OPERATIONAL RISK

EXAMINATION TECHNIQUES
OVERVIEW

• Examination Planning
• Oversight
• Policies, Procedures, and Limits
• Measurement, Monitoring, and MIS
• Internal Controls and Audit
Risk Assessment: Develop Hypothesis

- High Quantity
  - Weak RM Process
    - High Exposure
  - Strong RM Process
    - Low Exposure
- Low Quantity
  - Weak RM Process
    - High Exposure
  - Strong RM Process
    - Low Exposure
Exam Scope - Based on Risk Assessment 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
TRANSACTION TESTING

Inherent Risk

+ Knowledge of Processes, Systems, and Controls

= Amount & Type of Transaction Testing

In addition to transaction testing, the quality of risk management is reviewed and validated.
QUALITY OF RISK MANAGEMENT
- OVERSIGHT -

Operational Risk Governance Is Different

- Operational risk has always existed; our focus is relatively new
- Operational risk involves multiple disciplines
- Operational risk crosses business boundaries and has interdependencies
- Operational risk includes technology
QUALITY OF RISK MANAGEMENT - OVERSIGHT -

Components of Oversight

- Governance, guidance, and monitoring
- Integrated Control and Reporting Framework
- Infrastructure
QUALITY OF RISK MANAGEMENT
- OVERSIGHT -

Governance, Guidance, and Monitoring

- Active monitoring and direction by the board
- Management and supervision by the executive officers and line of business heads
- Policies and standards
QUALITY OF RISK MANAGEMENT
- OVERSIGHT -

The Board’s Role in Managing Operational Risk

- Define operational risk
  - Are critical areas of operational risk identified? Is a common risk language used? Is operational risk management a discipline equal to credit and market risk?

- Understand key operations that drive product and service delivery and their risks
  - Does the board understand operations and associated risks? Is an educational program in place where needed?

- Communicate risk tolerance and policy guidelines
  - Do policies complement strategy? Are limits and thresholds articulated? Are policies widely and clearly communicated?

- Monitor operational risk
  - Is risk reporting in board packages? Do reports address limits?

- Measure performance
  - Does reporting measure operational performance as well as risk management?
QUALITY OF RISK MANAGEMENT

- OVERSIGHT -

Executive Management’s Role in Managing Operational Risk

- Translate board risk tolerances into detailed policies and procedures
  - Do written procedures exist for all key processes? Are they consistent with broad policies and the organization strategy?
- Implement appropriate controls
  - Are processes mapped / documented and controls implemented?
- Validate control effectiveness
  - Are internal audit, self-assessment, and quality assurance programs implemented?
- Identify and monitor key operational metrics to establish accountability
  - Does management receive sufficiently detailed reports to monitor activity, risk level, and compliance with limits?
- Measure performance
  - Are operations monitored for variances in quality and effectiveness?
QUALITY OF RISK MANAGEMENT
- OVERSIGHT -

Integrated Control and Reporting Framework

- Comprehensive control framework
  - Does the control and risk management framework encompass the entire organization and all of its operational risks?

- Adequate MIS and risk reporting
  - Are reports generated for all identified risks? Do reports address current operations (performance) as well as future or emerging risks?

- Sound accounting and auditing practices

- Appropriate IT and business continuity planning
  - Are contingency plans in place for IT and critical business lines and tested annually?

- Sufficient risk management

- Suitable compliance
  - Does operational risk management also address compliance with laws and regulations?
Risk Management: Enterprise versus Business Lines

- Many individual risks are appropriately managed within business lines and functional support areas
- Other operational activities—such as IT infrastructure and information security administration—support multiple business lines, serving as a source of risk to each business unit and a conduit for risk migration throughout an institution

Examiner considerations: Does the enterprise risk view complement business line and functional area views? Are all risks represented? Are there common language, standards, and measurements for all areas? Have appropriate enterprise and business line tools for assessing and managing risks been implemented? Is there independent validation?
QUALITY OF RISK MANAGEMENT

