TURKS AND CAICOS ISLANDS
FINANCIAL SERVICES COMMISSION
Regulating with Honesty, Integrity and Transparency

13 July 2026

REGULATORY ADVISORY NO. 3 of 2026

Adoption of Basel Principles for the Sound Management of Operational Risk

For Banks Licensed under the Banking Act Cap. 16.02

This Advisory communicates the Commission's adoption of the Basel Committee on Banking Supervision's Principles for the Sound Management of Operational Risk, revised March 2021 (the "Basel Operational Risk Principles"), as the relevant international benchmark for the Commission's supervisory approach to operational risk in the banking sector.

The Basel Operational Risk Principles

The Basel Operational Risk Principles provide the internationally recognised prudential standard for the sound management of operational risk in banks. They address operational risk culture, governance, the operational risk management framework, board and senior management oversight, risk appetite, risk identification and assessment, change management, monitoring and reporting, control and mitigation, information and communication technology (ICT) risk, business continuity and disclosure.

The Commission will use the Basel Operational Risk Principles as the reference benchmark for its supervisory engagement with banks. In applying the standard, the Commission will have regard to proportionality and to the specific circumstances of the Turks and Caicos Islands banking sector.

For the purpose of this Advisory, operational risk means the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. This definition includes legal risk but excludes strategic and reputational risk.

Banks are encouraged to assess their existing governance, risk management, controls, incident reporting, ICT, risk management and business continuity arrangements against the Basel standard.

The Commission provides the following guidance for the sector's attention.

GUIDANCE

This guidance sets out the Commission's high-level supervisory expectations on operational risk management and introduces the Operational Incident and Loss Event Reporting Template set out in the Appendix A. **It applies to all banks licensed and supervised by the Commission.**

The Commission's expectations should be applied proportionately, having regard to each bank's nature, size, complexity, business model, risk profile, products, delivery channels, outsourcing arrangements and technology dependencies.

1. Basel-Aligned Principles and Supervisory Expectations

The following principles summarise the Commission's high-level expectations, aligned with the Basel Operational Risk Principles.

Principle 1: Operational Risk Culture

- Banks should promote a sound operational risk culture that is led by the board and embedded by senior management across the institution.
- The culture should support prudent behaviour, timely escalation of issues, accountability for control failures, open communication, and effective challenge within and across the three lines of defence.
- Policies on ethics, behavioural conduct, conflict of interest, remuneration, performance management and operational risk training should reinforce the bank's operational risk appetite and discourage excessive risk-taking or tolerance of unresolved control weaknesses.

Principle 2: Operational Risk Management Framework (ORMF)

- Banks should maintain a documented operational risk management framework that is comprehensive and integrated into the bank's overall risk management arrangements. The framework should be proportionate to its business model and risk profile, having regard to the bank's nature, size and complexity.
- The framework should define operational risk clearly, establish governance arrangements, allocate roles and responsibilities, describe the risk taxonomy, set out risk assessment and reporting processes, and link to internal control, ICT, outsourcing, business continuity and incident management arrangements.
- Business lines should own and manage operational risk in day-to-day activities. Independent risk management should provide oversight and challenge, while internal audit should provide independent assurance on the design and effectiveness of the framework.

Principle 3: Board Oversight

- The board should approve and periodically review the operational risk management framework and satisfy itself that the framework remains appropriate to the bank's activities, systems, outsourcing arrangements and strategic direction.
- The board should receive reliable and sufficiently detailed management information on material operational risk exposures, significant incidents, control weaknesses, emerging risks and remediation progress.
- Board oversight should include active challenge of senior management and appropriate follow-up where weaknesses are identified.

Principle 4: Operational Risk Appetite and Tolerance

- Banks should articulate an operational risk appetite and tolerance statement that is consistent with their strategy, financial capacity, control environment and operational resilience objectives.
- The risk appetite should be measurable where practicable and supported by indicators, thresholds and escalation triggers. It should inform business decisions, product approvals, technology changes, outsourcing arrangements, remediation priorities and incident escalation.

