# RSA® ARCHER® OPERATIONAL RISK MANAGEMENT

The number, complexity, and velocity of risks are increasing, and the speed at which these risks emerge means your organization has much less time to effectively respond. In addition, organizations are managing many different types of risks – like cyber, third party supplier, competitive and new products/service risks – within different business silos and assessing them using separate methodologies and measurements. Unfortunately, the current ad hoc risk management approach is overloading your resources and does not provide a consistent, real-time risk picture for your executive team.

## CHALLENGES

*87% of organizations surveyed have seen the volume and complexity of risks increase over the past five years. Another 20% of these organizations have seen the volume and complexity of risks extensively increase over the past five years.*

-American Institute of Certified Public Accountants & NC State University
"Current State of Enterprise Risk Oversight: Progress is Occurring but Opportunities for Improvement Remain"
July 2012

Business managers and their teams are overwhelmed with the increasing risk workload and, as a result, are either not aware of high risks or cannot get in front of these issues to adequately manage them. 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 (the second line of defense) must be able to effectively engage the business units (the first line of defense) 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 them 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 aggregated view, risk cannot be consistently managed within the organization's risk appetite.

Your executive team and Board of Directors must have confidence that they have a complete understanding of the organization's risk profile in order to make good business decisions and fulfill their fiduciary obligation. They need assurance that the organization's internal control framework is adequately designed and operating to insure that risk is being effectively managed.

## HARNESS RISK AND FUEL YOUR BUSINESS

Establishing a central repository for risk-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 (first line of defense) in risk management practices extends your ability to gain greater insight into known and emerging risks, and strengthens the effectiveness of your risk management program by assuring your risk data is accurate and complete. By more effectively harnessing risk intelligence, your organization can reduce the likelihood of negative events, lost opportunities, and surprises, resulting in maximized performance.

## RSA ARCHER AND 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, and oversee key risk indicators. RSA Archer brings together data often found in siloed risk repositories to identify, assess, decision, treat and monitor risks consistently across your organization. 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 to include additional business units and risks, or re-deploy risk management resources since resources are used more efficiently.

RSA Archer also enables you to reinforce desired risk management accountability and culture. This allows you to extend your program across business units and activities that introduce operational risk, and then discuss and manage risk consistently. With RSA Archer Operational Risk Management, your organization can harness risk intelligence to reduce the likelihood of negative events, lost opportunities, and surprises in order to maximize performance.

*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

## RISK INTELLIGENCE TO MAXIMIZE PERFORMANCE

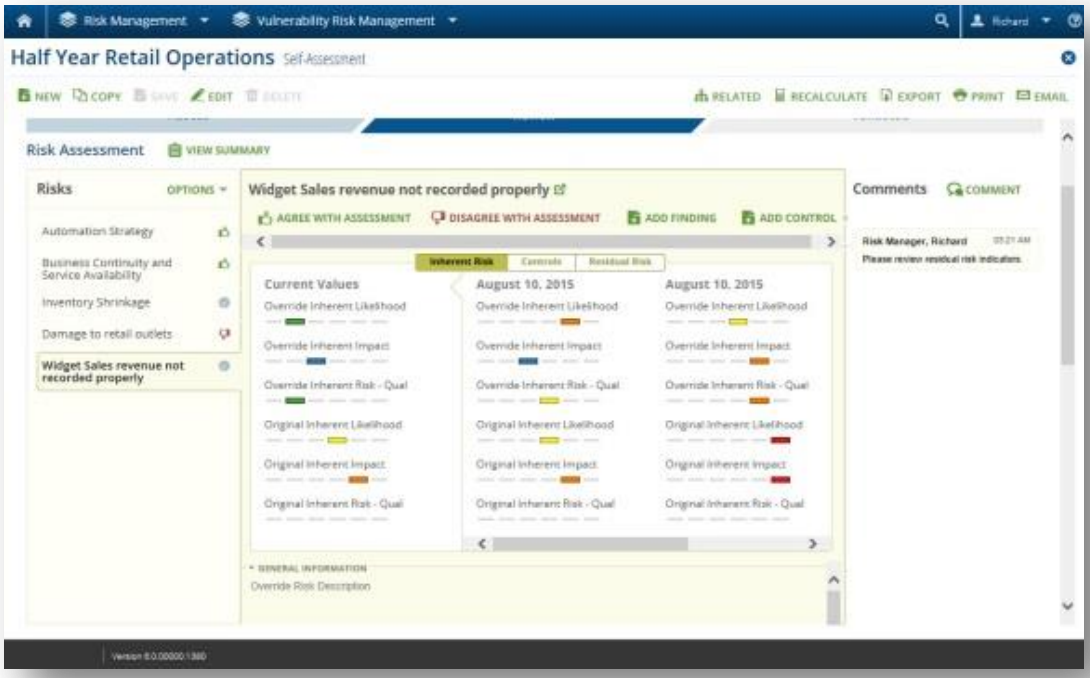
With RSA Archer Operational Risk Management, you get a consolidated and clear view of risk that allows you to prioritize risks, deploy resources to address the most critical threats, and elevate risk management as a new source of competitive advantage.

