

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. Nonstandardized 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

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. Risks 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, higher-level risk statements and scenarios.
- Establish a library of agreed-upon scenarios and perform assessments on selected scenarios.
- 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 signoff/approval of issues.
- Operationalize accountability for risks, controls, business processes, scenarios, risk assessments and outstanding issues.
- Establish delegated authorities for approving risk and enforce those authorities by automatically routing risk decisions to the authorized individuals.
- Visibility into risk and control inventory and assessment progress via predefined reports and risk dashboards.

Key Benefits

With 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.
- Manage risk scenarios on a consolidated basis, performing risk assessments and relating them to the risk register.
- Make certain that risk decisions are accepted only by those individuals with the authority to do so.
- Enforce consistent terminology, risk assessment methodology and rating scales.
- Ensure that all stakeholders are engaged in risk management commensurate with their scope of responsibility.
- 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

GENERAL INFORMATION

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

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
- Inherent Impact Direction: Increasing
- Volatility of Risk: High
- Calculated Risk Override: [Progress Bar]
- Warning Indicator: [Red Circle]
- Residual Likelihood Direction: Increasing
- Residual Impact Direction: Increasing
- Annual Loss Expectancy: [Progress Bar]
- Calculated Risk Override: N/A - utilizing assessment results
- Justification: [Text]

QUALITATIVE SURVEY

- Inherent Risk (In Absence of Controls and Risk Transfer)**
 - Inherent Likelihood: [Progress Bar]
 - Inherent Likelihood: In the absence of controls to prevent unauthorized access, the likelihood
- Residual Risk (Considering Controls and Risk Transfer)**
 - Residual Likelihood: [Progress Bar]
 - Residual Likelihood: Given the existine internal controls to prevent unauthorized access, there

ARCHER GRC | Version 6.0 | Enterprise Governance, Risk and Compliance



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.