- OVERSIGHT -

Infrastructure Adequacy:
Current and Future

- Appropriate planning for changes in business size, scope, and activities, including strategic planning, controls framework, information technology, personnel, policies, and standards
QUALITY OF RISK MANAGEMENT
- OVERSIGHT -

Examination Red Flags

- Board composition and demographics
  - Lack of operations background; Dominant official; Organization culture does not emphasize controls, transparency, and ethics; Oversight inconsistent with culture or cultural weaknesses exist

- Enterprise-level governance
  - Risks managed within business lines, but not across company

- Operations & technology oversight committees
  - No board or senior management committees for technology and operations; Lack of appropriate board and management representation; Participation is too narrow

- Roles and reporting lines
  - Roles are not clearly defined; Reporting lines are ambiguous

- Strategic operations & technology planning
  - No strategic technology and operations planning; Technology and operational planning not consistent with business plan

- Board reporting
  - Inadequate or absent operations reporting; MIS does not report on identified risk areas

- Internal controls and auditing
  - Limited or static audit programs; Over-reliance on external audit or examiners
Purpose of Policies, Procedures, and Limits

- Define responsibility and accountability for risk management decisions
- Define the strategies and processes for managing and mitigating risks in business lines and support areas, and for the institution as a whole
- Identify the frequency, methods, and metrics for measuring and monitoring risks
- Specify quantitative or qualitative residual risk thresholds or tolerances
QUALITY OF RISK MANAGEMENT - POLICIES, PROCEDURES, LIMITS -

Clear Lines of Authority and Responsibility

Responsibilities and accountabilities should address:

- Developing and implementing strategies and tactics for managing and mitigating risk
  - Are risk management strategies consistent with the business strategy and culture?
- Establishing and maintaining risk measurement and monitoring systems
  - Do individuals with specialized skills assess, monitor, and manage risks?
- Identifying, assessing, and approving potential risks related to new products, services, activities, or processes prior to implementation
  - Is a formal review and approval process in place? Is there appropriate representation?
- Developing risk management policies, procedures, and tolerances; authorizing exceptions; and reporting deviations
  - Are authorities and responsibilities clearly defined? Is accountability enforced?
QUALITY OF RISK MANAGEMENT
- POLICIES, PROCEDURES, LIMITS -

Authorized Activities

- Requires a common risk language and framework to ensure that risks are consistently identified and assessed.
  - Is a standardized risk assessment process or methodology in place for consistency?
- A review and approval process to assess risks in significant new or changed products, services, processes, and activities; mitigation or management strategies should be utilized concurrent with rollout or implementation.
  - Does the process require a clear description of new product / activity, inherent risk identification, planned controls, tolerances, and monitoring metrics?
- Identify the nature, type, and extent of use for instruments permissible for managing risk, either specifically or by their characteristics.
  - Are risk management tools or activities defined and consistent with the appetite for residual risk?
QUALITY OF RISK MANAGEMENT
- POLICIES, PROCEDURES, LIMITS -

Limits

- A framework for identifying and assessing risks—as well as residual risk after mitigation strategies—is required to establish quantitative or qualitative risk limits.
  - Is the rationale for tolerances documented and reasonable?
- The risk management framework should be an element of a well-articulated corporate strategy that establishes measurable corporate goals.
  - Is operational risk management one of the organization’s strategic initiatives?
- Aggregate operational risk limits clearly articulating acceptable residual risk should be approved by the board and periodically re-evaluated.
  - Are risk limits adjusted as the organization or its operating environment change, or at least annually? Is the review and approval process documented?
LIMITS (continued)

Limits should:

- Be appropriate to the culture, size, complexity, and financial condition.
  - Are tolerances consistent with skills, sophistication, or financial condition?

- Be consistent with the overall approach to measuring, managing, and monitoring risk, and address the potential impact of changes in the environment as well as internal operations.
  - Are tolerances beyond management or systems capacity for monitoring and managing?

- Be appropriate for the scale, diversity, and complexity of activities and the environment.
  - Are the limits appropriate relative to earnings, capital, loss reserves, or mitigants?

