EXECUTIVE PROFESSIONAL TRAINING

2026–2027 INTERNATIONAL TRAINING SERIES

CYBERSECURITY GOVERNANCE AND RISK OVERSIGHT

FOR CENTRAL BANKS

Strategic governance • cyber resilience • technology risk • regulatory oversight
for secure, resilient and trusted central banking systems

TRAINING DATES & INTERNATIONAL LOCATIONS

5-DAY EXECUTIVE PROGRAMME

- **UAE**
  16th – 20th Nov 2026
- **MALAYSIA**
  22nd – 26th Feb 2027
- **SOUTH AFRICA**
  17th – 21st May 2027
- **KENYA**
  23rd – 27th Aug 2027
- **SINGAPORE**
  04th – 08th Oct 2027
- **ITALY**
  13th – 17th Dec 2027

FEE: USD $ 2,750 PER PERSON

10% DISCOUNT APPLIES TO 3 AND ABOVE DELEGATES FROM SAME INSTITUTION

CYBERSECURITY GOVERNANCE • RISK OVERSIGHT • CENTRAL BANKING

Premium executive training cover • Prepared for high-quality 500 gsm cover-stock printing

The program aligns to the main themes found across NIST Cybersecurity Framework 2.0 (governance emphasis), ISO/IEC 27001/27005, CPMI-IOSCO cyber resilience guidance for FMIs, ECB cyber resilience oversight expectations, DORA's ICT-risk and third-party oversight requirements, and IMF/BIS central-bank cyber risk guidance.

Course Overview

This advanced professional programme equips central bank leaders and technical control functions with the governance, oversight, and practical implementation tools needed to manage cybersecurity and digital operational resilience in a central banking environment. The course covers cyber governance for monetary operations, reserves management, payment and settlement systems, supervision technology, market infrastructure oversight, financial stability operations, currency operations, cloud/third-party dependencies, and emerging digital public infrastructure/CBDC environments.

The programme blends governance frameworks, risk management, oversight methodology, case-based learning, scenario simulation, cyber crisis decision-making, and a capstone governance-improvement project. It is designed not only for cybersecurity specialists, but also for board members, executive committees, internal audit, operational risk, legal/compliance, payment systems, reserve management, and banking supervision functions that must exercise effective cyber risk oversight.

Course Goal

To strengthen the ability of central bank leaders and control functions to **govern, assess, oversee, and improve cybersecurity resilience** across critical central bank functions and across the wider financial ecosystem where the central bank has **oversight, supervisory, or crisis-coordination responsibilities**.

Training Outcomes

By the end of the programme, participants should be able to:

1. Explain the cyber risk landscape for central banks and distinguish between risks affecting the central bank as an institution and risks affecting the broader financial system it oversees.
2. Design or strengthen a central bank cyber governance model with clear board, executive, risk, security, audit, and business-line accountability.
3. Develop cyber risk appetite, tolerance statements, and escalation thresholds suitable for central banking and financial-market infrastructure environments.
4. Map critical business services and crown-jewel assets across payment systems, reserves/treasury, currency operations, supervisory systems, data platforms, and digital channels.
5. Apply risk assessment methods for cyber threats, vulnerabilities, business impact, systemic contagion, and concentration risk.
6. Oversee third-party and cloud cyber risk in line with leading supervisory expectations and resilience standards.
7. Evaluate cyber controls, monitoring, incident reporting, and crisis management arrangements at governance level.
8. Use resilience metrics, KRIs/KPIs, dashboarding, and board reporting to support informed oversight and challenge.
9. Assess cyber resilience testing programmes, including tabletop exercises, red-team/threat-led testing, backup/recovery exercises, and sector coordination drills.
10. Lead or support cyber crisis governance and post-incident lessons learned, including communications with government, regulators, law enforcement, financial sector participants, and the public.
11. Integrate cybersecurity into enterprise risk management, internal audit, compliance, operational resilience, and business continuity frameworks.
12. Produce a practical cyber governance improvement roadmap for a central bank or equivalent public financial institution.

