OPERATIONAL RISK

RISK ASSESSMENT
OVERVIEW

• Inherent Risk
• Risk Management
• Composite or Net Residual Risk
• Trend
INHERENT RISK

- Definition
- Sources
- Identification
- Quantification
OPERATIONAL RISK DEFINED

“The risk of direct or indirect loss due to inadequate or failed internal processes, people, and systems, or from external events.” — Basel, “Sound Practices for the Management & Supervision of Operational Risk”

Translation: Everything that’s not credit and market risk.
SOUCRES OF RISK

- **People**
  - Fraud
  - Breach of authorized limits
  - Human error

- **Processes**
  - Execution failure
  - Product failure

- **Systems**
  - Systems disruption or failure
  - Vendor/service provider failure

- **External events**
  - Natural disaster
  - Political events
UNDERSTANDING THE OPERATIONAL AREA

People

- Organization chart and reporting lines
  - What is department’s position within organization? What is department’s organization structure? Clear, direct, and sufficiently high reporting lines?
- Interfaces with other departments
  - What data, reports, or risk management responsibilities flow across departmental boundaries?
- Role definitions or job descriptions
  - Are departmental activities—and management’s roles—clearly defined?
- Staff and management qualifications
  - What is the experience level and expertise of management and key staff?
UNDERSTANDING THE OPERATIONAL AREA

Processes

- Workflow diagrams
  - Work process documents from business line or internal audit; Management interviews
- Dependencies and interfaces
  - With other internal departments; With external service providers.
- Products
- Transaction volumes and dollar amounts
- Risk & control assessments
- Procedures
- Monitoring reports
  - Obtain a complete list of MIS; Identify distribution and frequency.
- Strategy and major projects
UNDERSTANDING THE OPERATIONAL AREA

Systems

- Major systems and components
  - Architecture; Hardware and software inventories
- System interfaces
  - IT topologies; Data flow diagrams
- Outsourcing vendors
- Security
  - GLBA security report for board
- Contingency plans
  - Corporate contingency plan; business line and support area continuity plans
Understanding The Operational Area

External Environment

- Potential for natural disasters
- Stability of legal and political environment
  - Pending legislation and regulatory requirements
  - Trends in litigation and legal precedent
- Environment for crime
  - Federal and local crime statistics
  - Economic environment
- Market and competitors
  - New products, services, or technologies and the pace of change
  - Mergers, acquisitions, industry consolidation

Risk Sources

How mergers go wrong
PERFORMANCE VERSUS RISK

- **Performance Indicators**
  - Shorter term orientation
  - Profit & loss or income statement derived
  - Used by business or functional unit managers
  - Larger number of metrics useful to more people

- **Risk Indicators**
  - Longer term orientation
  - Balance sheet and capital
  - Used by executive management and the board
  - Fewer number of metrics useful to fewer people
INHERENT VERSUS RESIDUAL RISK

- Inherent – Risks intrinsic to the activity
- Residual – Risks remaining after consideration of the control environment or mitigants
- Indicators may be of either or both types, but the differences—and purposes—must be understood.
CATEGORIES FOR RISK INDICATORS

Basel Categories for Operational Loss:

- Fraud: Internal & External
- Employment Practices & Workplace Safety
- Execution, Delivery, & Process Management
- Business Disruption and Systems Failures
- Clients, Products, and Business Practices
- Damage to Physical Assets

Categories for Operational Risk:

- People
- Process
- Systems
- Events
PEOPLE RISK INDICATORS
-- QUANTITATIVE MEASURES --

- Turnover rates
- Vacancy rates
- Tenure of business or functional area and senior management
- Organizational changes
- Staff size in relation to activity volumes
- Reliance on key staff and management succession

- Misuse of systems
- Misuse of confidential information
- Position vacancies and time vacant
- Internal fraud rates
- False expense claims
- FTE to budget
PROCESS RISK INDICATORS
-- QUANTITATIVE MEASURES --