- Consider routine and predictable risks as well as infrequent but significant external events.
  - Are tolerances developed on historical experience as well as probable events? Is modeling used—where appropriate—for infrequent, high impact operational losses?
QUALITY OF RISK MANAGEMENT
- POLICIES, PROCEDURES, LIMITS -

Examination Red Flags

- Limits, tolerances, and thresholds
  - Excessive limits and residual risk volumes

- Written and comprehensive
  - Lack of documentation; Do not cover all important operational areas; Do not establish risk thresholds or limits, or are otherwise vague

- Processes for development & revision
  - No formal process for regularly updating policies as risks profile changes; Review is infrequent relative to rate of organizational change; Authority and responsibility for review and update are unclear

- Training & communication
  - No orientation program; No ongoing training; Policies and procedures not readily and widely available

- Roles and reporting lines
  - Roles and reporting are informal; Weak or absent accountability

- Compliance, enforcement, & exception reporting
  - No processes for monitoring compliance or reporting and tracking exceptions
QUALITY OF RISK MANAGEMENT - MEASUREMENT, MONITORING, MIS -

Key Elements of Risk Measurement, Monitoring & Reporting

- Regularly identify and assess all material operational risks.
- Identify and assess operational risk before making major changes in operations.
- Develop appropriate risk indicators.
- Senior management and the board—or a board committee—should receive regular reports on its operational-risk profile.
QUALITY OF RISK MANAGEMENT
- MEASUREMENT, MONITORING, MIS -

Identify and Assess Material Risks

Multi-dimensional approach:
- internal factors
- external factors
- major business lines
- major support functions

Examiner considerations: Do identification and assessment methodologies consider all business lines and activities? Does the methodology produce consistent results? Does it include quantitative and qualitative measures?
QUALITY OF RISK MANAGEMENT
- MEASUREMENT, MONITORING, MIS -

Identify and Assess Material Risks
(Continued)

Materiality and quality of mitigants
- Frequency and severity
  - High frequency / Low impact
  - Low frequency / High impact
- Probability
- Effectiveness of controls and mitigants

Examiner considerations: What is the source of risk data (internal, external, both)? Does data cover entire business cycle? How is probability estimated or derived? How are control and mitigant effectiveness measured?
Measure & Report

QUALITY OF RISK MANAGEMENT - MEASUREMENT, MONITORING, MIS -

**Identify and Assess Material Risks (Continued)**

Risk assessment skill sets:
- In-depth knowledge of the business lines
- Strong risk-management and control perspective

Risk assessment tools
- Risk control self assessments
- Risk mapping
- Loss data analysis

Examiner considerations: Are business line managers experienced in risk identification and management? Are tools adequate in scale, scope, variety, and applicability? Are assessment tools and outcomes validated?
QUALITY OF RISK MANAGEMENT
- MEASUREMENT, MONITORING, MIS -

Identify and Assess Risk Before Major Changes

- New products
- Material changes in or expansions of existing processes
- Mergers and acquisitions

Examiner considerations: Is the process formal? Is it documented? Appropriate participants: legal, audit, marketing, information security, contingency planning, key business lines and functional areas?
QUALITY OF RISK MANAGEMENT
- MEASUREMENT, MONITORING, MIS -

Develop Appropriate Risk Indicators

Risk Indicators should:
- Focus attention on the most important risks
- Be timely; material adverse events should be promptly escalated
- Be forward looking
- Be tailored to the needs of the audience
- Include qualitative and quantitative metrics
- Be accurate and subject to periodic verification
- Be reported consistently over time
- Use graphic presentations where practical
QUALITY OF RISK MANAGEMENT
- MEASUREMENT, MONITORING, MIS -

Regular Board and Management Reporting

- Regularly identify and assess all material operational risks.
  - Is there a relevant report for each identified risk area or limit?
- Identify and assess operational risk on an ad hoc basis before making major changes in operations.
  - Are new risk reports implemented when significant new process, systems, or products introduced?
- Develop appropriate indicators to provide early warning of an increased risk of future operational risk losses.
  - Do risk reports identify new and emerging risks as well as current performance? Are escalation triggers in place and included in reports?
- Senior management and the board—or a board committee—should receive regular reports on its operational-risk profile.
  - Does risk reporting also include educational material where necessary?
QUALITY OF RISK MANAGEMENT
- MEASUREMENT, MONITORING, MIS -

