Module Outline
ECF on Operational Risk Management (ORM)
Module 3 "Fundamentals of Operational Risk Management and Risk Governance"

Benchmarked HKQF Level:	4
No. of Credits:	20
Total Notional Learning Hours:	200
a) Class contact hours:	*15 hours (3-hour per session x 5)*
b) Self-study hours:	*182.5 hours*
c) Assessment hours:	*2.5 hours*
Pre-requisite:	N/A

Module Objective

The module aims to provide candidates with the concepts and building block of operational risk, the operational risk governance and framework. It also aims to equip the learners to adopt the operational risk principles into practice; execute the operational risk management cycle; and integrate with other risk functions to promote holistic view of risks.

Module Intended Outcomes (MIOs) and Units of Competencies (UoCs)

Upon completion of the Module 3, candidates should be able to:

MIOs	Intended Outcomes / Competence	*Unit of Competencies (UoCs)
MIO-1	Describe the objectives and the types of Operational Risk Management.	107405L5 107424L5 / 109369L5 107408L4 107409L4 109303L4 109310L5
MIO-2	Establish solid operational risk governance, define clear roles and responsibilities and support risk culture in the organisation.	
MIO-3	Implement and practice the operational risk principles and define the operational risk appetite.	
MIO-4	Execute the operational risk assessment, measurement and reporting.	
MIO-5	Apply and incorporate with technology, resiliency and enterprise risk assessment.	

**Note: For the details of the UoCs, please refer to the Specification of Competency Standards (SCS) of Retail Banking and Corporate & Commercial Banking which were developed by HKCAAVQ.*

Assessment

Examination duration:	2.5 hours
Examination format:	Multiple Choice Questions (MCQ) with 80 questions
Pass mark:	70%

Syllabus

Chapter 1: Overview Of Operational Risk	
1.1	**Introduction**
1.2	**Definitions**
1.2.1	- Definition of Risk Management
1.2.2	- Importance of Risk Management
1.2.3	- Types of Operational Risks faced by the Bank
1.2.4	- Taking Risk as Integral Part of Banking
1.2.5	- Definition and Types of Inherent Risks
1.2.6	- CAMEL Process
1.2.7	- Risk Management System
1.2.8	- Risks in Banking and Financial Services
1.2.9	- Evolution of Operation Risk
1.2.10	- Business Lines of the Banking Industry
1.2.11	- Definition of Risk (ISO 31000)
1.2.12	- Difference between Certainty VS Risk VS Uncertainty
1.2.13	- Definition of Operational Risk
1.2.14	- Operations Risk VS Operational Risk
1.2.15	- Inherent Risk VS Residual Risk
1.2.16	- Preview on Top 10 Operational Risks
1.2.17	- Top Operational Risk Issues Discussed in Board Room
1.2.18	- Operational Risk Management Framework
1.2.19	- FDIC 2024 Operational Risk Review

1.3	**Drivers**
1.3.1	- Benefits of Operational Risk Management
1.3.2	- Value of Operational Risk Management
1.3.3	- Key Deliverables of Sound Operational Risk Management
1.3.4	- Drivers of Good Operational Risk Management
1.3.5	- Lesson Learnt on Drivers Leading to 2008 Financial Crisis
1.3.6	- Reasons Leading to Management of Operational Risk
1.3.7	- Key Internal Operational Risk Drivers
1.3.8	- Categories of Operational Risk Drivers
1.3.9	- Operational Risk Causal Factors
1.3.10	- Process Factors
1.3.11	- People Factors
1.3.12	- System Factors
1.3.13	- External Factors
1.3.14	- Other Specific Operational Risk Drivers – Culture and Strategy
1.3.15	- Other Specific Operational Risk Drivers – Regulators and M&A
1.3.16	- Other Specific Operational Risk Drivers – Best Practice and Risk Aggregation
1.3.17	- Other Specific Operational Risk Drivers – New Products and Performance & Resource Allocation
1.3.18	- Expectation from Stakeholders
1.3.19	- Use of Operational Risk in Decision Making
1.3.20	- Positioning Operational Risk as Business Enabler
1.4	**Different Types**
1.4.1	- Risk Taxonomy
1.4.2	- Topology of Financial Risks
1.4.3	- Basel Level of Categorisation of Operational Risk
1.4.4	- Basel Categories of Business Lines
1.4.5	- Basel Categories of Event Types
1.4.6	- Typical Types Operational Risks
1.4.7	- Current Market Development that Requires Risk Attention
1.4.8	- Factors Leading to Operational Risk Vulnerabilities
1.4.9	- Samples of Major Prominent Operational Risk Events by Business Functions

