RSA® ARCHER® OPERATIONAL RISK MANAGEMENT

Solution Brief

20 percent of companies surveyed have no process to develop and aggregate a risk profile. A further 38 percent rely on self-assessments by the business units. Nearly half profess difficulties in understanding their enterprise-wide exposure.

"Global Risk Survey: Expectations of Risk Management Outpacing Capabilities – It's Time for Action"
KPMG, 2013

INTRODUCTION

With the increasing number, complexity and velocity of risks, existing ad hoc approaches to risk management leave risk management teams overwhelmed with their risk workload. As a result, they are either not aware of high risks or cannot get in front of these issues to adequately manage them with existing resources. Teams often struggle with identifying business priorities and assigning accountability to known risks and controls, leaving the team scrambling to react when risk incidents occur. The risk team must be able to effectively engage business units in the risk process.

Unfortunately, many organizations have not taken a proactive, comprehensive approach to managing risk. By managing many different types of risks in different business silos and assessing risks using separate methodologies and measurements, there is no way to provide management with an accurate and aggregated view of risk across the business. Without this aggregate view, risk cannot be consistently managed within the organization's risk appetite.

Your executive team and Board of Directors need assurance that your organization's internal control framework is adequately designed and operating to ensure that risk is being effectively managed. Without this visibility, risk cannot be consistently prioritized and managed within the organization's limits and there is no way to provide your executive team and Board with an accurate, aggregated, and timely view of risk across the business.

TAKE CHARGE OF RISK MANAGEMENT

Establishing a central repository for risk and control related data is the first step in ensuring you have an accurate and comprehensive view of risk that can be readily conveyed to your executive team and Board. Engaging your business units (the first line of defense) in risk management practices extends your ability to gain greater insight into known and emerging risks. It strengthens the effectiveness of your risk management program by assuring your risk data is accurate and complete and your business unit managers are taking appropriate responsibility for their risks and internal controls, and provides efficiencies that free up your risk management team to focus on more important issues than program administration. The ultimate goal is to reduce the likelihood and impact of negative events, lost opportunities, and surprises and increase the probability that your objectives will be met, in order to maximize the performance of your business.

THE RSA ARCHER OPERATIONAL RISK MANAGEMENT ADVANTAGE

With RSA® Archer® Operational Risk Management, you get a consolidated and clear view of risk that allows you to prioritize risks, efficiently deploy resources to address the most critical problems, and elevate risk management as a new source of competitive advantage.

Engage Business Units as the First Line of Defense

Operational risk management is not the responsibility of the risk specialist team alone. While they are certainly a fundamental part of the organization's risk management framework, your business units must be more directly involved with day-to-day risk management. Business unit managers know which risks are changing, which risks are

emerging, which risk treatments are being implemented, and which ones are operating. Since they are ultimately accountable for their risk and internal controls, they must be actively involved in understanding and assessing risks within their complex operations. By partnering with the first line of defense, risk managers can more easily consume new risk information into existing risk management processes and expand their risk programs to uncover emerging risks, including those emerging from business changes.

Address Risk Consistently Across the Business

Many businesses experience loss events and incidents that are not identified, assessed, treated, and monitored consistently across all business units. Each business unit talks about risk in a different "language" with different measurements, controls and reporting. The result: everyone has a different view and evaluation of the risks to the business.

By standardizing the risk management process across the enterprise, you can establish a common risk language, measurement approach, and rating scales and you can explicitly articulate individual responsibility for business activities, risks, controls, policies and procedures. This enables you to quickly prioritize risk, clearly inform all stakeholders, evaluate and manage risk consistently, and escalate risk decisions in accordance with the significance of each risk and the authority to accept risk that has been delegated to managers. As loss events occur, appropriate business unit managers and second line of defense risk specialists can be notified to perform root cause analysis and establish remediation plans. Senior management is given necessary visibility into losses and engaged to review or approve losses consistent with the organization's risk management thresholds.

"Experience told us that RSA Archer GRC was a trustworthy platform through which to manage policies and processes, identify and respond to risks, and maintain strong visibility and reporting across the organization…

It's been hugely beneficial to us to be able to address such a complex and critical business challenge while taking advantage of a tried and tested GRC platform that we know we can put our trust in."

First Data Corporation

Improve Risk Visibility

For effective operational risk management, you need to be able to understand the complex relationship between business processes and risks and controls, and quickly report and respond to risks that impede your organizational objectives as they emerge. Without a centralized approach that provides critical business context, it is difficult to get a complete view of the state of your organization's risk without spending weeks sifting through data. Your executive team and Board require an accurate, real-time picture of risk in order to properly allocate resources and make better business decisions.

By utilizing the robust reporting and risk management architecture available through RSA Archer, you can report and respond to risks that challenge your organizational objectives as they emerge. RSA Archer offers thousands of reports, dashboards and an ad hoc reporting tool to quickly get the answers you need to report to executive management and the Board. As loss events and key risk indicator warnings emerge, risk analyses are performed, and questions about root cause arise, you can quickly explore the entire risk management framework deeply in real-time to understand risk drivers and get an accurate picture of risk.

