptions to policy prior to implementation and exceptions are managed via the Security policy processes.

Insight into criticality of security events is based on both threat and asset information. Business criticality of assets involved in possible attacks is automatically included in the prioritization and triage processes. The Security Operations program is formalized with a catalog of staff including skills and experience and defined team structures of the Security Operations Center. Standardized risk assessments are performed for Incidents and Breaches to determine impact and risk severity improving prioritization processes.



THE ADVANTAGED STAGE: OPTIMIZED FOR RISK MANAGEMENT

In the Advantaged stage, business context has been infused in security processes and technologies. Security issues are reported on at macro and micro levels with integrated business attributes and impact.

Findings resulting from compliance processes are reconciled back to policies, standards, and procedures to identify and address underlying systemic issues. Compliance is providing a key feedback loop into the design and operating environments for controls. Policy exceptions are used as a leading indicator to identify misaligned or ineffective policies.

Vulnerability intelligence is used to identify emerging issues as intelligence changes through ad hoc, rules-based and queried analytics. External compliance reporting is produced in structured outputs as part of operational processes. Multiple risk and threat assessment approaches are utilized based on the business profile of the systems/processes assessed. Key metrics of vulnerability program are automatically created and reported on to security, IT and business management stakeholders.

Historical event/packet/log data is stored, managed and available for queries to possible past events or identify emerging issues as threat intelligence changes. Degrees and certifications of staff, continuing education and training of staff is tracked and documented to ensure skills are managed and the SOC team is current on industry practices. Control efficacy is analyzed based on actual incidents and provides insight and evidence into the effectiveness of controls. Data breach processes support emergency communications to Breach Team including stakeholders outside IT/Security (HR, legal, business, etc.).

MATURITY MODEL CROSSOVER

IT Security is a critical risk for all companies today and is a major piece of an overall Operational Risk Management program. Cited by executives as one of the fastest growing areas of risk today, IT Security has a significant place in an organization's strategic portfolio of risks and therefore should be factored into the Operational Risk program.

In addition, security incidents can quickly escalate into major crisis. Companies should address this issue by ensuring security incident response processes are aligned with crisis management, disaster recovery and business continuity processes within Business Resiliency strategies.

Another factor in security risk management is the growing reliance on outside providers within business processes. Third Party Governance must be tackled as part of managing IT security given many organizations provide access to internal systems to external parties or rely on third parties for critical business operations.

Finally, data protection is a critical component of today's Regulatory and Corporate Compliance environment. Compromise of the confidentiality of protected data, such as personally identifiable information (PII), can lead to significant regulatory fines, reputational damage and compliance issues.

CONCLUSION

Implementing a future-ready IT Security Risk Management program is not a simple click-the-button effort. It is a maturity journey that organizations must take to A security into an advantaged position to enable the business to exploit opportunities.

Companies in the **Siloed** stage must reduce "the noise" and evolve traditional approaches that may get the job done but will never keep pace with today's market. In order to move from Siloed to Managed stages, organizations **Transition** through projects that catalog and organize IT asset information and integrate security data sources. Companies in the **Managed** stage have solved (or are well on the way to solving) the integration of Security and Risk Management through better visibility into security issues through common data and analytical capabilities, effective security processes and efficient methods to measure, monitor and report on security activities. In order to reach the Advantaged stage, security processes **Transform** by focusing on better prioritization models to rationalize security controls and strategies, harmonizing across business requirements and reducing administrative overhead and costs. By prioritizing effectively using business context, security teams can keep up to speed with the business by enabling risk-based decisions.

Organizations in the **Advantaged** stage are ready to realize the competitive advantage of harnessing risk such as beating competitors to market, launching new products and services with calculated efficiencies and avoiding major issues that affect reputation and the bottom line. Security functions in this final phase speak the "business's language" and are able to identify and respond to emerging business requirements ahead of the curve using common taxonomies, common approaches and well-oiled decision making processes.

ABOUT THE RSA ARCHER MATURITY MODEL SERIES

RSA Archer's vision is to help organizations transform compliance, manage risk and exploit opportunity with Risk Intelligence made possible via an integrated, coordinated GRC program. The RSA Archer Maturity Model series of white papers outlines multiple segments of risk management that organizations must address to transform their GRC programs.

RSA

ABOUT RSA

RSA's Intelligence Driven Security solutions help organizations reduce the risks of operating in a digital world. Through visibility, analysis, and action, RSA solutions give customers the ability to detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, prevent IP theft, fraud and cybercrime. For more information on RSA, please visit rsa.com.