1.4.10	- Iceberg Model
1.5	**Risk Analysis Model – Cause, Events, Impact**
1.5.1	- Swiss Cheese Model
1.5.2	- Operational Risk Event and Causal Effects
1.5.3	- ORX Extended Causes and Impact Model
1.5.4	- ORX Operational Loss Industry Pattern
1.5.5	- ORX Extended Causes and Impact Model
1.5.6	- ORX Causes Categories
1.5.7	- ORX Event Categories
1.5.8	- ORX Impact Categories
1.5.9	- Risk Management Sequence
1.6	**Relationship with Other Risk Functions**
1.6.1	- Recap on Risks in Bank
1.6.2	- Linkage of Different Risks to the Risk Event and Impact
1.6.3	- Boundaries of Operational Risk
1.6.4	- Structural Differences between Risk Types
1.6.5	- Risk Relationships and Interconnectivity
1.6.6	- Risk Boundaries – Operational Risk and Credit Risk Examples
1.6.7	- Risk Boundaries – Operational Risk and Market Risk Examples
1.6.8	- Differences between Operational Risk and other types of risks
1.6.9	- Identification – Unit of Measure
1.6.10	- Quantification / Measurement
1.6.11	- Mitigation / Control
1.6.12	- Comparisons between Operational Risk, Market Risk, and Credit Risk Management
1.6.13	- Integrating Related Disciplines in Banks
1.6.14	- Good Risk DNA
1.6.15	- Cooling-off Period for Unsecured Consumer Credit Products
1.7	**Case Studies**
1.7.1	- Case Study: Unauthorized Trading
1.7.2	- Case Study: Staff Embezzlement
1.7.3	- Case Study: Breach of Fiduciary Duties

1.7.4	- Case Study: Leakage of Customer Data
1.7.5	- Case Study: Letters of Credit Card Fraud
1.8	**Best Practice Guidance**
1.8.1	- Use of Risk Exposure Indicators
1.8.2	- Risk Management Adoption Maturity Model
1.8.3	- Looking Forward Risk Radars
Chapter 2: Operational Risk Framework and Governance	
2.1	**Introduction**
2.2	**Risk Governance Structure**
2.2.1	- Operational Risk Management Framework
2.2.2	- Key Recent Regulatory Changes (CG-1, IC-1)
2.2.3	- HKMA Revision to Risk Management Module IC-1
2.2.4	- Elements of a Sound Risk Management System
2.2.5	- General Components of Operational Risk Framework
2.2.6	- ORM Frameworks and Goals
2.2.7	- Corporate Governance
2.2.8	- Operational Risk Governance
2.2.9	- Typical Operational Risk Governance Structure Diagram
2.2.10	- Risk Culture and Operational Risk Governance
2.2.11	- Operational Risk Leadership
2.2.12	- Modes of Accountability
2.3	**Three Lines of Defence**
2.3.1	- Three Lines of Defense
2.3.2	- Responsibilities of Three Lines of Defense
2.3.3	- Evolution of 1.5 Line
2.3.4	- Three Lines of Defence Approach
2.3.5	- An Alternative 'Blended' Approach
2.3.6	- Three Lines of Defence Partnership Model
2.3.7	- Institute of Internal Auditors (IIA)'s Three Lines Model
2.3.8	- Effective Lines of Defense
2.4	**Roles and Responsibilities**

