

# RSA® ARCHER® RISK CATALOG

## エンタープライズ/オペレーショナル リスク管理のユース ケース

### 課題

今日の組織は、ビジネスのさまざまな領域で発生する多様なリスクに直面しています。このようなリスクには、戦略、信用、企業および法令コンプライアンス、金利、流動性、市場価格、運営（エラー、不正行為、外部イベント）、評判などに関するものがあります。リスクは組織全体に分散し、多くの場合、相互に関連し合っていますが、リスクを効率的かつ効果的に管理するために必要なリスクの総合的なビューを得ることは困難です。

新しい製品やサービスの導入、M&A、ビジネス プロセスの変更、増大する不正行為の新たに浮上している要因によって、問題はさらに悪化しています。多くの組織では、リスクをスプレッドシートや文書によって無計画にドキュメント化するだけで、一貫性をもって共通アプローチ、方法論、評価スケールを使用することがありません。加えて、指名されたマネージャーやビジネス ユニットにリスクを割り当てることがないため、説明責任が曖昧になっています。これによって説明責任が確保できなくなり、重大なリスク イベントが発生する可能性が増大しています。

### 概要

RSA Archer Risk Catalog [g1] は、エンタープライズ全体でリスクの記録と追跡を行い、指名された第1 防御ラインと第2 防御ラインのマネージャーによる説明責任を明確化するための基盤を提供します。細分レベルからエンタープライズ リスク ステートメントまで、リスクの3 階層のロールアップを提供します。トップダウンの定性的なアプローチを使用して、固有リスクと残留リスクのアセスメントを行うことができ、評価の結果の値を中間リスク/エンタープライズ リスク ステートメントにロールアップすることができます。

### 主な特徴

- リスクのドキュメント化、説明責任の割り当て、リスク評価を行うための一貫したアプローチ
- あらゆるリスクの監視と管理を一元化
- エンタープライズ リスク ステートメントを促進する細分的リスクの把握が可能
- 優先順位付けされたリスク ステートメントの統合リスト

### 主なメリット

RSA Archer Risk Catalogによって、以下を行うことができます。

- 組織のリスクの統合リストの取得
- リスク評価のための一貫したアプローチの適用
- リスク対応計画について十分な情報に基づく決定を行うためのリスクの優先順位付け
- リスクの所有権に応じた説明責任の明確化

Audit Management Issue Management Operational Risk Management Business Resiliency SHOW ALL Susan

## 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 Business Unit Risk Owner: Business Unit Manager, Denise  
 Stakeholders: Customers Business Unit Manager, Jane  
 Shareholders Business Unit Manager, Jim  
 Risk Event Category: Operational Risk Business Unit Coordinator: Business Unit Coordinator, Al  
 Driver: Internal Factors Risk Manager: Manager2, Risk  
 Assessment Approach: Qualitative Survey Manager3, Risk  
 Risk Manager Specialist: Rick Manager1, 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.

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:

## 詳細情報

EMCの製品、サービス、ソリューションがお客様のビジネスやITの課題の解決にどのように役立つかの詳細については、担当営業または認定リセラーまでお問い合わせください。あるいは、当社のWebサイト ([www.rsa.com/ja-jp](http://www.rsa.com/ja-jp)) をご覧ください。RSA Archerの既存のお客様であり、ライセンスについてご質問があるか、追加情報を必要としている場合は、RSA Archer ([info-i@rsa.com](mailto:info-i@rsa.com)) までお問い合わせ頂くか、03-6830-3341までお電話ください。