FINANCIAL INSTITUTIONS: MANAGING OPERATIONAL RISK WITH RSA® ARCHER®

As a board-level discussion topic at all financial institutions (FI) today, operational risk is real and public disclosure of significant operational risk events has become an all too common occurrence. The growing complexity of FI activities, changing workforce, expansive and shifting regulatory requirements, and dependencies on third parties can dramatically impact an FIs operational risk profile in the absence of an effective operational risk management strategy. FI executives, shareholders, regulators and the public expect financial institutions to be proactively looking at risk, adjusting operations and reacting in a strategic manner that appropriately limits risk. RSA Archer, a leader in GRC technology, helps FIs achieve a balance between risk and business agility through a comprehensive approach to Operational Risk Management.

CONTENTS

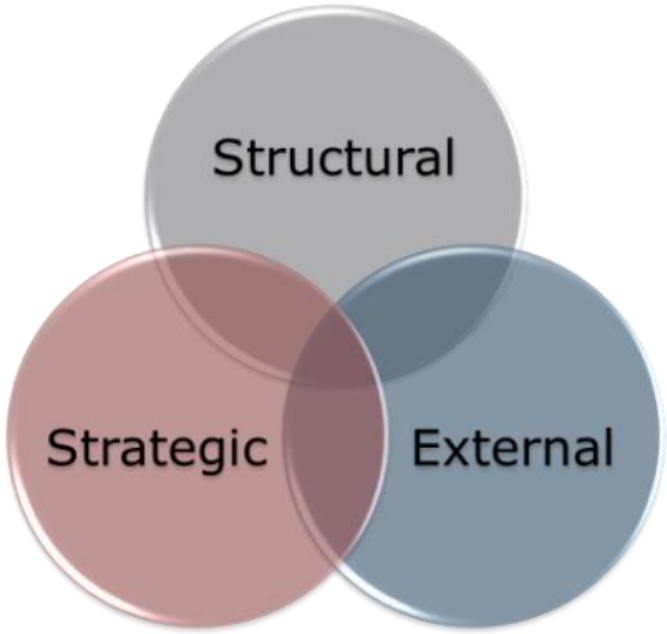
RSA PERSPECTIVE

RSA

EMC²

OPERATIONAL RISK IN FINANCIAL SERVICES

Operational risk -- defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events -- is inherent in all FI products, activities, processes and systems. Consequently, effectively addressing this risk has always been a fundamental objective of an FI's risk management program. FIs face structural, strategic and external factors that affect their operational risk profile. By combining these factors, FIs are able to understand their operational risks and how they need to respond to manage it.



Risks that influence the Operational Risk Profile

STRUCTURAL FACTORS

The complexity, size, scope and magnitude of the FI's organization and business activities will play a role in establishing the overall quantity of operational risk. FIs must deal with a high volume of transactions, product and service portfolios of varying size and complexity, the people, process, and technology to support them, and all of the related regulations pertinent to the business. The structure of organizational entities and management reporting lines can create a complex governance environment. It may often be difficult to establish clear accountability for risk taking, process and control ownership, and alignment of risk decisions with tolerances.

Understanding inherent and residual risk of the existing business is difficult enough but to be effective, FIs must also understand and manage risk introduced as a result of structural change. Reorganizations, mergers and acquisitions, introduction of new products, processes, technologies, third party relationships, ventures into new markets and geographies, and key employee turnover can all create shocks to established operational risk management programs. For some FIs, structural change comes at a manageable pace, while in others the velocity of change is extremely challenging.

STRATEGIC FACTORS

Strategic initiatives, such as new ventures, mergers and acquisitions, divestitures, product innovation, or changes in risk appetite and tolerance affect operational risk. Many FIs are being forced to move rapidly into new market spaces by developing new services or acquiring other financial institutions. As FI's merge, the operational risk profile of those organizations changes.

If an FI's strategy is to rely heavily on acquisition to expand product portfolios and markets, the FI needs to adapt its operational risk strategy to address risks with introducing new business, product line, organizational and technological infrastructures. If the expansion is driven by expanding geographically, the FI must address the risks associated with new infrastructures and facility locations. If new markets are being created organically, then risks associated with introducing new products and services must be addressed. While the formulation of business strategy should always consider risk, ORM programs should effectively respond to changes in risk profile driven by the FI's strategy.