RSA Archer Operational Risk Management enables your organization to:

- **Identify, assess, decision, treat and monitor existing and emerging operational risks** – Establish a consistent approach to identify and analyze risk across organizational silos and appropriately respond and monitor these risks based on priority and impact.
- **Manage operational controls** – Ensure control systems are properly designed and operating effectively by documenting controls, performing management self-assessments, conducting control tests, capturing audit results, and identifying and responding to gaps.
- **Establish business context for risk** – Provide a complete view of risk exposure across your organization by relating risks to your business hierarchy and business objects such as strategies, products and services, business processes, IT infrastructure, controls and risk transfer, loss events, and key performance, risk and control indicators.
- **Define and implement policies and standards** – Understand the relationship between your risks and controls and associated policies, procedures, standards and regulatory requirements. Easily identify and manage gaps and demonstrate due diligence to examiners and auditors with a comprehensive, consistent process for managing the lifecycle of compliance.

## 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 (the first line of defense) must be more directly involved with day-to-day risk management. Business unit managers know which risks are changing, what risks are emerging, which risk treatments are being implemented, and which controls are operating and which are not. Business unit managers are ultimately accountable for their risk and internal control framework. Therefore, business units must be actively involved in understanding and assessing risks within their complex operations.



With RSA Archer, risk managers can easily expand the view of risk by engaging business units in the risk identification, assessment, and ongoing management process. RSA simplies the risk manager's job by simplifying the self assessment campaigns, cataloguing metric libraries, and automating the loss event routing process. RSA Archer Operational Risk Management tailors the business unit's user experience to easily view risk-related tasks and quickly complete self-assessments. By partnering with the business, risk managers can easily consume new risk data into existing risk management processes. RSA Archer provides an efficient mechanism to collect, analyze, prioritize and deploy resources to the threats or opportunities that are most important to your business. With the business units engaged, you can expand your risk program to uncover emerging risks.

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 threats, and elevate risk management as a new source of competitive advantage.

## ADDRESS RISK CONSISTENTLY ACROSS THE ORGANIZATION

It is a very common situation: the business experiences loss events and incidents that have not been identified, assessed, treated, and monitored consistently across all business units. Each business unit talks about risk in a different "language" with different measurements, controls (if any) and reporting. The result: everyone has a different view of the risks to the business and executives do not have a clear picture of risks needed to make the right business decisions.

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

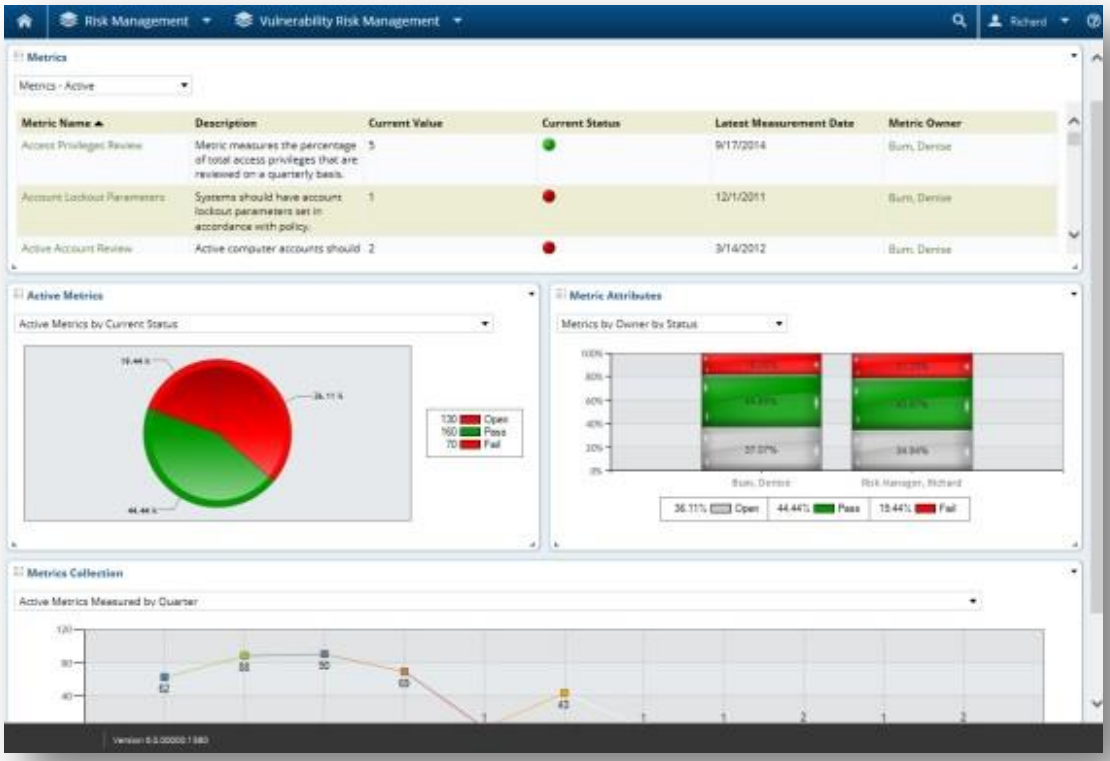
KPMG
"Global Risk Survey: Expectations of Risk Management Outpacing Capabilities – It's Time for Action" 2013

