RSA® ARCHER® OPERATIONAL RISK MANAGEMENT

Use Case for Enterprise & Operational Risk Management

The Challenge

Effective management of errors and fraud associated with people, processes, and technology is inherently complex. As organizations change and grow, the complexity, frequency, and impact of errors and fraud increase, and can be catastrophic in some cases. It is very difficult for businesses to manage this operational risk due to its complexity and the speed at which it can develop. Managing operational risk requires an organization to tie together all the necessary pieces that provide an understanding of the business context of the risk. For risk managers, this undertaking can overwhelm available resources and tax the limits of their knowledge and understanding of the inner workings of the organization's business activities. Risk management teams can counter this by better engaging business managers, the first line of defense, in risk management. The first line of defense is best able to identify and manage the risks and controls within their domain of responsibility.

Without engaging the first line of defense in identifying risk, and using consistent methodologies and measurements to assess risk, there is no way to provide executive management and the Board with an accurate and aggregated view of risk across the business so that it can be managed within the organization's risk appetite.

Overview

RSA® Archer® Operational Risk Management is a combination of use cases that are core to a typical operational risk management program. These elements include: Top-Down Risk Assessment, Bottom-Up Risk Assessment, Loss Event Management, Key Indicator Management, Risk and Control Self-Assessments, and Issues Management. RSA Archer Operational Risk Management enables cataloging business processes and sub-processes, documenting risks associated with business processes, and mitigating controls. Risk assessments can be performed on a top-down basis, through first line of defense self-assessments, and through targeted bottom-up assessments. Loss events can be cataloged, root-cause analysis performed and routed for review and approval. Key risk and control indicators can be established and associated with risk and control registers, respectively, and monitored to provide early warning of changes in the organization's risk profile. By integrating these use cases, risk managers have a comprehensive operational risk management program that reinforces desired accountability and risk management culture throughout the organization, providing necessary transparency through reporting, dashboards, and notification alerts.

Key Features

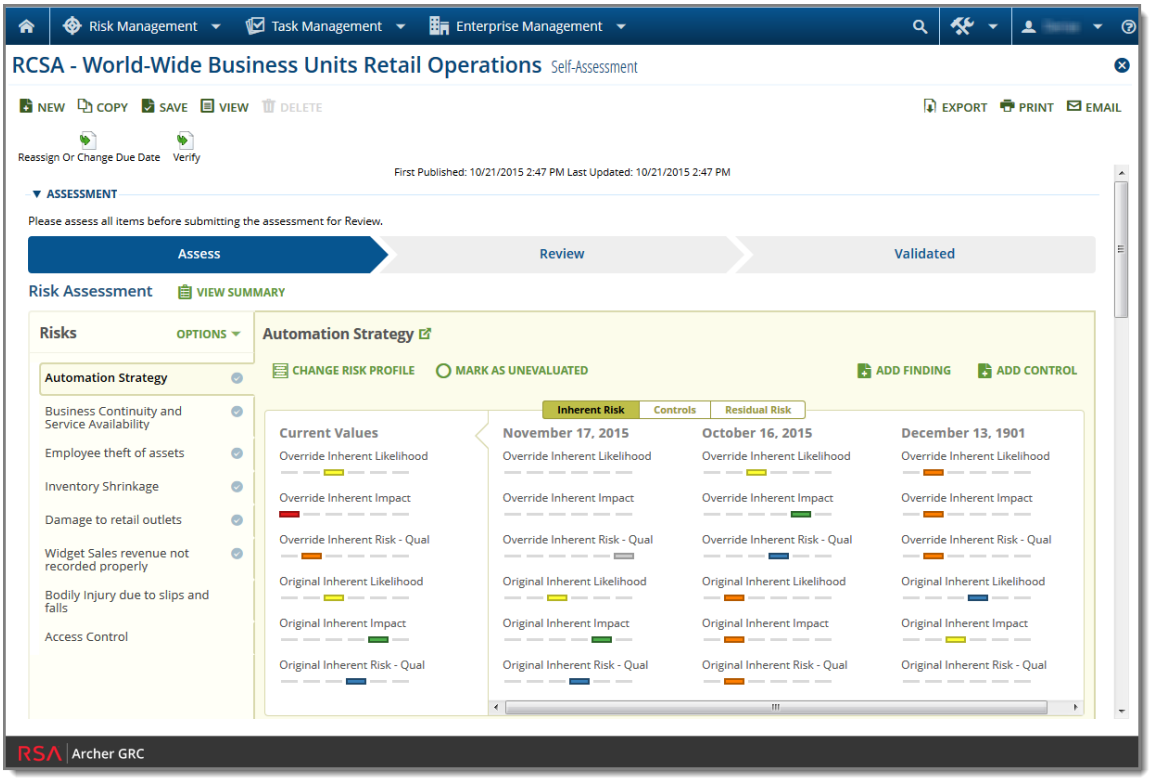
- Consolidated view into business processes, risks, controls, loss events, key indicators, and outstanding issues and how they are all related
- Support for first line of defense self-assessments and top down and bottom up risk assessments
- Efficient management of self-assessment campaigns by second line of defense stakeholders, including necessary workflow to vet and challenge first line of defense assessments
- Capture and perform root cause analysis on internal losses and near misses, and relevant external loss events

- Understand inherent and residual risk and observe changes in calculated residual risk while rolling up risks by business unit and enterprise risk statement
- Robust key risk and control indicator program management to provide early warning and remediation
- Consolidated issues management with a clear understanding at all times of the status of all open remediation plans and exceptions
- Visibility into operational risk via predefined reports, risk dashboards, workflow, and notifications

Key Benefits

RSA Archer Operational Risk Management provides:

- Better understanding of risks throughout the organization
- Improved risk management and risk management culture by engaging the first line of defense (business users) to take ownership of their risks and controls
- Quicker detection and management of changes in risk profile
- More efficient administration of the operational risk management program, allowing second line of defense teams to spend more time on analysis and less time on administration and reporting
- Less time required to identify and resolve operational risk related problems
- Reduction in audit findings, surprises, loss events, and incidents
- Ability to demonstrate design and effectiveness of risk management program



For more information

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.rsa.com. If you are an existing RSA Archer customer and have questions or require additional information about licensing, please contact RSA Archer at archersupport@rsa.com or call 1-888-539-EGRC.

RSA
www.RSA.com