2.4.1	- Roles and Responsibilities
2.4.2	- Role of Board and Senior Management
2.4.3	- Role of Business and Support Units – 1st LOD
2.4.4	- Role of Corporate Operational Risk Function (CORF) – 2nd LOD
2.4.5	- Role of Corporate Subject Matter Specialists – Part of 2nd LOD
2.4.6	- Communication, Consultation and Collaboration Among the Three Lines
2.4.7	- Operational Risk Committee
2.4.8	- Points of Escalation to Various Committees
2.5	**Risk Culture and Indicators**
2.5.1	- Definition of Risk Culture
2.5.2	- Levels of Risk Culture
2.5.3	- Risk Sub-Culture
2.5.4	- Assessing Risk Culture
2.5.5	- Definition of Operational Risk Culture
2.5.6	- Attitudes, Behaviours and Culture
2.5.7	- Importance of Risk Culture
2.5.8	- Risk Culture (Principle 1 of PSMOR)
2.5.9	- Risk Culture Aspects Model
2.5.10	- Some Indicators of Good Risk Culture
2.5.11	- Monitoring Risk Culture: Risk Culture Metrics
2.5.12	- Monitoring Risk Culture: Risk Culture Metrics - Example
2.5.13	- Influencing Risk Culture
2.5.14	- Implication on Strategy and Leadership (Including Tone)
2.5.15	- Implication on Risk Appetite and Tolerance
2.5.16	- Implication on HR Policies and Procedures
2.5.17	- Implication on Communication: Formal and Informal
2.5.18	- Implication on Process and System Design
2.5.19	- Implication on Risk Governance
2.5.20	- Reflection on HKMA Bank Culture Self Assessment
2.6	**Risk Governance on Handling of Emerging Risk**
2.6.1	- Definition of Emerging Risks

2.6.2	- Interconnection of Risks
2.6.3	- Typology of Uncertainties
2.6.4	- Types of Emerging Risk
2.6.5	- ORX 2019 Top Emerging Risks
2.6.6	- Emerging Risk Trend
2.6.7	- Emerging Risk Radar
2.6.8	- Projection of Emerging Top Risks
2.6.9	- Emerging Risk – Cyber Risk
2.6.10	- Emerging Risk – Emerging Technology
2.6.11	- Emerging Risk – Climate Risk Hazards
2.6.12	- Emerging Risk Framework
2.6.13	- Drivers of Emerging Operational Risks
2.6.14	- Contributing Factors to Emerging Operational Risk
2.6.15	- Governance of Emerging Risk
2.6.16	- Risk Biases Leading to Hidden Emerging Risks
2.6.17	- Identification of Emerging Risks and Opportunities
2.6.18	- Tools for Identification of Emerging Risks
2.6.19	- Increasing Awareness of Potential Risks
2.6.20	- Risk Velocity
2.6.21	- Action on Emerging Risk
2.6.22	- Solution to Overcome Risk Biases
2.6.23	- 3rd Line Perspective: ECIIA Top Risk Survey
2.6.24	- Monitoring and Improvement of Emerging Risks Management
2.7	**Case Studies**
2.7.1	- Case Study: Misappropriation of an AI's money by a staff member
2.8	**Best Practice Guidance**
2.8.1	- Building Blocks of Operational Risk Culture
2.8.2	- Embedding Risk in Business Strategy
Chapter 3: Operational Risk Principles and Appetite	
3.1	**Introduction**
3.2	**Principles of Operational Risk Management Framework and Implementation**

3.2.1	- Basel Consultative Paper – Revisions to Principles for the Sound Management of Operational Risk (PSMOR)
3.2.2	- Structure of Principles for the Sound Management of Operational Risk
3.2.3	- Key Objectives of Operational Risk Principles
3.2.4	- Summary of the 12 Basel PSMOR
3.2.5	- Role of Supervisors
3.2.6	- Deep Dive on Operational Risk Framework (Principle 2 of PSMOR) - Framework
3.2.7	- Deep Dive on Operational Risk Framework (Principle 3 of PSMOR) - Governance
3.2.8	- Principles for Effective Risk Management (ISO 31000)
3.2.9	- Stages of ORM Implementation in Banks
3.2.10	- Commencement of Basel III Final Reform Package
3.2.11	- Revised Pillar 3 Disclosure Package
3.3	**Risk Control and Mitigation**
3.3.1	- Definition of Internal Controls
3.3.2	- Deep Dive on Control and Mitigation (Principle 9 of PSMOR)
3.3.3	- HKMA Requirement on Internal control System
3.3.4	- Internal Control Model
3.3.5	- Several Typical Operational Risks in Business Processes and the Related Control Measures
3.3.6	- Internal Control System
3.3.7	- Types of Internal Controls
3.3.8	- Definition of Control Testing
3.3.9	- Types of Internal Control Testing
3.3.10	- Risk Based Internal Control Testing
3.3.11	- Active Failures and Latent Conditions
3.3.12	- Effect of Internal Controls on Risks
3.3.13	- Effectiveness of Controls
3.4	**Operational Risk Planning and Processes**
3.4.1	- Operational Risk Planning
3.4.2	- Overview of Operational Risk Management Process
3.4.3	- Operational Risk Management Process
3.4.4	- Operational Risk Management Process-Broad Steps