EXTERNAL FACTORS

Externally originating fraud and information theft, regulatory compliance obligations, business resiliency and risk introduced through service providers and FI counterparties are common sources of external factors that affect an FIs operational risk profile. Changing regulatory requirements and difficulties anticipating changes in the security threat landscape make proactive risk management around these areas difficult. FIs doing business across geographical borders may face new national requirements as well as new local and regional regulations. Finally, outsourcing services and interacting with FI counterparties will influence the quantity of operational risk. FIs that outsource services, such as IT application systems, call centers, human resources or other shared services, will need to factor in the risks introduced by these external parties.

OPERATIONAL RISK LANDSCAPE

Taking risk factors, FI business activities, and the hierarchy of business delivery into consideration, FIs have many operational risks in common:

- Human error processing transactions, including not processing transactions fast enough or within required timeframes, or in accordance with regulatory obligations. These errors often manifest themselves as compensation losses or fines such as from erroneous money movement transactions or compliance violations.

- Programming / software errors in transaction processing, risk models, governance, etc., that introduce systemic risk that can result in very large losses as a result of transactions that must be unwound, decisions based on bad information, regulatory fines, and significant litigation claims.
- Information Security breaches from external hacking, phishing, social engineering, man-in-middle, data leakage, etc., can result in substantial losses and reputational damage.
- Theft and robbery of assets, customer information, intellectual property from insiders or external parties
- Property damage and business interruption from wind, fire, earthquake, or man-made event
- Litigation claims from employee wrongful termination, discrimination, sexual harassment, and breach of contract, and from customer and third party breach of contract or product liability claims
- Sub-optimal or failed process and internal control design and operation resulting in inefficiencies or failure to adequately enable design objectives. An example of this is represented by non-compliance with laws and regulations (AML, Terrorist financing, FCPA, CFPB, PCI, GLBA, etc.).
- Risk introduced by third parties as a result of their bankruptcy, error, fraud, disaster or failure to fulfill contract, SLA or regulatory obligations.
- Injuries to employees, customers and third parties from slip and falls, day-to-day tasks or other environmental factors
- New or changed products, processes, regulations or external threats that introduce risk that is not captured, well understood or appropriately managed
- M&A integrations and divestitures

EFFECTIVE OPERATIONAL RISK MANAGEMENT

In the "early days" of FI risk management, few dedicated risk management practitioners existed and those that did likely charted their organization's risk management course based on best guesses and trial and error. Regulators were in a learning mode, too, and few best practices or robust proscriptive guidance yet existed.

Today, widely adopted global risk management principles exist, such as the Basel Committee on Banking Supervision's Principles for the Sound Management of Operational Risk and the International Association of Insurance Supervisors' Insurance Core Principles, Standards, Guidance and Assessment Methodology. These are accompanied by ISO Standards on Risk Management and a long list of regional, country and local regulation and regulatory guidance on everything from fraud and anti-money laundering to incentive compensation, model risk management and market conduct. Keeping current across the broad changing regulatory landscape and internalizing changes within an FI's organization have become sources of operational risk in themselves.

While there is no grand harmonization of standards, principles and subject-specific FI regulations, there is general agreement on the characteristics of a good operational risk program:

- A strong risk management culture lead by the FI's Board of Directors that promotes responsible behavior and oversees the evaluation of the effectiveness of the ORM framework and associated policies, processes and systems
- An ORM framework that is integrated into the FI's overall risk management process, including common taxonomy, assessment approach, risk harmonization, integrated reporting, and well-defined, transparent, and consistent responsibilities and decision escalation
- An effective methodology for the identification and assessment of inherent operational risk across all prospective and existing material products, activities, processes and systems
- Operational risk appetite and tolerances consistently applied to the decision and management of all material products, activities, processes and systems
- Application of well-designed and effective internal controls and risk transfer to lower residual risk within tolerances
- Robust monitoring and transparent reporting of the FI's risk profile, internal control posture, and incidents, delivered to appropriate stakeholders, commensurate with their delegated responsibilities
- ORM governance alignment with the three lines of defense methodology: (1) business line management, (2) an independent ORM function, and (3) independent review of the ORM program by internal and/or external audit or other suitably qualified external independent source

These characteristics are enabled by appropriate policies, people, processes and technology. How an FI strategically enables these components will unequivocally shape how well operational risk is managed.

POLICIES

Operational policies must define how day-to-day business is executed and reflect the FI's appetite and tolerance for risk within each activity. Policies must be connected to key drivers, such as key risks and regulatory obligations, and provide the oversight and governance for business operations. This requires a consistent, active program, not just guidance thrown over the transom to the operational units. Periodic review, the quality of the guidance, ownership and accountability, and the connection between the organization's policy and operational procedures are all elements of a comprehensive, defensible policy program.