- The board should approve the operational risk appetite and review it periodically, including after material incidents or significant business changes.

Principle 5: Senior Management Governance

- Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well-defined, transparent and consistent lines of responsibility.
- Senior management should implement the operational risk management framework consistently across the bank and ensure that sufficient resources, systems, skilled personnel and reporting arrangements are in place.
- Roles and responsibilities should be clearly documented, including the responsibilities of business units, risk management, compliance, ICT, operations, legal, finance and internal audit.
- Senior management should establish escalation procedures, monitor remediation actions, and ensure that lessons from incidents, audit findings and control reviews are incorporated into the framework.

Principle 6: Risk Identification and Assessment

- Banks should identify and assess operational risk on an ongoing and forward-looking basis across all material products, activities, processes, systems, legal entities, delivery channels and outsourced activities.
- Appropriate tools may include risk and control self-assessments, key risk indicators, control testing, internal loss event data, external event data, scenario analysis, business process mapping, issue tracking and risk registers.
- Banks should capture material operational incidents and loss events, including relevant near-misses, in a manner that supports trend analysis, root cause analysis, remediation and management reporting.

Principle 7: Change Management

- Banks should assess operational risks arising from new products, services, systems, delivery channels, outsourcing arrangements, organisational changes and other material changes before implementation and throughout the change lifecycle.
- Change assessments should consider people, process, systems, data, legal, compliance, customer, ICT, cyber, third-party and business continuity implications.
- Material changes should be subject to appropriate approval, independent challenge, implementation monitoring and post-implementation review.

Principle 8: Monitoring and Reporting

- Banks should have in place a process to regularly monitor operational risk profiles and material operational exposures.
- Banks should monitor operational risk exposures, incidents, control weaknesses, key risk indicators and remediation actions on a regular basis.
- Reporting to senior management and the board should be timely, accurate, decision-useful and proportionate to the bank's risk profile. It should highlight significant incidents, risk trends, breaches of appetite or tolerance, overdue actions, emerging risks and lessons learned.

Principle 9: Control Environment, Mitigation and Third-Party Risk

- Banks should maintain a strong internal control environment that is commensurate with their operational risk profile and business complexity.
- Controls should include segregation of duties, reconciliations, approvals, exception monitoring, access controls, control testing, issue management, independent review and timely remediation.
- Banks should also manage operational risks arising from outsourcing and other third-party arrangements through due diligence, contractual safeguards, performance monitoring, contingency planning, exit planning and appropriate oversight of critical or material service providers.

Principle 10: Information and Communication Technology Risk

- Banks should identify, assess, monitor and control ICT-related operational risks as an integral part of the operational risk management framework.
- ICT risk management should address cyber security, data confidentiality, integrity and availability, system resilience, privileged access, identity and access management, change and release management, vulnerability management, backup and recovery, incident response and technology third-party dependencies.
- Business, risk and technology functions should coordinate to ensure that ICT risk decisions are aligned with business strategy, operational risk appetite and customer service obligations.

Principle 11: Business Continuity and Recovery

- Banks should maintain business continuity and recovery arrangements that are proportionate to their operations, risk profile and critical services.
- Arrangements should be informed by business impact analysis, scenario analysis, recovery time objectives, recovery point objectives, crisis management procedures, communication plans and regular testing.
- Business continuity planning should be linked to operational risk management, ICT recovery, third-party arrangements, incident management and board and senior management oversight.

Principle 12: Disclosure

- Banks should make operational risk disclosures that are appropriate to their size, complexity and stakeholder needs, while avoiding disclosures that could create additional operational or security risk.
- Disclosures should be accurate, clear and consistent with the bank's governance and risk management arrangements. They should include information on the bank's approach to operational risk governance, risk management, control environment and significant risk exposures where relevant.

2. Operational Incident Notification and Loss Event Information

Operational incident reporting is an important part of sound operational risk management and supervisory engagement. Banks should maintain internal processes for identifying, escalating, recording, analysing and remediating material operational incidents and associated loss events.

