RSA® ARCHER® MATURITY MODEL: REGULATORY AND CORPORATE COMPLIANCE MANAGEMENT

OVERVIEW

Today's organizations face a litany of operational challenges in the modern digital business world. Maintaining compliance requires a mixture of technology, effective and efficient processes and skilled, informed people. The RSA Archer Maturity Model for Regulatory and Corporate Compliance Management outlines RSA Archer's role in the critical stages along a company's transitional journey from reactive, single-serving compliance processes to a risk-informed, opportunity-focused portfolio of compliance and a new source of competitive advantage to fuel the enterprise.

CONTENTS

Why Compliance Management? 2
Key Capabilities....3
The Maturity Journey....4
Maturity Model Crossover 8
Conclusion.... 8
About RSA Archer Maturity Models 9

WHY COMPLIANCE MANAGEMENT?

Throughout history, risk and compliance activities have existed in one way or another for as long as people have pursued commercial endeavors. For centuries, kingdoms have imposed rules, defended against aggressors, protected trade routes and established order. Even back then, security, risk management and compliance were daily doctrine. Over time, operational challenges have become exceedingly complex as businesses have continued to modernize and grow, requiring more structured risk and compliance programs to emerge. Yet, in heavily regulated industries like financial services, healthcare and the various energy sectors, statutory compliance requirements have been a formal operational fixture for hundreds of years or more. So what's different today?

One reason the compliance landscape has become so much more challenging than it was even 20 years ago is the velocity and volume of changes a typical organization encounters on a daily basis, combined with a significantly advanced threat landscape. Today's marketplace is a global interconnected web of virtual storefronts, fierce competition and lightning fast business dynamics. One of the great equalizers facing the modern enterprise may be the regulatory climate itself, posing a staggering burden of confusing rules and penalties that most organizations are simply not equipped to manage effectively.

Traditional approaches to compliance have largely been episodic and reactive. Whether a new requirement emerges or the business itself changes (perhaps through a merger that exposes it to new obligations), the result is often the same fire drill reaction – individuals scrambling to try to ascertain the impact and marshal enough resources to adapt the business before regulators can issue fines for non-compliance. And so it goes until the next change emerges and the process is repeated.

In simpler times, those manual processes (although painful) could remain functional possibly indefinitely. However, amid growing deficits and social pressures, governments are operating nearly unbounded to increase revenues through any means possible. This is not the only driver for sweeping regulatory changes. Protecting consumers from unethical corporate behavior, privacy breaches and other risks is also a useful and necessary mandate. Regardless of the specific motivations, the net effect to the average organization is the same: more rules, more compliance activity, more expenses.

Even smaller businesses can find themselves exposed to hundreds of different rules and obligations and thousands of potentially impactful changes per year requiring review. With systemic inefficiency in the overall process of compliance, it is easy to see how even the most committed and diligent organizations can quickly become overwhelmed, leaving most to worry about what tomorrow may bring.

- Compliance functions are challenged with managing many layers of exposure.
- Each layer adds a level of complexity to overall compliance risk.
- As organizations grow more sophisticated, they create additional complexity from a business and technological perspective.

Compliance functions are also wrestling with a growing data problem. Each year brings new business developments, more obligations and more audits, adding to an already huge mountain of security and compliance data. Increasing business complexities further expand the volume of compliance-relevant information the organization must maintain. As the data piles up, compliance teams struggle to consolidate everything into concise, useful representations of the overall risk and compliance portfolio, and extract useful contexts to help inform process improvement activities and broader strategy.

These factors are further impacted by changes in today's technology transformations. As concepts like "the Internet of things" and the shift to the "Third Platform" continue to take shape, traditional boundaries around assets, like cardholder data environments, patient data networks, etc., are blurring or disappearing entirely. Faced with increasingly threatening data breaches and regulatory scrutiny, many organizations are finding it difficult to effectively balance resource priorities to both adequately protect the integrity and confidentiality of operational assets and gain compliance efficiencies. This says nothing of trying to simultaneously meet shareholder expectations to grow the business and exploit market opportunities while diverting more and more resources away from R&D to address complex security and compliance issues.

Finally, almost every day in the news, we see an emerging story of either a data breach or a public regulatory finding, either of which can deal an eight figure blow to an organization. This constant stream of changing threats has driven cyber and regulatory risk to the top of the list of concerns among executive leaders and become a consistent topic of conversation in C-suite and Board-level discussions.