Regular Board and Management Reporting (continued)

Examples of reporting content

- Risk control self assessment results
- Issues
- Loss-event data
- Forward-looking indicators
- Other
QUALITY OF RISK MANAGEMENT - MEASUREMENT, MONITORING, MIS -

Examination Red Flags

- Risk assessment process and results
  - Risk assessments not comprehensive; Management skills sets inadequate for risk identification and management; Assessment tools are inadequate

- Risk measurement metrics
  - Not relevant to identified risks; Not focused on both current and future risks; Not independently validated

- Reporting
  - Irregular, inconsistent, & not understandable; Does not include escalation triggers; Reports on business line only without enterprise perspective
QUALITY OF RISK MANAGEMENT
- INTERNAL CONTROLS & AUDIT -

Internal Control Activities

- Safeguarding assets
- Segregating and rotating duties
- Identifying, minimizing, and monitoring conflicts
- Establishing and enforcing authorities and risk limits
- Maintaining staff levels and expertise
- Conducting ongoing monitoring
Safeguarding Assets

- Original documents protected against destruction or loss
- Access to marketable or negotiable assets under dual control
- Access to systems is controlled
- Audit trails for transactions are documented
- Numerical sequences for documents and transactions are logged and inventoried
QUALITY OF RISK MANAGEMENT
- INTERNAL CONTROLS & AUDIT -

Segregating & Rotating Duties

- Segregation in organizational charts and actual practice
- Accounting for and access to assets is segregated
- Duty rotations & vacations; approval for exceptions
- Transaction origination, processing, and reconcilement are segregated
- IT operations are separate from programming and testing
- Approval of funds disbursement and the actual disbursement are segregated
- Responsibility for customer and proprietary accounts are segregated
QUALITY OF RISK MANAGEMENT
- INTERNAL CONTROLS & AUDIT -

Identify, Minimize, and Monitor Conflicts

- Employees must disclose close affiliations or relationships
- Procedures and systems are designed to restrict transactions with declared personal interests or relatives
- Conflicts are independently reviewed and monitored
- Instances of noncompliance are documented and reported to management. Suspicious activity reports are filed when appropriate
- Credit reviews are completed for key employees
QUALITY OF RISK MANAGEMENT
- INTERNAL CONTROLS & AUDIT -

Establish and Enforce
Authorities and Limits

- Risk limits and approval authorities are clearly established and communicated via policies, procedures, or guidelines
- Adherence to risk limits or thresholds is closely monitored
- Exceptions to limits are infrequent, documented, and reported to management
QUALITY OF RISK MANAGEMENT
- INTERNAL CONTROLS & AUDIT -

Maintain Staff Levels and Expertise

- Screening procedures—background checks & credit reviews—particularly for employees in high risk positions
- Effective communication about duties and control responsibilities; Job descriptions and reference manuals
- Communication of policies and procedures
- New employee training and orientation
- Periodic ongoing training
- Accountability for responsibilities and authorities
QUALITY OF RISK MANAGEMENT
- INTERNAL CONTROLS & AUDIT -

Conducting Ongoing Monitoring

- Periodic reconciliation of accounting systems and actual physical asset counts
- Effective Information security monitoring
- Regular review and revision of policies and procedures
- Management review of performance and exception reports; Investigation of and action taken on significant variances
- Overrides are monitored and appropriate corrective action is taken
QUALITY OF RISK MANAGEMENT
- INTERNAL CONTROLS & AUDIT -

Conducting Ongoing Monitoring (continued)

- Timely, independent account reconciliation ensures that outstanding items are resolved and cleared
- Regular reviews of high-risk accounts and expense reports
- Periodic self-assessments or evaluations of the design and effectiveness of internal controls
QUALITY OF RISK MANAGEMENT  
- INTERNAL CONTROLS & AUDIT -

Core Components of the Audit Function

- Board oversight of the audit function
- Audit department staffing and structure
- Risk and control assessments
- Audit planning
- Audit program content and execution
- Reporting and resolution of audit findings
QUALITY OF RISK MANAGEMENT
- INTERNAL CONTROLS & AUDIT -