Inherent

- Complexity
- Activity volumes – Monetary value per transaction & in aggregate
- Structural changes or growth rates: merger, consolidation, integration, outsourcing
- New or changing product or process
- Fraud and operational losses
- Policy breaches, exceptions, and overrides
- Customer satisfaction
- Remoteness of operations

Residual

- # deposit return items
- ACH rejects
- Customer and internal help desk call abandon rate
- Statement cycle errors
- % account balancing completed by deadline
- % new loans processed by internal goal
- Error rates in new products or processes
SYSTEMS RISK INDICATORS

-- QUANTITATIVE MEASURES --

Inherent

- Clarity of IT strategy
- Vendor dependence
- Mature vs. emerging technology
- Degree & complexity of projects
- Processing performance
- Availability and stability
- Capacity and scalability
- Level of integration
- Contingency planning & resiliency
- Access control and security

Residual

- Vendor performance to SLAs
- $-weighted or criticality-weighted project status
- Mainframe and network availability
- Capacity utilization: processing, storage, and data communication
- Disaster recovery response time vs. goal
- Volume, severity, and duration of system outages
- Volume, severity, and type of security incidents
- System response time
EXTERNAL RISK INDICATORS
-- QUANTITATIVE MEASURES --

- Economy
- Competitive environment
- Regulatory
  - Laws and regulations
- Nationalization
- Social unrest
- External/criminal threats
- Natural disasters
- Time required to reposition balance sheet or modify business activity
- Insurance coverage and deductible amounts
- Business continuity recovery time versus goal
### OTHER RISK INDICATORS

--- QUALITATIVE MEASURES ---

<table>
<thead>
<tr>
<th>General Measures:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization culture</td>
</tr>
<tr>
<td>Organization structure</td>
</tr>
<tr>
<td>Compensation structures and incentives</td>
</tr>
<tr>
<td>Systems</td>
</tr>
<tr>
<td>Complexity and maturity</td>
</tr>
<tr>
<td>External connectivity</td>
</tr>
<tr>
<td>Centralized versus distributed</td>
</tr>
<tr>
<td>Level of automation and integration</td>
</tr>
<tr>
<td>Existence of quality assurance programs and metrics</td>
</tr>
<tr>
<td>Internal and external</td>
</tr>
<tr>
<td>Existence of comprehensive compliance risk management</td>
</tr>
<tr>
<td>Geographic footprint</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unique Measures:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACH</td>
</tr>
<tr>
<td>Number and type of correspondents used for processing or settlements</td>
</tr>
<tr>
<td>Type of transactions (WEB, TEL, RCK, ARC)</td>
</tr>
<tr>
<td>Accounting/Financial Reporting</td>
</tr>
<tr>
<td>Attestation / certification processes</td>
</tr>
<tr>
<td>Human Resources</td>
</tr>
<tr>
<td>Hiring practices</td>
</tr>
<tr>
<td>Training practices</td>
</tr>
<tr>
<td>Other</td>
</tr>
<tr>
<td>Examination ratings by other regulatory bodies (nonbanking activities)</td>
</tr>
</tbody>
</table>
RISK IDENTIFICATION
-- INFORMATION SOURCES --

General Information Sources:

Financial statements
Websites
Interviews
Media publications
Brochures

Management reports
Organization charts
Audit reports (internal and external)
Examination reports
Competitors and market share

Specialized Information Sources:

Information technology schematics
Regulatory publications

Economic studies
Industry studies
INFORMATION SOURCES
-- GENERAL --

- Accounts: number by type, growth rates
- Transaction: volumes by account type, individual and aggregate size,
- Fraud losses: stratified by account type and cause
- Litigation: stratified by type, exposure, and cause
- Error rates: granular by account type and cause
- Quality of performance rates and error resolution times
- Policy and limit breaches
- Geographic footprint
INFORMATION SOURCES
-- SPECIALIZED --