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

## IMPROVE RISK VISIBILITY

Without a centralized approach, it is difficult to get a complete view of the state of your organization's risk without spending weeks sifting through data. That means you cannot provide an accurate risk picture to your executive team or Board of Directors at a moment's notice as threats occur. Without accurate, complete, meaningful and timely risk reporting, your executive management and Board cannot fulfill their fiduciary responsibilities. As a result, your organization is much less likely to achieve your strategic objectives. Bottom line: without a solid understanding of your organization's risk exposure, your executives' jobs are on the line.

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 and deeply explore the entire risk management framework in real-time to understand risk drivers. These capabilities provide you, the executive team and Board of Directors with the accurate picture of risk required to quickly allocate resources and make better business decisions.




## ENABLE CORE RISK MANAGEMENT PROCESSES

Operational risk management requires a full lifecycle approach, including:

- **Risk identification** – Risks are identified through business unit self-assessments, loss events and incident analysis, and input from the second and third lines of defense. Risks are cataloged and include description, high level risk statements, responsible business units and individual stakeholders, risk type, risk drivers, the direction of the risk and its volatility.
- **Business context** – A complete view of the exposure to and connections between risks across your organization can be established by relating risks to objects such as controls, objectives, business processes, facilities and technologies.
- **Risk assessment** – Risks and controls can be assessed by business units using a standard self-assessment template. Inherent and residual risk can also be assessed top-down in multiple ways (qualitative, quantitative and through Monte Carlo simulation), offering various levels of complexity depending on the maturity of your organization's risk management program and risk assessment strategy. Lastly, detailed bottom-up assessments can be performed using questionnaires tailored specific to the target being assessed such as a special project, new product, or a software application.
- **Risk decisions** – Delegation of authority for risk consistent with your organization's risk appetite can be enforced through embedded workflow based on your unique taxonomy and delegated authorities.
- **Risk treatment** – Responses to accept, reject or reduce risk can be documented along with associated internal controls and insurance risk transfer.
- **Risk monitoring** – With a robust reporting engine, risk managers can report on any element of the ORM framework and associated data in the form of an email alert, workflow alert, online report and dashboard.

*"A major benefit we've seen since implementing RSA Archer GRC is more information transparency. Before we implemented our ERM system, silos of data were not used effectively. Now data may go into the system for one issue, but it can be cross-applied to all aspects of the business and aggregated for an overall view of risk rather than a variety of broken views."*

Financial services organization

- **Risk metrics** – A comprehensive strategy of KPIs, KRIs and KCIs can be implemented with association to their respective objectives, risks and controls. Metrics may be measured against minimum and maximum thresholds, expected direction and standard deviations from the historical mean. Notifications are distributed and action plans are solicited automatically for metrics that exceed tolerance.

- **Loss events** – Losses and near misses are an important element in managing operational risk. Without a defined centralized repository of loss data, the organization will lack this key feedback on the effectiveness of operations. A full loss event cataloging system is included with response tracking, root cause analysis and workflow.

## CONCLUSION

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, and oversee key risk indicators. RSA Archer brings together data often found in siloed risk repositories to identify, assess, decision, treat and monitor risks consistently across your organization. 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 of negative events, lost opportunities, and surprises in order to maximize performance.

* Features and functionality delivered with RSA Archer GRC Platform Release 6.0 are currently available only for new, on-premises installations.