PEOPLE

There must be sufficient personnel with the appropriate experience and capabilities to manage day-to-day operations in accordance with policies and procedures, make risk decisions and maintain internal controls.

These individuals need to understand their roles and responsibilities, including the activities, risks and controls they "own," and be accountable for their actions or lack thereof. Incentives should be designed in a manner that discourages risk taking that exceeds the FI's risk tolerances and does not in any way encourage persons tasked with internal control responsibilities to compromise the desired control environment. There needs to be appropriate tone at the top of the organization to reinforce this strong risk culture.

PROCESS

Policies are enacted and implemented through business processes. How well those processes are designed and follow company policies and best practices is a key element of managing operational risk. Therefore, there must be a method to fuse operational procedures to organizational policy.

Secondly, internal controls must be aligned with the business processes and consistently implemented. This includes not only the discipline on execution but also processes to ensure proper compliance to organizational mandates and a well-defined internal control framework.

Finally, as business is always changing, there should be a mechanism in place to capture new and changed business activities to ensure that affected stakeholders, including risk managers, have input to ensure the changes are appropriate.

TECHNOLOGY

Technology that inherently introduces risk should be governed by:

- Appropriate policies to adequately manage the risk
- Individuals qualified and capable of identifying the risk and administering the controls
- Sufficient processes to enforce adequate oversight and change control to ensure that only and all authorized transactions are processed in a timely, complete, and accurate manner

From a risk governance perspective, adequate technology should exist to understand and manage the risk profile of the organization at any particular point in time.

ORM programs are a never-ending work in process, adapting to changes in the FI's structure (people, business entities, process, technology), objectives and strategy, regulatory and business environment, competition, and direct and indirect interdependencies with service providers and financial counterparties. Program refinements reflect this work in process and the desire to find the optimal balance between risk and risk treatments that are always constrained by human and financial capital resource limitations. The degree of program effectiveness depends on this balance and the degree to which the ORM program leverages tools and techniques that enable repeatable, process-based ORM in the most efficient manner possible.

RSA ARCHER AND OPERATIONAL RISK MANAGEMENT

Using this discussion as a backdrop for operational risk, RSA Archer's Operational Risk Management solution provides FIs with a comprehensive yet flexible infrastructure to enable an enterprise class program.

MANAGING THE ORGANIZATIONAL STRUCTURE

The first factor in managing operational risk is understanding the complex nature of the organization. RSA Archer's ORM solution provides a central repository to catalog the business hierarchy of the organization, products and services, business processes, supporting IT infrastructure, physical facilities and personnel. The catalog enables an aggregate view of the organization and its interdependencies to form the business context of ORM initiatives across your enterprise, including for purposes of understanding business resiliency.

The centralized system allows you to understand risk and compliance by company, division, business unit, products and service, business processes, and IT asset. As each item can be assigned to an individual, it also allows you to understand and enable the accountability and workflow that is so critical to an effective ORM program.

Business hierarchy and operational infrastructure provide business context

ENABLING CORE RISK MANAGEMENT PROCESSES

RSA Archer's ORM solution enables FIs to deploy a systematic and methodical approach to identify, assess, decision, treat and monitor operational risks consistent with your risk appetite and tolerances. The Risk Management function can build an integrated, holistic view of risks facing the organization that serves as an aggregation and visualization point for your ORM program. The risk team can bring risk information together from disparate, siloed risk repositories and identify, assess, decision, treat and monitor risks from one central solution. This integrated approach enables analysis of multiple risks across organizational silos and provides actionable insights to help optimize performance within a dynamically changing business climate.

Risk Management Processes

ORM requires a full lifecycle approach including:

- Risk Identification – Risks are cataloged and include description, high level risk statements, responsible business units and individual stakeholders, risk type, risk drivers, the direction of the risk and its volatility.
- Business Context –A complete view of exposure across your organization can be established by relating risks to objects such as controls, objectives, processes, facilities and technologies to integrate risk management with key business processes.
- Risk Assessment – Inherent and residual risk can be assessed in multiple ways (qualitative, quantitative and through Monte Carlo simulation), offering various levels of complexity depending on the maturity of your organization's risk management program and risk assessment strategy.