- Human Resources
  - Management succession plan
  - Training costs and penetration
- Technology
  - Topology and data flow diagrams
- Loan Operations
  - Payment processing exceptions
  - Document handling measurements
  - Overrides & limit exceptions
  - Suspense account resolution
- Deposit Operations
  - Deposit processing exceptions
  - Encoding error rates
  - Research request response time
  - Statement mailing measurements
  - Suspense account resolution
QUANTITY OF RISK

- Volume
- Measurement
- Information sources

For some operational risks, measures are necessarily qualitative rather than quantitative!
QUANTITY OF RISK

- Frequency and severity
  - High frequency / Low impact
  - Low frequency / High impact
- Probability
QUANTITY OF RISK - HIGH

People:

- Staff performing operational duties demonstrate unfamiliarity with job requirements or are not adequately trained.
- Turnover is at a level where difficulty filling open positions impacts the business process and/or the number of assets per employee significantly exceeds peer.
- Critical activities are heavily dependant on a small number of staff / management (e.g., their loss will significantly impact operations).
- Staff size small in relation to peer, or the volume and complexity of activities conducted. Workloads such that staff frequently works overtime.
QUANTITY OF RISK - HIGH

Process:
- Activities consists of multiple control points, several interrelationships with other activities, and/or requires a high level of staff proficiency.
- Activities where transaction volume is high relative to infrastructure capacity, and/or significantly exceeds peer transaction volumes.
- Activities with individual transactions of above-average monetary value, or where core activities pose a high dollar exposure.
- Business process requires extensive manual processing.
- The organization: is undergoing significant changes (mergers, consolidations, or system conversions); maintains branch offices, operations centers, and personnel over several states or countries; and/or has a significantly greater number of facilities per asset size than peer.
QUANTITY OF RISK - HIGH

Systems:

- The organization’s business operations are highly dependent on an extensive, complex network infrastructure.
- Performance upgrades and capacity planning hampered by serious system constraints, and/or substantial system downtime.
- Existing/legacy systems unstable. Obsolete or not supported effectively by outside vendor or in-house staff.
- Excessive access granted to internal/external parties for critical applications/data.
- Significant amount of complex systems development and acquisition projects in light of the entity’s size and complexity. Projects affect critical business processes.
- The rate of adoption of technological change and the aggressive implementation of emerging technologies may impact the organization’s ability to operate its internal systems.
QUANTITY OF RISK - HIGH

External Events:

- The organization operates in areas highly susceptible to natural disasters, or infrastructure dislocations (e.g., water quality, telecommunications, and electrical power).
- The organization operates in areas highly susceptible to acts of war or terrorist activity.
- The organization engages in businesses with highly complex laws and regulations (e.g., cross-border issues, securities law).
- Significant reliance on outsourcing arrangements / outside vendors for critical services or systems.
- Market is highly competitive and several other financial institutions are creating pressure for changes in product or technology.
- Activities that are highly susceptible to major-market fluctuations, (e.g., capital markets, labor markets, stock markets, etc.).
QUANTITY OF RISK - MODERATE

People:

- Staff possesses basic skills to perform job responsibilities. Some staff may require additional expertise and guidance.
- Turnover precludes the business from retaining optimal staffing levels; however, basic business functions satisfactorily.
- Critical activities are supported by a reasonable number of key staff / management.
- Staff size adequate in relation to peer, or the volume & complexity of activities conducted; overtime is insignificant.
QUANTITY OF RISK - MODERATE

Process:
- An activity that consists of traditional well-established products and services, and requires some experience as a prerequisite (e.g., retail services, trade finance, commercial lending).
- Infrastructure on par with volume.
- An activity with individual transactions of average monetary value.
- The organization is moving toward straight-through processing and currently has limited manual intervention.
- The organization is implementing insignificant mergers, consolidations, or conversions.
- The organization maintains branch offices, operations centers, and personnel within a regional geographic area.
QUANTITY OF RISK - MODERATE