KEY CAPABILITIES

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.

All companies face similar compliance challenges, with regulatory compliance in particular now representing a significant "cost of doing business." Companies that can execute efficiently and effectively can convert this cost into a source of competitive advantage simply by reducing efforts, reducing costs and approaching compliance with strategic enablers. With better compliance processes in place, the business has a safety net to pursue and exploit opportunities such as adopting new technologies, expanding markets and launching new products and services.

For executives charged with compliance responsibilities to get an accurate picture of compliance risk, it requires multiple dimensions and operational groups to collaborate and coordinate efforts.

- Operational policies must be aligned to regulatory and business requirements.
- Intelligence gathering processes must be agile to keep key stakeholders informed of new compliance obligations and changes to existing obligations so they can react and respond.
- Business functions must be active and diligent participants in governance, risk, and compliance processes.
- Compliance strategies must look beyond the immediate and tactical to bring innovative cost effective solutions to bear.
- Compliance efforts must ensure the proper controls are designed and operating effectively.

To achieve these goals, RSA Archer's Regulatory and Corporate Compliance Management solution focuses on the following key capabilities:

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

.

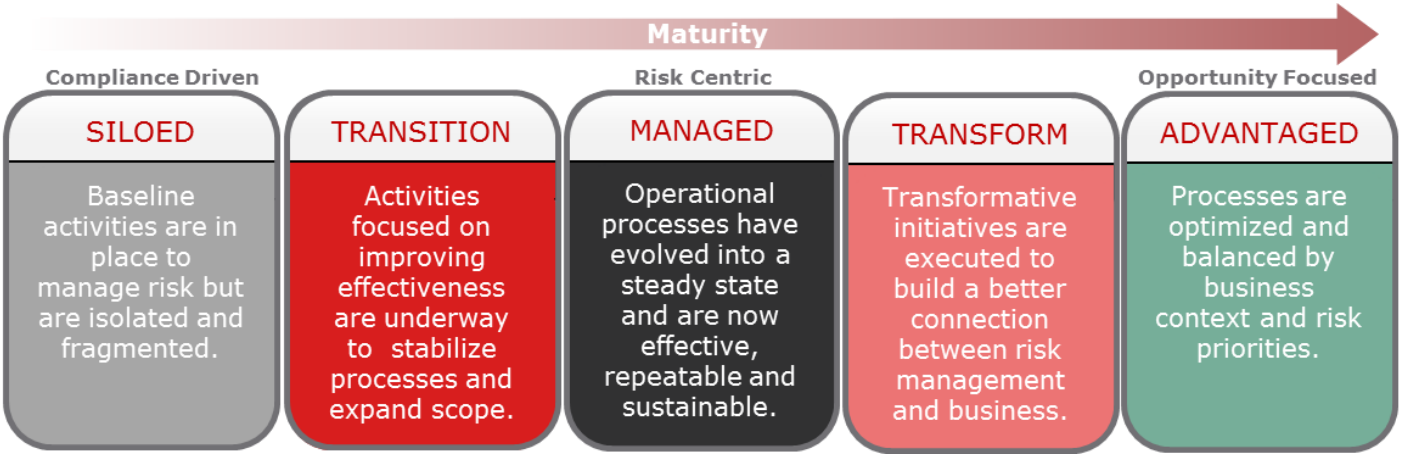
Identify and meet regulatory obligations
Efficient methods to identify, track, measure the impact of all the various regulatory and other corporate compliance obligations in order to set priorities, allocate appropriate resources necessary to achieve compliance and effectively adapt to changes in compliance requirements.

Define and implement policies and standards
Processes to establish a fully functional lifecycle of governance across the organization, aligned with regulatory and corporate requirements and leveraging best practices to lay a solid foundation for implementing effective operational controls.

Implement and monitor operational controls
Supporting an end-to-end solution for defining and implementing technical and process controls that are fully rationalized to risk-based drivers and efficiently reportable, and monitoring the performance of the control universe to ensure controls operate effectively and inform continuous refinement processes.

THE MATURITY JOURNEY

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



The RSA Archer 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 compliance challenges.