Target Participants

This programme is suitable for:

Executive / Governance level

- Governors, deputy governors, board members
- Executive directors / directors general
- Board risk committee / audit committee members
- CIO, CISO, CRO, COO, CFO, General Counsel
- Heads of payment systems, reserves management, financial stability, supervision

Control and assurance functions

- Enterprise risk management teams
- Operational risk and resilience managers
- Information security / cybersecurity teams
- Internal audit and inspection teams
- Compliance, legal, data governance and privacy officers
- Business continuity / crisis management teams

Technical and business functions with oversight responsibilities

- Payment and settlement system operators
- Currency operations and cash management teams
- Treasury and reserve management staff
- Supervisory technology / regtech / suptech teams
- Financial market infrastructure oversight units
- Digital transformation, cloud, and IT architecture leads
- CBDC / digital payments programme teams

Course Structure: 10 Units with Sub-Units

UNIT 1 — Cybersecurity Governance in the Central Bank Context

Unit Objective: Establish the governance architecture, leadership roles, accountability model, and strategic oversight principles for cyber resilience in central banks.

Sub-units: 1.1 Central bank cyber risk universe

- Cyber threats to central bank operations
- Threats to the financial system and market infrastructures
- Difference between enterprise cyber risk and systemic cyber risk
- Cyber risk in monetary, supervisory, reserve, payments, and currency functions

1.2 International governance standards and regulatory expectations

- NIST CSF 2.0 governance function and board oversight concepts
- ISO/IEC 27001 leadership and ISMS governance
- ISO/IEC 27005 risk management concepts
- CPMI-IOSCO cyber resilience guidance for FMIs
- ECB cyber resilience oversight expectations
- DORA governance, ICT risk management, incident reporting, and third-party oversight themes
- IMF/BIS perspectives on cyber risk in central banking

1.3 Governance model for central banks

- Board, executive committee, and management accountability
- Role of the CISO, CRO, CIO, COO, internal audit, legal, and business owners
- Three lines model for cyber governance
- Committee structures: cyber steering committee, crisis committee, risk committee

1.4 Cyber strategy and governance charter

- Cybersecurity strategy aligned to central bank mandate
- Governance charter, policy hierarchy, and delegated authorities
- Approval, review, and exception management

- Integration into enterprise strategy and risk governance

1.5 Board oversight responsibilities

- Risk appetite approval and oversight
- Monitoring of cyber posture and major incidents
- Escalation thresholds and challenge questions for directors
- Oversight of critical investments and remediation programmes

1.6 Ethical, legal and public-interest dimensions

- Public trust and reputational implications for central banks
- Confidentiality of market-sensitive information
- Decision-making under uncertainty and national-security considerations

UNIT 2 — Central Bank Cyber Risk Landscape, Threat Intelligence and Risk Drivers

Unit Objective: Understand the threat environment, risk drivers, adversary types, and systemic implications of cyber incidents affecting central banks and the financial sector.

Sub-units: 2.1 Threat actors and motivations

- Nation-state actors
- Organized cybercrime and ransomware groups
- Insider threats and privileged misuse
- Supply-chain attackers and compromised vendors
- Hacktivist and geopolitical threat vectors

2.2 Central bank attack surfaces

- Core banking/finance systems
- Payment and settlement systems
- RTGS and securities settlement infrastructure
- Treasury, reserves, SWIFT, dealing-room environments
- Currency issuance, vault and cash systems
- Supervisory data platforms and regulatory reporting systems
- Cloud, remote access, endpoints, mobile, collaboration tools

2.3 Threat scenarios relevant to central banks

- Ransomware affecting critical payment operations
- SWIFT/payment fraud and payment redirection
- Credential compromise and business email compromise
- DDoS against public or market-facing services
- Data integrity attacks and manipulation of reports
- Cloud outage or third-party compromise
- Destructive malware and wiper attacks
- Insider sabotage and unauthorized privileged activity

2.4 Cyber threat intelligence for governance

- Strategic, tactical, and operational threat intelligence
- Intelligence sources: internal telemetry, FS-ISAC equivalents, national CERTs, law enforcement, sector sharing forums
- Converting intelligence into governance action
- Threat-informed board briefings

2.5 Risk drivers and emerging issues

- Legacy systems and technical debt
- Concentration in cloud and software providers
- Cross-border interdependencies
- AI-enabled attacks and deepfakes
- Quantum considerations, crypto key risk, and future-proofing
- CBDC / digital identity / open API ecosystem exposure

UNIT 3 — Cyber Risk Management Framework, Risk Appetite and Control Architecture

Unit Objective: Build a cyber risk management framework tailored to central banks and aligned with enterprise risk management.