Systems:
- The organization’s business operations utilize industry standard networks.
- Systems are flexible enough to upgrade performance levels and increase capacity within reasonable time frames.
- Existing / legacy systems relatively stable and supported adequately by outside vendor or in-house staff, but significant enhancements may be necessary to support all or parts of critical business processes.
- Restricted access granted to internal / external parties.
- Manageable amount of systems development and acquisition projects given the entity’s size and complexity.
- The organization retains a reasonable level of technological innovation, and selectively implements emerging technologies that are consistent with its business plan.
QUANTITY OF RISK - MODERATE

External Events:

- The organization operates in areas with limited potential for, or some prior history of natural disasters and / or has access to relatively stable infrastructure with some providers available.
- The organization operates in areas with limited potential for acts of war or terrorist activity.
- The organization engages in businesses which have a generally stable legal framework, however, it may engage in activities with some exposure to legal and regulatory issues.
- Moderate reliance on outsourcing arrangements/outside vendors for standard, noncomplex services.
- The market is moderately competitive and only a few competitors exist, with modest pressure for changes in products or technology.
- Activities with average susceptibility to market fluctuations.
QUANTITY OF RISK - LOW

People:

- Staff is knowledgeable and proficient in performing job responsibilities.
- Turnover is low and/or the number of assets per employee is significantly less than peer.
- Critical activities are supported by a considerable number of staff/management (e.g., the loss of individual staff members has little impact on operations).
- Staff size generous in relation to peer, or the volume and complexity of activities conducted. Staff rarely works overtime.
QUANTITY OF RISK - LOW

Process:

- Activity consists of few control points; simple, easy to understand activities and a relatively non-specialized knowledge base (e.g., teller operations, check processing).
- Volume well below infrastructure capacity and / or is far less than peer transaction volumes.
- An activity with individual transactions of below-average monetary value (e.g., items processing).
- Extensive use of straight-through processing with little or no manual intervention.
- The organization is relatively stable with no major mergers, consolidations, or system conversions.
- branches, operations center, and personnel operate within a local geographic area, and / or the firm has a significantly smaller number of facilities per asset size than peer.
QUANTITY OF RISK - LOW

Systems:

- The organization uses simple networks of proven network components with minimal reliance on new technologies (e.g., land based voice networks).
- Minimal resources required upgrading performance levels and increasing system capacity as warranted.
- Existing / legacy systems stable and receive effective vendor / in-house support. Systems support business strategies.
- Logical / physical access is appropriate for the size and complexity of operations.
- Level of systems development and acquisition projects appropriate for entity’s size and complexity.
- The organization adopts technological change only after it has been proven effective with minimal reliance on emerging technologies and a robust systems development life cycle process.
External Events:

- The organization operates in areas not known to be susceptible to natural disasters and/or operates in geographic areas with varied and robust access to infrastructure facilities.
- The organization operates in areas not known to be susceptible to acts of war or terrorist activity.
- The organization operates in an environment with a relatively stable and thoroughly tested laws and regulations (e.g., consumer compliance regulations).
- Reliance on outsourcing arrangement / outside vendors is minimal.
- Competition in the market is slight and there is little or no pressure for changes in products or technology.
- Market fluctuations have little effect on the institution’s business lines.
### INHERENT RISK:

#### Overall

<table>
<thead>
<tr>
<th></th>
<th>High</th>
<th>Moderate</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Processes</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Systems</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Overall</td>
<td>?</td>
<td></td>
<td>?</td>
</tr>
</tbody>
</table>
QUALITY OF RISK MANAGEMENT

- Board and Senior Management Oversight
- Policies, Procedures, and Limits
- Measurement, Monitoring, and MIS
- Internal Controls and Internal Audit
BOARD & SENIOR MANAGEMENT OVERSIGHT

What to look for
- Operations & technology oversight
- Board diversity; management experience

Information sources
- Organization charts
- Committee minutes
- Board & committee packages
POLICIES, PROCEDURES, AND LIMITS

What to look for

- Policies, procedures & limits for major operational areas
- Policy compliance testing and enforcement

