

RSA® ARCHER® TOP-DOWN RISK ASSESSMENT

Use Case for Enterprise & Operational Risk Management

The Challenge

Risk professionals are continually challenged in managing scattered lists of risks and internal controls documented in different ways in various areas of the organization. Non-standardized risk management terminology, inconsistent risk assessment methodology, and inconsistent risk rating scales mean there is no comprehensive visibility to or accountability in addressing known risks. With everyone speaking differently about risk, inconsistent risk assessments can lead to bad risk management decisions, potential violations of regulatory mandates, and an overall poor risk management culture.

Overview

RSA® Archer® Top-Down Risk Assessment enables practitioners to document risks and controls throughout the organization. Risks can be assessed on an inherent and residual basis, both qualitatively and across multiple risk categories using monetary values. Controls can be linked to the risks they treat for consideration as a part of a residual risk assessment. Risk and controls can be assigned to named individuals and organizational structure to establish appropriate accountability and to provide relevant reporting.

Key Features

- Catalog a consolidated view of risks and internal controls within the organization
- Map risks to business processes, controls, and higher level risk statements
- Perform qualitative and monetary assessments of inherent and residual risk
- Monitor risks against established tolerances and risk appetite
- Enforce consistent terminology, risk assessment methodology, and rating scales
- Organized, managed process to escalate issues to ensure proper sign-off/approval of issues
- Named accountability for risks, controls, and business processes
- Visibility into risk and control inventory and assessment progress via predefined reports and risk dashboards

Key Benefits

With RSA Archer Top-Down Risk Assessment, you can:

- Catalog a consolidated view of risks and internal controls within the organization
- Map risks to business processes and controls
- Understand the linkage between risk register statements and enterprise risk statements
- Perform qualitative and monetary assessments of inherent and residual risk
- Monitor risks against established tolerances and risk appetite
- Enforce consistent terminology, risk assessment methodology, and rating scales

- Establish an organized, managed process to escalate, approve, and remediate issues
- Provide consistent risk and control reports from one consistent system of record

RSK-246905 Risk Register

NEW COPY SAVE EDIT DELETE Record 2 of 186 RELATED RECALCULATE EXPORT PRINT EMAIL

GENERAL INFORMATION

Risk ID: RSK-246905
 Risk: Access Control
 Description: Operational fraud, loss of intellectual property, and loss of customers from damaged reputation resulting from an access control breach
 Business Units: Alberta Add Business Unit Risk Owner: Bum, Al Bum, Denise
 Stakeholders: Customers Shareholders Business Unit Coordinator:
 Risk Event Category: Risk Manager: Risk Manager, Richard
 Driver: Internal Factors Risk Manager Specialist:
 Assessment Approach: Qualitative Survey Status: Active

OVERALL RISK

Inherent Risk: Inherent Risk represents an opinion of the overall risk to the organization without consideration of any risk responses and treatments.

Residual Risk: Residual Risk represents an opinion of the overall risk to the organization when considering existing risk responses and treatments applied to the inherent risk.

Calculated Residual Risk: Calculated Residual Risk estimates overall risk to the organization taking into account any failed metrics, non-compliant controls, open findings, and variance between annual expected losses and actual losses.

Inherent Likelihood Direction: Increasing Residual Likelihood Direction: Increasing
 Inherent Impact Direction: Increasing Residual Impact Direction: Increasing
 Volatility of Risk: High Annual Loss Expectancy:
 Calculated Risk Override: Calculated Risk Override: N/A - utilizing assessment results
 Justification:
 Warning Indicator:

QUALITATIVE SURVEY

Inherent Risk (In Absence of Controls and Risk Transfer)

Inherent Likelihood:
 Inherent Likelihood In the absence of controls to prevent unauthorized access, the likelihood

Residual Risk (Considering Controls and Risk Transfer)

Residual Likelihood:
 Residual Likelihood Given the existing internal controls to prevent unauthorized access, there

RSA Archer GRC Enterprise Governance, Risk and Compliance Version 6.0

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.