- Risk Decisions - Delegation of authority for risk consistent with your organization's risk appetite can be enforced through system workflow based on your taxonomy and the accountabilities for risk and risk management processes.
- Risk Treatment - Responses to accept, reject or reduce risk can be documented along with associated internal controls and insurance risk transfer.
- Risk Monitoring - With the robust reporting engine, risk managers can report on any element of the ORM framework and associated data in the form of an email alert, workflow alert, online report and dashboard.
- Risk Metrics - A comprehensive strategy of KPIs, KRIs and KCIs can be implemented with association to their respective objectives, risks and controls. Metrics may be measured against minimum and maximum thresholds, expected direction and +/- 2 standard deviations from the historical mean. Notifications are distributed and action plans are solicited automatically for metrics that exceed tolerance.
- Loss Events - Losses and near misses are an important element in managing operational risk. Without a defined centralized repository of loss data, the organization will lack this key feedback on the effectiveness of operations. A full loss event cataloging system is included with response tracking, root cause analysis and workflow.
- Operational Risk Self Assessments - Risk and Control Self Assessments can be performed to automate business unit risk reviews on a scheduled basis to reaffirm existing risks and controls and emerging changes in a business unit's risk profile.

ESTABLISHING CORPORATE AND FUNCTIONAL POLICIES

Policy Management forms the foundation for your ORM program with a comprehensive, consistent process for managing the lifecycle of policies and their exceptions. Key elements of ORM regarding policies are:

- Centralizing policies, standards and operational procedures to establish the authoritative system for organizational policy;
- Enabling key operational risk processes including exception management, training and awareness and review/maintenance of policies and procedures; and
- Demonstrating due diligence easily to examiners and auditors.

The RSA Archer Operational Risk Management solution provides a single point for creating policies, standards and controls and mapping them to objectives, regulations, industry guidelines and best practices. The solution provides the infrastructure to communicate policies, track acceptance, assess comprehension and manage exceptions. RSA Archer's GRC Content Library is an industry-leading knowledgebase of policies, standards and controls for key operational risks such as information security, IT security, business continuity, disaster recovery and audit management.

MONITORING CONTROL EFFECTIVENESS

ORM must also ensure the control systems are properly designed and effectively operating. The RSA Operational Risk Management solution provides a centralized, access-controlled environment for automating compliance processes, assessing deficiencies and managing remediation efforts. The compliance team can document process and technical controls, perform risk-based scoping, execute design and operating tests, and respond to gaps. Assessment results and remediation activities can be presented to management and regulators and managed through real-time dashboards.

SUPPORTING MODULES

Operational risk is an expansive challenge. RSA Archer also provides solutions to enable management of key operational risks. The ability to manage the ORM program, in addition to these critical operational risks, is a high value benefit of the flexible RSA Archer platform.

RESPONDING TO REGULATORY CHANGE

As regulatory compliance is a critical operational risk, RSA Archer's Regulatory Change Management solution assists your organization in staying abreast of emerging regulatory and industry requirements. This process complements the RSA Archer Policy Management program by using a central system to collect, analyze and track regulatory changes. Regulatory intelligence can be consumed from a variety of sources and workflows enabled to perform impact analysis and track remediation efforts in response to regulatory changes.

TRACKING OPERATIONS INCIDENTS

Operational risk events will most often manifest in incidents detected or reported through operations. RSA Archer Incident Management centralizes and streamlines the case management lifecycle for all risk incidents and ethics violations. The module lets you capture events that may escalate into loss events or are indicators of operational weaknesses.

MANAGING THIRD PARTY RISKS

A key operational risk that FIs face today is the risk inherited from outsourcers, third party service providers and suppliers. Key elements of third party risk management include:

- Vendor On-Boarding – Evaluate prospective vendors and conduct a due diligence review to assure the third party does not pose an unnecessary risk to your business.
- Relationship Management – Aggregate key vendor information including profiles, subsidiary hierarchy, sub-contractor relationships, contacts, facilities, contracts and engagements, financial statements, SSAE16s and certificates of insurance.
- Vendor Risk Assessments – Perform risk assessments on third parties. The solution includes pre-built questionnaires to evaluate inherent and residual risk of each vendor engagement across Sustainability, Information Security, Compliance/Litigation, Resiliency, Strategic, Financial and fourth party risk categories.
- Third Party Performance Review - Evaluate and monitor the vendor relationship by tracking key performance indicators, SLA objectives and the status of deliverables.
- Certificates of Insurance Review - Evaluate the adequacy and manage the completeness of certificates of insurance maintained on vendors.
- Vendor Profile Review - Evaluate and monitor the vendor's overall risk and performance profile, their ongoing financial viability, and filing of current assessments and supporting documentation.