3.4.5	- Operational Risk Management Actions and Tools
3.4.6	- The Bow Tie Diagram
3.4.7	- Operational Risk Event, Cause and Effect
3.4.8	- "Swiss Cheese" Model of Defences
3.5	**Operational Risk Appetite Framework**
3.5.1	- Definition of Operational Risk Appetite
3.5.2	- Benefits of Operational Risk Appetite
3.5.3	- Focus of Operational Risk Appetite
3.5.4	- Operational Risk Tolerance
3.5.5	- Determination of Operational Risk Appetite and Risk Tolerance
3.5.6	- The R&R of the Board on the Determination
3.5.7	- The R&R of the Business Management on the Determination
3.5.8	- The R&R of the Internal Audit on the Determination
3.5.9	- Diagrammatic Explanation of Risk Appetite Funnel
3.5.10	- Top-down and Bottom-up Approaches to Setting the Appetite
3.5.11	- Alignments of the Frameworks to the Different Forms of Risk Appetite Expression
3.5.12	- Expressing the Operational Risk Appetite (ORA) Quantitatively and Qualitatively
3.5.13	- Deciding on the Appropriate Level of the ORA and Risk Tolerances
3.5.14	- Implementing the ORA and Tolerances
3.5.15	- Aggregation and Reporting
3.5.16	- Management and Decision Making
3.5.17	- Sample Operational Risk Appetite Template
3.5.18	- Structure of Actionable Risk Appetite
3.5.19	- Consistent Operational Risk Appetite
3.5.20	- Articulating Operational Risk Appetite
3.5.21	- Defining Operational Risk Appetite
3.5.22	- Setting Operational Risk Appetite and Tolerance
3.5.23	- Setting Operational Risk Appetite Thresholds
3.5.24	- Setting and Application
3.5.25	- Market View on Operational Risk Appetite
3.5.26	- Operational Risk Assessment for New Business, Product, and Changes

3.5.27	- Operational Risk Heatmap
3.5.28	- Background, Methodology, and Deliverables of the Critical Operational Risk Registers
3.5.29	- Examples of Operational Risk Appetite Statements
3.6	**Operational Risk Impact**
3.6.1	- Developing Assessment Criteria
3.6.2	- Sample of Operational Risk Rating Scale
3.6.3	- ORX Impact Categories
3.7	**Case Studies**
3.7.1	- Case Study: Ineffective Call-back Verification on Third-party Fund Transfer
3.8	**Best Practice Guidance**
3.8.1	- Best Practice Principles on Operational Risk Appetite
3.8.2	- Internal Controls (Control Environment and Business Process Controls)
3.8.3	- Interaction between Operational Risk Management Tools
3.8.4	- Operational Risk Management Tools Metrics
Chapter 4: Operational Risk Assessment, Measurement And Reporting	
4.1	**Introduction**
4.2	**Operational Risk Assessment**
4.2.1	- Stages of Operational Risk Assessment Process
4.2.2	- Methods for Assessing Risks
4.2.3	- Identifying Operational Risk
4.2.4	- Tools of Operational Risk Assessment
4.2.5	- Benchmarking for Identification
4.2.6	- Risk Factors for Consideration
4.2.7	- HKMA Requirement on Operational Risk Assessment Methods
4.3	**Quantification of Operational Risk**
4.3.1	- Explanation of Quantification of Operational Risk
4.3.2	- Value at Risk (VaR)
4.3.3	- Conditional VaR
4.3.4	- Extreme Value Theory
4.3.5	- Peaks-over-Threshold
4.3.6	- Fuzzy Logic

4.3.7	- Bayesian Belief Network
4.3.8	- Artificial Neural Networks
4.3.9	- Bootstrapping
4.3.10	- Heat Map
4.3.11	- Risk Registers
4.3.12	- Practical Consideration
4.4	**Risk Reporting and Dashboard**
4.4.1	- Objectives of Operational Risk Reporting
4.4.2	- Factors of Operational Risk Reporting
4.4.3	- Process of Operational Risk Reporting
4.4.4	- Typical Contents of Operational Risk Reports
4.4.5	- Timeliness of Operational Risk Reports
4.4.6	- Features of Operational Risk Reporting
4.4.7	- Types of Operational Risk Reporting
4.4.8	- Action of Operational Risk Reporting
4.4.9	- Best Practice Principles of Operational Risk Reporting
4.4.10	- Critical Success Factors of Operational Risk Reporting
4.4.11	- Examples of Operational Risk Reports
4.4.12	- Checkpoints on Good Operational Risk Reporting
4.5	**Nature of The Financial Products**
4.5.1	- Overview of Financial Service Products
4.5.2	- Funds Intermediation Products
4.5.3	- Transaction Intermediation Products
4.5.4	- Information Intermediation Products
4.5.5	- Risk Intermediation Products
4.5.6	- Work Activity Related to Financial Services Products
4.5.7	- Managing Risk in New Product Development
4.5.8	- Key Features of Equity
4.5.9	- Demonstrate Understanding of Equity
4.5.10	- Key Features of Various Types of Bonds
4.5.11	- International Bond Markets