The Commission expects banks to give timely notice of material operational incidents, particularly where an incident affects customers, critical services, financial condition, ICT systems, data security, legal or regulatory obligations, third-party service providers, or market confidence. **Such incidents and associated loss events should be reported using the Operational Incident and Loss Event Reporting Template set out in Appendix A.**

Banks are encouraged to consider the following factors when assessing the significance of an operational incident:

- **Impact on customers and other stakeholders:** number of customers affected, severity of harm, service unavailability, complaints, redress requirements and disruption to critical services.
- **Regulatory or legal considerations:** suspected or confirmed breach of laws, regulations, licence conditions, AML/CFT obligations, sanctions requirements, data protection obligations or other supervisory expectations.
- **Capital, liquidity and financial impact:** actual or potential effect on capital adequacy, liquidity, funding access, solvency metrics, gross and net losses, recoveries, provisions and plausible future losses.
- **Operational disruption and resilience:** duration and extent of disruption, failed recovery objectives, repeated incidents, reliance on workarounds, and concentration in a critical process or system.
- **Information security and data compromise:** confidentiality, integrity or availability impacts, scope of data affected, personal data implications and third-party technology involvement.
- **Third-party and outsourcing considerations:** material service provider involvement, contractual issues, oversight concerns, exit challenges and concentration risk.
- **Reputational and market impact:** media interest, customer confidence effects, investor sensitivity and cross-jurisdictional implications.
- **Complexity of the matter:** multiple business lines or entities affected, cross-border elements, uncertain root cause, forensic investigation needs and the expected duration of remediation.

3. Supervisory Engagement

The Commission will use the Basel Operational Risk Principles to inform its supervisory engagement with banks using a risk-based approach. This may include off-site reviews, supervisory meetings, thematic work, on-site examinations, review of operational incidents and assessment of governance, ICT risk, outsourcing and business continuity arrangements.

Where weaknesses are identified, the Commission will generally seek constructive engagement with the bank to understand the issue, assess risk significance, and agree proportionate remediation. The Commission expects boards and senior management to take ownership of material operational risk weaknesses and to ensure timely and sustainable remediation.

Please be guided accordingly.

TCI Financial Services Commission

Appendix A - Operational Incident and Loss Event Reporting

This Reporting Template is issued to support supervisory engagement and promote consistency in how banks bring material operational incidents and associated loss events to the Commission's attention.

Operational incident notification to the Commission

The Commission expects banks to notify it of material operational incidents as soon as reasonably practicable and, in the ordinary course, within **three (3) working days** of discovery, having regard to the nature, size and complexity of the incident. This supervisory expectation applies **whether or not a financial loss has been incurred** and **whether or not all relevant facts are available at the time of discovery**. Where information is incomplete, the bank should submit an initial notification within that period and provide, at a minimum, on a weekly basis, further information as investigations progresses. Where an incident has had, or could reasonably be expected to have, significant adverse consequences, the Commission expects the bank to notify it promptly by telephone or other appropriate means, followed by submission of the completed incident report.

In applying this supervisory expectation proportionately, banks should determine the appropriate level of urgency, and at a minimum, this assessment should take account of the factors set out in Section 2 of the Guidance. The Commission may request additional information or encourage more frequent or accelerated updates where warranted.

Banks should use the *Operational Incident and Loss Event Reporting Template* for initial notification and subsequent updates, so that timelines, impacts, losses and remediation actions are recorded clearly and consistently for supervisory purposes. As mentioned, the template may be completed on the basis of information available at the time and updated as further facts emerge.

This template sets out the minimum information banks should capture and maintain. It supports supervisory review and promotes consistency with Principles 6, 8 and 9.

Banks should ensure that operational incidents are recorded on a timely basis, internally escalated in accordance with approved thresholds, and brought to the Commission's attention in line with the supervisory expectation set out above.