RSA Archer Vendor Management automates and streamlines the oversight of vendor relationships addressing this critical operational risk. The module facilitates risk-based vendor selection, relationship management and compliance monitoring as part of the operational risk management program.

MANAGING BUSINESS CONTINUITY AND DISASTER RECOVERY

As defined previously, any event that can disrupt business operations is a potential operational risk. RSA Archer Business Continuity Management provides a centralized, integrated approach to business continuity and disaster recovery planning, allowing you to respond swiftly in a crisis to protect your operations.

The module combines business impact analysis, business continuity, disaster recovery, and crisis management in a single operational risk management system. By understanding the linkages between the organization's products and services, business processes and IT infrastructure, assessing the criticality of your business processes and technologies and developing business continuity and disaster recovery plans using automated workflow for testing and approval, the organization can plan execution and communication in a crisis to minimize harm to operations.

MANAGING IT SECURITY RISKS

IT security risks are growing more and more complex. FIs face threats from a wide variety of sources – from criminal elements to state-sponsored corporate espionage – exploiting an extraordinary array of vulnerabilities within business processes and technology. RSA Archer supports multiple elements of IT Security Risk Management programs to expand tactical IT security into a risk management discipline.

Through a combination of capabilities driven by a business-oriented foundation to reduce IT security risks, RSA Archer enables the two major components of information security – Threat Prevention and Threat Detection and Response. Together these components contain the functions and processes necessary to:

- Identify IT assets and the business context and criticality of those assets
- Implement proactive threat management controls based on vulnerability intelligence, testing, threat modeling and analysis
- Monitor IT assets, detect active threats and manage incidents and investigations

FOCUSED SOLUTIONS

RSA Archer has a myriad of other solutions focused on individual elements of an FI's ORM program. These solutions complement the core modules and provide support for singular use cases.

The RSA Archer Model Risk Management solution helps organizations address the challenges of effectively managing business risk model inventory by providing:

  - A centralized system to track and monitor risk models
  - Visibility across the enterprise to the health and status of risk model inventory
  - Consistent and repeatable processes to track model changes across the enterprise
  - Processes for model validation and testing
  - Clear reporting and metric tracking
- RSA Archer Model Risk Management solution-- Complements the RSA Archer Risk, Enterprise and Incident Management solutions and helps organizations apply and enforce effective measures to better manage their risk model inventory, capture changes, track performance across key performance indicators, provide risk certifications and sign-offs, organize associated documentation, and provides a mechanism to perform validation and reviews to track quality of fit using various tools and task management.

- RSA Archer Stakeholder Evaluations solution -- New regulations and directives such as Solvency II, FFIEC and the UK's Corporate Governance Code require that organizations examine how employee remuneration, qualifications, suitability, financial status and criminal history could influence and incentivize behavior that may be counter to corporate policies and laws. Helps organizations to verify that employee incentives are correctly aligned with corporate and regulatory policies so as to not incent behavior that would otherwise expose the organization to additional risk, fines or penalties. In addition, the solution enables organizations to effectively document, track and verify that employee qualifications and certifications are suitable for the roles they possess within the organization.
- Mergers and Acquisitions solution -- For FIs, mergers and acquisitions could be a major operational risk element. Merger and acquisition processes involve coordination of corporate strategy, financial forecasts, and the performance of in-depth due diligence investigations into targeted companies. Careful organization and analysis of materials is necessary to ensure that the acquired entity improves the position of the acquiring company. The Mergers and Acquisitions solution is a collection of applications used to facilitate the evaluation of merger and acquisition targets, consolidating data and tracking all activities associated with the identified organization. Using this solution, your organization can document corporate strategy, financing plans and management structures associated with buying, selling and combining companies.

CONCLUSION

ORM is a balance between the quantity of operational risk – as influenced by the structural, strategic and external factors -- and the quality of operational risk management. FIs must strive to build this balance through a combination of policies, processes, personnel and control systems relevant to their operational needs. RSA Archer provides a suite of solutions to:

- Define and manage the complexities of the organizational structural elements
- Organize and communicate corporate policies and operational procedures
- Enable a holistic, consistent operational risk management function
- Monitor compliance to operational controls

In addition to these core ORM elements, RSA Archer helps organizations manage the key operational risks such as Third Party Risk, IT Security Risk, Business Continuity Risk and others with an integrated approach and platform. RSA Archer's solutions provide an organization with the comprehensive and strategic technology enablers to implement an efficient and effective ORM program.

CONTACT US

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.EMC.com/rsa

www.EMC.com/rsa