RSA ARCHER OPERATIONAL RISK MANAGEMENT

RSA Archer Operational Risk Management makes it easy to engage your first line of defense to identify and assess risk, evaluate, approve and respond to loss events, oversee key risk indicators, and manage day-to-day tasks, issues, and remediation plans. Serving as an aggregation point for your organization's operational risk management program, RSA Archer brings together data often found in siloed risk repositories to identify, assess, evaluate, treat and monitor risks consistently across your organization. With the ability to better understand, prioritize and manage known risks, you can expand your program to include additional business units and risks, or re-deploy risk management resources freed up as a result of more efficient program management.

With RSA Archer you get a consolidated and clear view of risk that allows you to prioritize risks, deploy resources to address the most critical problems, and elevate risk management as a new source of competitive advantage. RSA Archer Operational Risk Management provides several use cases to meet your specific business needs and risk management program maturity journey.

RSA

Issues Management

RSA Archer Issues Management applies to any risk or compliance-related use case to capture and consolidate risks that exceed acceptable levels and need to be addressed; failed or deficient internal controls; key indicators outside boundaries; and loss events requiring remedial actions. Issues Management enables organizations to catalog their 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.

Risk Catalog

The RSA Archer Risk Catalog provides the foundation to record and track risks across your enterprise and establish accountability by business unit and named first line of defense manager. The catalog provides a three level rollup of risk, from a granular level up through enterprise risk statements. Inherent and residual risk can be assessed utilizing a top-down, qualitative approach, with assessed values rolling up to the associated business unit and enterprise risks.

Top-Down Risk Assessment

RSA Archer Top-Down Risk Assessment enables practitioners to document risk and control procedures. Risk register statements can be rolled up through a two-level risk hierarchy to provide enterprise-level risk statements. Risks can be associated with business processes and assessed on an inherent and residual basis, both qualitatively and across multiple risk categories using monetary values. Control procedures can be documented and linked to the risks they treat, for consideration as a part of the residual risk assessment.

Loss Event Management

Core to an effective operational risk management program, RSA Archer Loss Event Management allows you to capture and inventory actual loss events, near misses, and external loss events that may be relevant to your business and industry. Loss event root cause analysis can be performed for the purpose of taking appropriate actions to reduce the likelihood and impact of similar losses occurring in the future and robust reporting of loss events can be generated to help understand and better manage your organization's losses.

"I'm glad we chose to trust RSA Archer GRC as the basis for our risk governance solution. Its flexibility has enables us to respond quickly to demands from the Board. At the same time, it has enabled us to build a user-friendly platform that will make the culture change we're trying to drive less painful for end users."

Corporate Risk Manager
T-Systems LTD

Key Indicator Management

RSA Archer Key Indicator Management provides a means to establish and monitor metrics related to risks, controls, strategies and objectives. With configuration, metrics can also be associated with other elements of a GRC framework, such as products, services and business processes, to monitor quality assurance and performance. In an operational risk management program, key indicators often serve to provide early warning of changes in risk likelihood and impact, including changes in risk treatment. As indicators fall outside acceptable boundaries, key stakeholders can be automatically notified to initiate remedial actions.

Bottom-Up Risk Assessment

With RSA Archer Bottom-Up Risk Assessment, you can engage in targeted project risk assessments. Projects could include fraud assessments or assessments of new or changing products and services, business processes, mergers or acquisitions. Projects can be documented and questionnaires can be created with custom questions and questions derived from RSA Archer's extensive library of thousands of out-of-the-box questions. When risks are deemed too high, risk treatments and remediation plans can be documented and tracked.

Operational Risk Management

RSA Archer Operational Risk Management is an umbrella of several risk management activities, including risk and control registers, loss event documentation, root cause analysis and workflow review and approval; risk hierarchy roll-up and risk library; key indicator management, including a key indicator library and approval workflow; Top-Down Risk Assessments; Bottom-Up Risk Assessments; Issues Management; and risk self-assessments campaigns (control self-assessments(CSAs), risk & control self-assessments (RCSAs), and process, risk & control self-assessments (pRCSAs). Self

RSA

assessments incorporate workflow that allows the second line of defense program manager to create, distribute, review, and approve assessments.

RSA Archer serves as an aggregation point for your organization's operational risk management program. With the ability to visually understand, prioritize and manage known risks, you can expand your program or re-deploy risk management resources since resources are utilized more efficiently. With RSA Archer Operational Risk Management, it is easy to establish accountability for risk management activities; engage your first line of defense to identify and assess risk, evaluate, approve and respond to loss events; utilize key risk indicators; and manage outstanding issues. RSA Archer brings together data often found in siloed risk repositories to identify, assess, evaluate, treat and monitor risks consistently across your organization.

CONCLUSION

RSA Archer serves as an aggregation point for your organization's operational risk management program, enabling you to visually understand, prioritize and manage known risks and then expand your program. With RSA Archer Operational Risk Management, your organization can harness risk intelligence to reduce the likelihood and impact of negative events, lost opportunities, and surprises and increase the likelihood of achieving your objectives in order to maximize performance.