Operational Incident and Loss Event Reporting Template

Section 1: General Information

Field	Description
Bank Name	Legal name of the bank
Reporting Unit / Business Line	Business line or function affected
Incident Reference Number	Unique internal reference
Date Incident Occurred	Date and time the incident occurred
Date Incident Detected	Date and time the incident was identified
Report Prepared By	Name and role of preparer

Section 2: Incident Classification

Field	Description
Operational Risk Category	e.g. Internal Fraud, External Fraud, Employment Practices and Workplace Safety, Customers, Products and Business Practices, Damage to Physical Assets, Business Disruption and Systems Failures, and Execution, Delivery and Process Management
Incident Type	Brief classification (e.g. system outage, processing error, cyber incident)
Root Cause	Underlying cause (e.g. process failure, human error, system failure, third-party failure)
ICT-Related Incident	Yes / No (if yes, specify system or service impacted)

Section 3: Incident Description and Impact

Field	Description
Incident Description	Clear description of what occurred
Date Incident Resolved	Date and time resolved (if applicable)
Operational Impact	Description of service disruption, delays, or control failures
Customers Affected	Number and type of customers affected (if any), without including customer-specific identifying information
Regulatory Notification Required	Yes / No (and to whom), where any other regulatory or legal notification obligation arises

Section 4: Financial Loss Information

Field	Description
Gross Loss Amount	Total financial loss before recoveries
Recoveries Expected	Insurance or other recoveries expected
Net Loss Amount	Loss net of recoveries
Currency	Currency of loss
Accounting Date	Date loss recognised in financial records

Section 5: Control Actions and Remediation

Field	Description
Immediate Actions Taken	Actions taken to contain or mitigate the incident
Control Weakness Identified	Yes / No (describe if yes)
Remedial Actions	Planned or completed corrective measures
Responsible Owner	Individual accountable for remediation
Target Completion Date	Expected completion date

Section 6: Governance and Escalation

Field	Description
Escalated to Senior Management	Yes / No (with date)
Reported to Board / Committee	Yes / No (date and forum)
Included in Management Reporting	Yes / No
Follow-up Review Required	Yes / No

Note: Banks should retain supporting documentation (e.g. incident reports, root cause analyses and customer communications) and ensure consistency with internal loss data collection and business continuity frameworks. Information should be provided at an appropriate level of detail and should not include customer-specific identifying information.

Appendix B - Operational Risk Categories

Banks should classify operational risk events using the categories below.

1. Internal Fraud

Losses resulting from acts intended to defraud, misappropriate property, or circumvent the law, regulations or company policy, involving at least one internal party.

Examples: unauthorised trading, misappropriation of assets, intentional misreporting of positions, bribery by staff.

2. External Fraud

Losses resulting from acts intended to defraud, misappropriate property, or circumvent the law, committed by a third party.

Examples: robbery, cyber-enabled fraud, hacking damage, cheque fraud, identity theft.

3. Employment Practices and Workplace Safety

Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity or discrimination events.

Examples: workers' compensation claims, wrongful termination, harassment claims.

4. Customers, Products and Business Practices

Losses arising from an unintentional or negligent failure to meet a professional obligation to specific customers or from the nature or design of a product.

Examples: fiduciary breaches, suitability failures, disclosure errors, mis-selling, breach of customer data protection requirements.

5. Damage to Physical Assets

Losses arising from loss or damage to physical assets from natural disasters or other external events.

Examples: damage from hurricanes, floods, fires, vandalism, or terrorism.

6. Business Disruption and Systems Failures

Losses arising from disruption of business or system failures, including ICT-related incidents.

Examples: core banking system outages, network failures, cyber incidents, data centre failures, telecommunications disruptions.

7. Execution, Delivery and Process Management

Losses arising from failed transaction processing or process management, including those involving trade counterparties, vendors and suppliers.

Examples: data entry errors, failed settlements, model errors, accounting mis-postings, third-party service provider failures.

Note: *Banks should apply these categories proportionately and ensure consistent use across internal loss data collection, management reporting, and incident escalation processes.*