

RSA® ARCHER® RISK CATALOG

Use Case for Enterprise & Operational Risk Management

The Challenge

Organizations today face a wide range of risks originating in different areas of their business, related to strategy, credit, corporate and regulatory compliance, interest rates, liquidity, market prices, operations (errors, fraud, and external events), and reputation, among others. While risks are spread out across an organization and often interrelate, it is difficult to get a holistic view of risk necessary to manage it efficiently and effectively.

The problem is further compounded with the introduction of new products and services, mergers and acquisitions, business process changes, and new and intensifying sources of fraud. In many organizations, risks are documented haphazardly in spreadsheets and documents without consistent use of a common approach, methodology, or rating scale. In addition, accountability for risk is tenuous because risks are not assigned to named managers and business units. This undermines accountability and increases the likelihood that a significant risk event will occur.

Overview

RSA® Archer® Risk Catalog provides the foundation to record and track risks across your enterprise, and establish accountability by named first and second line of defense managers. It 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 intermediate and enterprise risk statements.

Key Features

- Consistent approach to documenting risk, assigning accountability, and assessing risks
- Oversight and management of all risks in one central location
- Ability to understand granular risks that are driving enterprise risk statements
- Consolidated list of prioritized risk statements

Key Benefits

With RSA Archer Risk Catalog, you can:

- Obtain a consolidated list of the organization's risk
- Enforce a consistent approach to risk assessments
- Prioritize risks to make informed decisions about risk treatment plans
- Create accountability for the ownership of risks

[Audit Management](#) | [Issue Management](#) | [Operational Risk Management](#) | [Business Resiliency](#) | [SHOW ALL](#)

Access Control Risk Register

NEW COPY SAVE EDIT DELETE | Record 2 of 94 | RELATED RECALCULATE EXPORT PRINT EMAIL




First Published: 1/26/2016 10:10 AM Last Updated: 1/26/2016 10:10 AM

ABOUT
GENERAL INFORMATION

Risk ID: RSK-218196
 Risk: Access Control
 Description: An electronic information security breach could result in financial losses that include direct loss of company assets including cash and intellectual property, soft dollar costs of remediation, and costs to notify customers and authorities.
 Business Units: [Alberta](#) Add
 Stakeholders: Customers, Shareholders
 Risk Event Category: Operational Risk
 Driver: Internal Factors
 Assessment Approach: Qualitative Survey

Intermediate Risk: [Electronic Information Security](#)
 Business Unit Risk Owner: Business Unit Manager, Denise
 Business Unit Manager, Jane
 Business Unit Manager, Jim
 Business Unit Coordinator: Business Unit Coordinator, Al
 Risk Manager: Manager2, Risk Manager3, Risk Rick Manager1, Richard
 Risk Manager Specialist:
 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. 
 Warning Indicator: 


[Risk Analysis](#) | [Risk Response and Treatment](#) | [Risk Monitoring](#) | [Calculated Risk](#) | [Assessment History](#) | [Mappings](#) | [Content Provider Information](#)

QUALITATIVE SURVEY


Inherent Risk (In Absence of Controls and Risk Transfer)


Inherent Likelihood: 
 Inherent Likelihood Justification: In the absence of controls to prevent unauthorized access, the likelihood of this risk occurring is high.


Inherent Impact: 
 Inherent Impact Justification: Unauthorized access to and exploitation of customer information and intellectual property of the organization could have catastrophic consequences.

Inherent Risk - Qual: 

Residual Risk (Considering Controls and Risk Transfer)

Residual Likelihood: 
 Residual Likelihood Justification: Given the existing internal controls to prevent unauthorized access, there remains a possibility that an access controls could be compromised.

Residual Impact: 
 Residual Impact Justification: Given the existing internal controls to prevent and detect unauthorized access, unauthorized access would be detected with sufficient speed to limit the magnitude of the impact.

Residual Risk - Qual: 

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.