- The **Siloed stage** focuses on baseline activities that all organizations need to manage risk.
- The **Managed stage** is intended to depict the phase that organizations reach a coordinated, sustainable compliance program.
- The **Transition stage** and **Transform stage** help the organization "turn the corner" with initiatives that evolve critical capabilities setting the stage for advanced capabilities.
- 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 Regulatory and Corporate Compliance Management focuses on building these capabilities over time, implementing the broad strategy with tactical, intelligently designed processes.

Foundations

Foundations are critical elements necessary for the overall success of the Maturity Journey. Without these foundations in place, the organization will face difficulties throughout the journey either through the lack of focus, commitment, resources or strategy.

- **Management commitment** – The degree and level of leadership commitment to IT security risk management culture, strategy and priorities
- **Performance and acceptable risk -** Defined levels of performance and acceptable risk for IT Security
- **Expectations and measurement** - Clear expectations and success criteria defined for the IT Security program
- **Stakeholder involvement** – Importance of improvement and maturity of IT security risk processes to your stakeholders and business constituents
- **Budget and resources** – Sufficient resources for IT security risk management program to achieve success

Any organization looking to improve overall compliance maturity should discuss and address these foundations.

The Siloed Stage: Implementing the Basics

In the Siloed stage, the organization has begun to catalog its business hierarchy. Key physical locations, business processes, applications, and related support personnel are identified, as well as external roles such as auditors, regulators, and other related third party affiliates. The organization has policy process stakeholders and developed policies aligned with key corporate and regulatory compliance objectives. Internal personnel and relevant external parties understand corporate policy expectations through comprehensive training and awareness support. Organizational policies are individually acknowledged by affected personnel to ensure they understand and agree to abide by policy expectations.

If the organization already understands most or all of its broader compliance obligations, that understanding is likely scattered among individual stakeholder groups and contributors. Each area manages its own regulatory and corporate compliance affairs separately without a centralized view of the organization's broader risk and compliance portfolio including overlaps and gaps.

Control performance is assessed either ad-hoc or as part of an external audit or regulatory assessment. Any resulting findings are documented for follow up. Issues and gaps that require remediation are assigned to stakeholder owners with due dates and business unit visibility established. Basic compliance reporting is established to communicate issues and gaps related to key business processes, applications, facilities, etc.

The Transition Stage: Building Context for the Future

An organization in the Transition stage begins by creating a comprehensive catalog of all its compliance requirements, stakeholders, and areas throughout the enterprise affected by those requirements. Additional details are also documented about the organization from the top down including relevant corporate information, divisions and business units, and key information assets. Personnel role assignments are clarified and understood throughout the organization.

Operational standards are developed with input from key regulatory compliance process stakeholders to ensure all corporate and regulatory policy objectives are accounted for. A policy lifecycle maintenance process is established to periodically review policies and related standards to ensure they remain aligned with the directional needs of the organization.

The status of remediation activities to resolve issues and gaps identified during control assessments is being monitored and reported consistently to ensure remediation plan execution is effective for all open issues.

The Managed Stage: Operationally Sound

In the Managed stage, the understanding of the organization continues to mature as devices and other technical assets are added to the compliance inventory. This asset catalog is now actively managed and updated as the business changes and enables the business hierarchy to then be mapped to related business and IT asset catalogs. Those direct relationships between business assets and related IT assets are also understood and managed. With a centralized inventory of regulatory and corporate compliance objectives fully defined the organization can link those objectives to the specific business and technical hierarchies that are impacted or in-scope.

By establishing a system of record, the full lifecycle of policy and compliance activities can be managed, measured, and reported efficiently. Key risk and control processes and supporting policies are defined collaboratively with individual stakeholders to ensure an effective policy and control environment and clear ownership is established relative to the organization's obligations. Detailed control procedures are defined to ensure operational activities are managed effectively to satisfy corporate and regulatory compliance obligations.

The organization also develops and executes comprehensive internal compliance assessments against policy, standard, and control activities and reflects any related findings against the backdrop of established business context. Expanded control performance assessment activities include evaluations of the effectiveness of control designs.

Findings from assessments are reconciled back to related policies, standards, and procedures to ensure any systemic root cause issues are identified and addressed as part of an ongoing refinement process. If changes to existing policies, standards, or procedures are required those changes are documented and tracked through a policy change process in conjunction with the remediation plan.