Proactive Board Oversight

The audit committee:

- Is guided by a charter
- Includes outside directors with the necessary business, financial, and/or internal control expertise
- Packages facilitate monitoring audit effectiveness and major risk categories, including operational risk
- Approves all deviations from the plan and has the authority to request additional audits or follow-up audits
- Approves any special projects requested of the internal audit function
- Meets with the internal auditor at each meeting without management
- Has the authority and the funding to engage consultants or legal expertise
QUALITY OF RISK MANAGEMENT
- INTERNAL CONTROLS & AUDIT -

Competent Audit Staff;
Independent Structure

- Audit department reports to a high level executive
- Not restricted from any areas or information
- Duties exclude management or operational functions that could impair independence
- Staffing reflects the complexity, structure and size of the bank. Staff skill sets are adequate to review inherent operational risks
- Training ensures skill sets remain adequate for changing operational risks
- Specialized skills are developed or contracted for more complex audits
QUALITY OF RISK MANAGEMENT
- INTERNAL CONTROLS & AUDIT -

Risk and Control Assessments

- The audit committee should review and approve risk assessments
- Assessments should address operational risks by business line and functional area, as well as for the overall enterprise
- The audit function should collaborate with line management in risk and control assessments
- Risks and controls should be continuously updated for environmental changes
- The formality, sophistication, and documentation of the risk assessment process should be appropriate to the institution
QUALITY OF RISK MANAGEMENT
- INTERNAL CONTROLS & AUDIT -

Audit Planning

- Audit plans should address individual as well as enterprise operational risks
- Audit plans should be adjusted for changes in the operational risk profile or environment
- Audit frequency should be based upon the identified level of risk
- The use of outside or contract resources should be addressed in the audit plan
QUALITY OF RISK MANAGEMENT
- INTERNAL CONTROLS & AUDIT -

Program Content and Execution

- Work programs should explicitly address identified operational risks
- The level of transaction testing should be sufficient to validate operational risk controls
- Work programs should include testing of compliance with laws and regulations
Quality of Risk Management

- Internal Controls & Audit -

Reporting and Issue Resolution

- Reports should clearly identify operational and control weaknesses.
- Operational and control weaknesses should be rated for severity or importance.
- Reports should establish line or operational managers responsible for corrective action and the time frames for corrections.
- Exceptions should be tracked until resolved.
- There should be an escalation process for unresolved exceptions, particularly for high priority operational and control weaknesses.
- Audit should promptly validate the completeness and effectiveness of corrective actions.
QUALITY OF RISK MANAGEMENT
- INTERNAL CONTROLS & AUDIT -

Examination Red Flags

- Internal Controls
  - Data integrity is poor or inconsistent; Lack of numerical consistency in reports; Controls over data entry insufficient or ineffective
  - Systems access is excessive and beyond business needs
  - Segregation of duties or dual controls are lacking in key control areas
  - Security monitoring is weak, absent, or lacks independence
  - Continuity planning is inadequate at business line or functional support areas, or for the enterprise as a whole
  - Reconcilements are infrequent; Reconcilements are not independently reviewed; Outstanding items not handled timely
  - Hiring and background checking processes are weak; Chronic staff shortages and vacancies in key positions
QUALITY OF RISK MANAGEMENT
- INTERNAL CONTROLS & AUDIT -

Examination Red Flags

- Audit
  - Staffing is inadequate; key skills missing
  - Training inadequate for operational risks; Training budget doesn’t support professional development
  - Outsourced vendor management is delegated to executive with operational responsibilities
  - Risk assessment universe is inadequate; Process is not lacks sophistication or completeness; Rating system overly subjective or unevenly applied
  - Audit program scope & procedures incomplete or undocumented; Key risks omitted; Limited or no transaction testing
  - Focus is on technology versus people & processes
  - Communication of risk issues is poor or incomplete; Issues not ranked for criticality; Accountability not established
OPERATIONAL RISK EXAMINATION TECHNIQUES

Questions