Information sources

- Policy, procedures, & limits documentation
- Compliance mechanisms; exception reports
MEASUREMENT, MONITORING, AND MIS

What to look for

- Comprehensive & appropriate board, committee, and management reporting
- Reporting validation

Information sources

- Board and committee packages; management reports
- Internal audit reports
INTERNAL CONTROLS AND AUDIT

What to look for

- Effective control environment
- Audit staff knowledgeable of operations and technology risks

Information sources

- Internal audit risk assessments and audit plan
- Internal audit reports
- External auditor management letters
RISK MANAGEMENT - STRONG

- Management clearly understands and actively manages operational risks. Risk management practices are appropriately adjusted to reflect industry and regulatory developments.

- A comprehensive written operational risk management framework place, including an appropriate definition, tolerance levels, and effective processes for identification, assessment, response, monitoring, and controls. The framework is consistent with the institution’s size, complexity, and risk profile. Policies clearly delineate accountability and lines of authority across the institution’s activities. Policies provide for the review of new activities before they are initiated.

- Monitoring and MIS reports address all material risks. Assumptions, data sources, and procedures used for monitoring are appropriate, adequately documented, and tested for reliability. Operational risk is systematically identified and assessed at least annually. Indicators have been developed for the most important risks. Comprehensive reporting is included in regular board and executive packages.
RISK MANAGEMENT - STRONG

- The audit function exceeds expectations. Risk-assessment processes comprehensively identify and routinely monitors risk. The board actively oversees internal and external audit functions. Audit staff is qualified, sufficient, and independent. Risk-assessment allows audit managers to quickly adapt to changing conditions. Audit plans and scope are well defined and provide full coverage within the audit cycle. Work programs are appropriate. Audit reports are actionable, and there is immediate corrective action to resolve audit and regulatory concerns.

- No internal control weaknesses exist in high-risk areas, and weaknesses in low-risk areas are minor. Identified control weaknesses are addressed timely. Material assets are safeguarded against unauthorized access. Segregation and rotation of duties are in place and enforced. Potential conflicts of interest are identified, minimized, monitored, and reviewed. Authority and risk limits are documented and enforced. Staffing is appropriate and employees are well-trained and competent. Performance and exception reports are reviewed, variances investigated, and appropriate action taken. Reconciliations, verifications, and controls testing are timely and effective in all material areas. Timely self-assessments have identified no—or minimal—exceptions, and audit has verified the findings.
The board and senior management have a good understanding of operational risks and provide adequate oversight, although practices may be lacking in some modest degree.

A written framework is in place for managing operational risk, covering all major business areas. Any deficiencies or gaps are minor in nature and in the process of being addressed. Policies provide for the review of new activities before activities are initiated.

Monitoring and MIS reports for operational risk cover major risks and business areas. The institution is beginning to comprehensively identify and assess operational risk, but some risks are inadequately covered or documented. Some indicators have been developed, but some key risks are omitted, or monitoring needs improvement. Some reporting of operational risks is done, but the quality is uneven and not on a par with credit and market risk.
RISK MANAGEMENT - ACCEPTABLE

- Only minor internal control weaknesses are found in higher-risk processes. More significant concerns may be noted in low-risk business lines, but no weakness significantly impacts safety and soundness. All weaknesses are correctable in the normal course of business. Segregation of duties is in place in all high-risk processes, and inability to segregate duties in lower-risk areas is mitigated. Conflicts are appropriately identified and monitored, but additional action may be needed to minimize them. Authority and risk limits are in place, but compliance monitoring may need improvement. Employees responsible for high-risk functions or critical control processes have appropriate expertise. Lower-risk processes may be lacking in proper self-assessments. Audit has identified only minor exceptions to self-assessment findings.