Consolidated status reports establish management visibility into the overall status of compliance issues and remediation activities based on the defined business hierarchy.

The Transform Stage: Prioritization and Control

In the Transform stage, the organization has established monitoring capabilities to alert for potentially impactful regulatory changes. Informed by clearly defined hierarchical relationships in the business and technical asset catalogs, responsible stakeholders can quickly analyze and measure the potential impact to determine how the business must adapt and the time horizon to do so. Key linkages to individual products, services, and other value-generating assets are also added to the picture. As the compliance environment changes, end-to-end impact analyses are performed at the business process level. This portfolio view of compliance empowers strategic decision makers with a comprehensive, measured understanding of criticality and potential effects to the business. This clear understanding of overall compliance posture allows the organization to efficiently review and process ad hoc policy change requests and periodically reaffirm any outstanding exceptions previously granted.

The organization has extended the alignment of the control universe to include connections to key risks and strategic objectives like corporate stewardship and responsibility goals. With effective control assessment, remediation, and reporting processes established the organization is now able to leverage the embedded business context to apply a standardized approach for evaluating risk and control compliance across the entire business hierarchy and catalogs of enterprise assets including products and services, business and IT applications, business units and facilities, etc.

The Advantaged Stage: Optimized for Risk Management

In the Advantages stage, business context has been infused in compliance processes and technologies. Compliance issues with clarified business impacts are reported at macro and micro levels. Strategic decision makers leverage the output from compliance impact analyses to balance action priorities against other strategic objectives in the broader risk and compliance portfolios.

This complete business context is also embedded into risk and control activities allowing the ability to apply an informed, risk-based approach to managing any corporate, business, or regulatory compliance pursuit across the entire suite of enterprise assets. Changes to the business or regulatory environment are addressed inline as part of an optimized business process. A state of compliance is maintained as a byproduct of ongoing normal operations. Efficiencies realized throughout the process make demonstrating and reporting on risk and compliance status a simple exercise that can be performed at any time with minimal effort.

The organization is able to leverage the embedded risk and business contexts to overlay the standardized operational compliance processes in place to drive effective prioritization and escalation based on criticality to the business. The business context overlay also allows the organization to realize additional data-driven value from control assessment activities by aggregating those consolidated results to inform higher order compliance and risk performance metrics.

Monitoring policy lifecycle processes allows the organization to combine metrics like policy exception requests with compliance assessment findings related to policy violations to establish a leading indication of policies that have become misaligned or are no longer compatible with the changing needs of the business.

MATURITY MODEL CROSSOVER

Compliance risk is critical 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, regulatory scrutiny has a significant place in an organization's strategic portfolio of risks and therefore should be factored into the Operational Risk program. In addition, regulatory findings can quickly escalate into a major crisis. Companies should address this issue by ensuring incident response processes are aligned with crisis management processes within Business Resiliency strategies. Another factor in compliance risk management is the growing reliance on outside providers within business processes. Third Party Governance must be tackled as part of managing security and compliance risk since many organizations provide access 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 Regulatory and Corporate Compliance Management program is not a simple click-the-button effort. It is a maturity journey that organizations MUST take to turn compliance into an advantaged position to enable the business to exploit opportunities.

For companies in the Siloed stage, compliance functions must reduce "the noise" and evolve traditional approaches to 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 compliance data sources. Companies in the Managed stage have solved (or are well on your way to solving) the integration of Policy, Compliance and Risk Management through better visibility into issues through common data and analytical capabilities, effective compliance processes and efficient methods to measure, monitor and report on policy and compliance activities.

In order to reach the Advantaged stage, processes Transform through rationalizing plans and strategies, harmonizing across business requirements and reducing administrative overhead and costs. By prioritizing effectively through business context and awareness when new requirements emerge or incidents occur, compliance functions can keep pace with the business to enable risk-based decisions and confidently explore the Opportunity Landscape.

Organizations in the Advantaged stage are now ready to realize the competitive advantage of harnessing risk – beating competitors to market, launching new products and services with calculated efficiencies, and avoiding major issues that affect reputation and the bottom line. Companies in this phase are focused on speaking "business language" and are able to identify and respond to emerging business requirements ahead of the curve – using common taxonomies, common approaches, well-oiled decision making processes and, most importantly, data to support their conclusions.

.

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.

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 www.rsa.com.