

Archer® Risk Catalog

Use Case for Enterprise & Operational Risk Management

The Challenge

Organizations today face a wide range of risks 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 originate in different areas of an organization and are often interrelated, it is difficult to get the holistic view of risk that is necessary for efficient and effective risk management.

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 any consistent 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 of a significant risk event.

Overview

Archer® Risk Catalog allows you to record and track risks across your organization and establish accountability by named first and second line of defense managers. It provides a three-level rollup of risk, from a granular level 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.

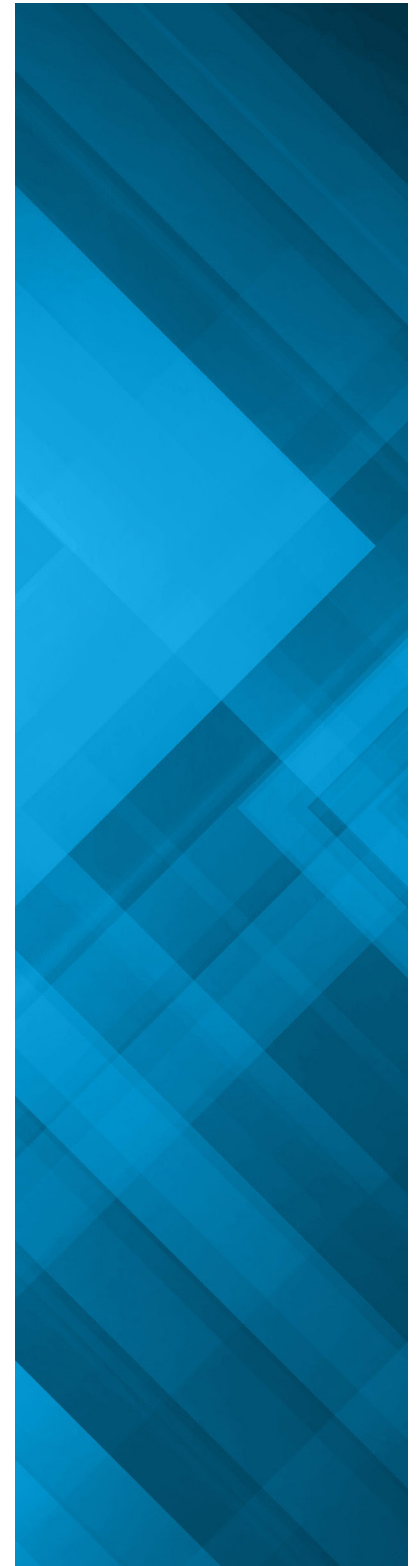
Key Features

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

Key Benefits

With Archer Risk Catalog, you can:

- Maintain a consolidated list of risks.
- Enforce a consistent approach to risk assessments.
- Prioritize risks to make informed decisions about risk treatment plans.
- Create accountability for risk ownership.



Risk Register : Breach of Physical Security

EDIT VIEW

First Published: 1/9/2019 1:22 PM Last Updated: 4/3/2019 4:20 PM

Record 4 of 54

ABOUT

GENERAL INFORMATION

Risk ID: RSK-462996
 Risk: Breach of Physical Security
 Description: Encompasses all threat-source pairs associated with breach of physical information.
 Business Units: [Services and Strategy](#)
 Stakeholders: Customers, Human Resources, Legal, Operations
 Risk Event Category: Operational Risk
 Damage to Physical Assets
 Terrorism
 Vandalism
 Driver:
 Assessment Approach: Qualitative Survey

Intermediate Risk: [Physical Information Security Breach](#)
 Business Unit Risk Owner: BusinessUnitManager, Denise
 Business Unit Coordinator:
 Risk Manager: Risk Manager, Robert
 RiskManager, Richard
 Risk Manager Specialist: RiskManager, Richard
 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: ●
 Inherent Impact Direction: Stable
 Volatility of Risk: Average
 Calculated Risk Override:
 Warning Indicator: ●

Residual Likelihood Direction: Decreasing
 Residual Impact Direction: Decreasing
 Annual Loss Expectancy:
 Calculated Risk Override Justification:

Risk Analysis | Risk Response and Treatment | Risk Monitoring | Calculated Risk | Scenario Analysis | Assessment History | Mappings | Content Provider Information

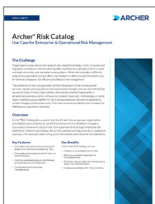
QUALITATIVE SURVEY

Inherent Risk (In Absence of Controls and Risk Transfer)

Inherent Likelihood: ● ● ● ●
 Inherent Likelihood Justification:
 Inherent Impact: ● ● ● ●
 Inherent Impact Justification:

Residual Risk (Considering Controls and Risk Transfer)

Residual Likelihood: ● ● ● ● ●
 Residual Likelihood Justification:
 Residual Impact: ● ● ● ●
 Residual Impact Justification:



Discover More

Archer, an RSA company, is a leader in providing integrated risk management solutions that enable customers to improve strategic decision making and operational resiliency. As true pioneers in GRC software, Archer remains solely dedicated to helping customers understand risk holistically by engaging stakeholders, leveraging a modern platform that spans key domains of risk and supports analysis driven by both business and IT impacts. The Archer customer base represents one of the largest pure risk management communities globally, with over 1,500 deployments including more than 90 of the Fortune 100.