4.5.12	- Major Categories of Money Market Products
4.5.13	- Differences and Similarities between the Major Types of Cash Money Market
4.5.14	- The Major Commodity Categories
4.5.15	- Major Categories of Derivative Products
4.5.16	- The Markets where Major Categories of Derivative Products Are Usually Traded
4.5.17	- Major Categories of Alternative Investments
4.6	**Common Risk Types**
4.6.1	- Types of Operational Loss
4.6.2	- Types of Categorisation of Operational Risk
4.6.3	- Rationale for Operational Risk Categorisation
4.6.4	- Key Principles for Categorising Operational Risks
4.6.5	- Designing an Operational Categorisation Framework
4.6.6	- Minimising Gaps and Overlaps
4.6.7	- Improving Granularity
4.6.8	- Implementation – Roles and Responsibilities
4.6.9	- Implementation – Ensuring Consistent Use
4.6.10	- Implementation – Reporting
4.6.11	- Implementation – Addressing Boundary Events
4.6.12	- Common Risk Types of Services and Products
4.6.13	- Typology of Operational Risks
4.7	**Case Studies**
4.7.1	- Case Study: Mistake in Allowing an Authorized Person to Bring in Another Person when Accessing a Safe Deposit Box
4.8	**Best Practice Guidance**
4.8.1	- Theme and Metrics for Conduct Risk Reporting
4.8.2	- Example of Conduct Risk Metrics Reporting
Chapter 5: Technology, Resiliency And Enterprise Risk Assessment	
5.1	**Introduction**
5.2	**Technology Risk Framework**
5.2.1	- Operational Risk in Information Technology
5.2.2	- Regulations for Technology Management in Banking Industry
5.2.3	- Managing Information and Communication Technology

5.3	**Cybersecurity**
5.3.1	- Typology of Information Security Risk
5.3.2	- Types of Cyber Security Threats
5.3.3	- Sample of Information Security Risk Assessment
5.3.4	- Key Controls in Information Security
5.3.5	- Sample of KRI in Information Security
5.3.6	- Cybersecurity Standards
5.3.7	- Information Security Management System
5.3.8	- ISO/IEC 27001 Information Security Management Systems Standard
5.3.9	- Sharing of Cyber-threat Information
5.3.10	- Principal Cyberactivities that are Criminalised by the Law
5.3.11	- Information Security Challenges Associated with Cloud Computing
5.3.12	- Cybersecurity Laws Affect Foreign Organisations
5.3.13	- Additional Cybersecurity Protections Beyond What Is Mandated by Law
5.3.14	- Government Incentivize Organizations to Improve Their Cybersecurity
5.4	**Data Privacy**
5.4.1	- Overview of Data Privacy
5.4.2	- Regulation on Data Privacy PDPO
5.5	**System Change Control**
5.5.1	- Risk Management in Change
5.5.2	- Quality Assurance, Testing, and Change Management
5.6	**Resiliency Risk**
5.6.1	- Definition of Resiliency
5.6.2	- Threats to Financial Resilience
5.6.3	- Interconnects of Financial and Operational Resiliency
5.6.4	- Drivers of Operational Resilience
5.6.5	- Risk, Resilience and Sustainability
5.6.6	- Managing Business Continuity Planning
5.6.7	- Business Continuity Management
5.7	**Types of Disasters**
5.7.1	- Types of Disasters