- The internal audit function is adequate. Staffing is adequate, and auditors are independent. Risk-assessment processes adequately identify and periodically monitor risk. Annual risk assessments and audit plans are defined but may require clarification, better coordination, or improved communication. Audit management anticipates but fails to respond quickly to changes in market, business, and technology. Work programs include appropriate general steps but may not be sufficiently detailed. Audit reports include all findings and management normally takes appropriate action; however, too much reliance is placed on audit and regulatory intervention to identify and resolve concerns.
RISK MANAGEMENT - WEAK

- Management may not be adequately informed about key aspects of operational risk and may not be able to provide timely corrective actions for deficiencies identified. Deficiencies involve a wide range of activities or are material to a major business line or activity and include lack of knowledge, insufficient oversight of risk management, under-utilized management reporting, or inability to respond to industry or regulatory developments.

- A written framework for managing operational risk may be lacking or may not adequately identify, assess, monitor, or control key operational risks. These deficiencies involve a wide range of activities or are material to a major business line or activity. Policies may not be consistent with the institution’s size, complexity, and risk profile. Policies may not provide for adequate due diligence before engaging in new activities or products.

- There may be no comprehensive identification or assessment of operational risk, or risk identification may be impaired by inappropriate assumptions, inaccurate data, poor documentation, or lack of testing. Deficiencies involve a wide range of activities or are material to a major business line or activity. Operational risk may not be monitored or reported as a separate discipline. MIS reports may not be distributed to the appropriate decision-makers, adequately monitor significant risks, or properly identify adverse trends and the level of risk faced by the institution.
RISK MANAGEMENT - WEAK

- There are serious chronic weaknesses that require substantial improvement in internal controls. Conditions may result in unreliable financial records or managerial reports, or in operating losses affecting safety and soundness. Management has been unresponsive or slow to correct control weaknesses. Material assets are not appropriately safeguarded. Job duties in high-risk processes are not appropriately segregated. Conflicts are not disclosed or are not monitored to restrict inappropriate transactions. Authority and risk limits are either absent or not enforced in material functions or processes. Employees in high-risk areas or responsible for critical control points lack expertise. Performance and exception reports are not generated, or variances are not investigated. Reconciliations and verifications are not timely. Self-assessments are not completed or audit has found them ineffective.

- The audit function is inadequate. The board provides little or no oversight. Audit staff may lack the expertise or independence to perform its duties. Risk assessments do not effectively identify risks and may not be appropriate for the size, complexity, or risk profile of the organization. Annual audit plans do not provide adequate audit coverage for the audit cycle or may not provide adequate audit programs for auditable units. Management has difficulty responding to changes in business, market, and technology. Work programs do not address all controls to be tested. Audit reports do not include all findings or may not be rated. Management is generally reactive to audit or regulatory exceptions. Repeat concerns may exist, indicating that management lacks the ability or willingness to resolve concerns.
RISK ASSESSMENT: Determine Trend

- The probable change in the risk profile over the next 12 months. The risk trend is characterized as decreasing, stable, or increasing.
- The direction of risk often influences the supervisory strategy, including how much validation is needed.
RISK ASSESSMENT: Develop Hypothesis

High Quantity
Strong RM Process

High Quantity
Weak RM Process

Weak RM Process

Low Quantity
Weak RM Process

Low Quantity
Strong RM Process

High Exposure

Low Exposure
RISK ASSESSMENT:
Examination Scope Based on Hypothesis

**High Qty. - Weak Mgmt.**
- Confirm risk assessment
- Low reliance internal measures
- Full on-site procedures

**Low Qty. - Weak Mgmt.**
- Confirm risk assessment
- Low reliance internal measures
- Target “Management” section of on-site procedures

**High Qty. - Strong Mgmt.**
- Confirm risk assessment
- Rely on internal measures
- Modified on-site procedures targeting specific areas

**Low Qty. - Strong Mgmt.**
- Confirm risk assessment
- Rely on internal measures
- Minimal on-site procedures
Risks Are Interactive

Reputational

Market

Operational

Legal

Credit

Liquidity

Risk Relationship
OPERATIONAL RISK
RISK ASSESSMENT

Questions
RESOURCES

- “Internal Control – Integrated Framework,” Committee of Sponsoring Organizations (COSO)