5.7.2	- Classification of Disasters
5.7.3	- Disasters VS Catastrophes
5.8	**Business Impact Analysis Overview**
5.8.1	- Definition of Business Impact Analysis
5.8.2	- Analysis of Business Impact Analysis
5.8.3	- Business Impact Analysis VS Risk Assessment
5.8.4	- HKMA Requirement on Business Impact Analysis
5.9	**Resiliency Plan**
5.9.1	- Definition of Business Continuity
5.9.2	- Roles and Responsibilities of Business Continuity Management
5.9.3	- Components of Business Continuity Management
5.9.4	- BCM Lifecycle
5.9.5	- Contingency Planning
5.10	**Plan Testing Overview**
5.10.1	- HKMA Requirement on Contingency Planning Testing
5.10.2	- HKMA Requirement on Contingency Planning Maintenance
5.11	**Enterprise Risk Framework**
5.11.1	- Overview of Enterprise Risk Management
5.11.2	- Definition of Enterprise Risk Management
5.11.3	- HKMA Requirement on Firm-wide Risk Management
5.11.4	- COSO Enterprise Risk Management Framework
5.11.5	- New COSO ERM - Integrating with Strategy and Performance
5.11.6	- Capability of Enterprise Risk Management
5.11.7	- Key Elements of an Effective Operational Risk within ERM Framework
5.11.8	- Integration of ORM Framework into ERM
5.12	**Enterprise Risk Appetite**
5.12.1	- Enterprise Risk Appetite
5.12.2	- Roles and Responsibilities in Risk Appetite Framework
5.12.3	- HKMA Requirement on Enterprise Risk Appetite Framework
5.13	**Enterprise Risk Limit**
5.13.1	- Enterprise Risk Limit

5.13.2	- Best Practice on Enterprise Risk Limit
5.13.3	- Structure on Enterprise Risk Limit
5.13.4	- HKMA Requirement on Enterprise Risk Limit
5.14	**Case Studies**
5.14.1	- Case Study: Misappropriation of a Customer's Funds by a Staff Member Using a Returned ATM Card
5.15	**Best Practice Guidance**
5.15.1	- The Main Industry Standards and Codes of Practice Promoting Cybersecurity (HKMA, SFC, IA, OGCIO, PCPD)
Chapter 6: Integrated Case Studies And Best Practices	
6.1	**Integrated Case Studies**
6.1.1	- Case Study: The Collapse of Barings Bank 1995
6.1.2	- Case Study: Safety Deposit Boxes at DBS
6.1.3	- Case Study: Société Générale Taken to the Brink
6.1.4	- Lessons Learnt from Risk Cases
6.2	**Best Practice Guidance**
6.2.1	- Ten Principles of the Best Practices in ORM

Recommended Readings

Essential Readings:

1. Ariane Chapelle. (2018). Operational Risk Management: Best Practices in the Financial Services Industry (1st ed.). WILEY.
2. The Hong Kong Institute of Bankers. (2013). Operational Risk Management (1st ed.). WILEY.
3. HKIB Handout. (2021). Fundamentals of Operational Risk Management and Risk Governance.

Supplementary Readings

1. Basel Committee. (2021). Revisions To The Principles For The Sound Management Of Operational Risk.
2. Basel Committee. (2020). The Basel Framework: Frequently Asked Questions.
3. Basel Committee. (2021). Principles For Operational Resilience.
4. Basel Committee. (2019). Launch Of The Consolidated Basel Framework.
5. Basel Committee. (2018). Sound Practices: Implications Of Fintech Developments For Banks And Bank Supervisors.
6. Basel Committee. (2017). Basel III: Finalising Post-Crisis Reforms.

7. Hong Kong Monetary Authority. (2019). TM-E-1: Risk Management of E-Banking.
8. Hong Kong Monetary Authority. (2017). IC-1: Risk Management Framework.
9. Hong Kong Monetary Authority. (2022). OR-1: Operational Risk Management in Supervisory Policy Manual.
10. Hong Kong Monetary Authority. (2022). TM-G-2: Business Continuity Planning.
11. Hong Kong Monetary Authority. Operational Incidents Watch.
12. Hong Kong Monetary Authority. (2020). Report on Review of Self-assessments on Bank Culture.
13. Hong Kong Monetary Authority. (2018). Supervision for Bank Culture.
14. Hong Kong Monetary Authority. (2017). Bank Culture Reform.

Further Readings

1. McKinsey. (2020). The Future Of Operational-Risk Management In Financial Services.
2. BCG. (2016). Five Practices Of Operational Risk Leaders.
3. Accenture. (2016). The Convergence of Operational Risk and Cyber Security.
4. Accenture. (2015). Reaping The Benefits Of Operational Risk Management.
5. COSO. (2021). Enterprise Risk Management Framework.
6. ISO 31000:2018. Risk Management Guidelines.