Sub-units: 3.1 Cyber risk management framework design

- Cyber risk policy and framework components
- Alignment with ERM, operational risk, BCM, and compliance
- Scope, taxonomy, and ownership
- Integration with project governance and procurement

3.2 Risk appetite and tolerance

- Defining cyber risk appetite in a central bank context
- Translating appetite into tolerance thresholds
- Thresholds for availability, integrity, confidentiality, third-party dependency, and recovery
- Escalation and reporting triggers

3.3 Risk identification and risk register design

- Asset/process/service-based risk identification
- Threat-vulnerability-impact-consequence model
- Risk statements and root cause analysis
- Risk aggregation across business lines

3.4 Risk assessment methodologies

- Qualitative and quantitative methods
- Inherent vs residual risk
- Likelihood, impact, detectability, velocity, and systemic contagion factors
- Scenario-based risk analysis
- Control effectiveness assessment

3.5 Control architecture and assurance mapping

- Preventive, detective, corrective and recovery controls
- Control ownership and evidence requirements
- Mapping to NIST / ISO / DORA / internal policy requirements
- Key control testing and self-assessment

3.6 Governance reporting and risk acceptance

- Exception approvals and compensating controls
- Treatment plans, deadlines, and remediation governance
- When to transfer, accept, mitigate, or avoid cyber risk
- Risk committee reporting packs

UNIT 4 — Critical Services, Crown Jewels and Business Impact in Central Banking

Unit Objective: Identify critical services and assets and assess cyber risk in terms of operational, financial stability, policy, and reputational impact.

Sub-units: 4.1 Identifying critical business services

- Monetary policy operations
- Reserves and treasury operations
- Payment, clearing and settlement services
- Currency operations and cash distribution
- Banking supervision and data reporting services
- Market intelligence, financial stability and public communication functions

4.2 Crown-jewel asset identification

- Payment engines, settlement ledgers, SWIFT infrastructure
- Reserve management systems
- Identity, privileged access, HSMs and key management
- Data warehouses, supervisory databases, public websites and communication channels

4.3 Business impact analysis from a cyber perspective

- Financial loss and operational disruption
- Policy disruption and delayed monetary/market operations
- Systemic contagion and loss of confidence
- Data integrity and decision-quality risks
- Reputational, legal, and diplomatic impacts

4.4 Service dependency mapping

- Applications, data, networks, people, sites, vendors, cloud services
- Single points of failure and concentration risk
- Manual workarounds and minimum service levels
- Interdependencies with commercial banks, FMIs, government, and telecoms

4.5 Setting impact tolerances and recovery priorities

- Maximum tolerable downtime
- Recovery time objective (RTO) and recovery point objective (RPO)
- Integrity recovery and reconciliation priorities
- Tiering of systems and crisis decision thresholds

UNIT 5 — Cybersecurity Controls Oversight: Identity, Data, Infrastructure, Detection and Resilience

Unit Objective: Give participants a governance-level understanding of the control domains that central bank leadership must oversee.

Sub-units: 5.1 Identity, privileged access and segregation of duties

- IAM governance model
- Privileged access management
- Joiner-mover-leaver controls
- Segregation of duties in treasury, payments and finance systems
- MFA and high-risk access monitoring

5.2 Data protection and integrity

- Data classification and handling
- Encryption at rest/in transit
- Key management and HSM governance
- Data loss prevention
- Integrity controls, reconciliation, and tamper detection

5.3 Infrastructure and endpoint security oversight

- Network segmentation and zero-trust principles
- Hardening, patching and vulnerability management
- Endpoint detection and response oversight
- Secure remote access and administrative access
- Backup architecture and immutability

5.4 Security monitoring and detection

- SOC governance and operating model
- Logging strategy and SIEM oversight
- Threat detection use cases
- Detection coverage metrics and blind spots
- Alert triage, escalation and case management

5.5 Secure development and change governance

- Secure SDLC principles
- Change management and emergency changes
- Security testing in projects
- DevSecOps governance for digital programmes
- Configuration baselines and release approvals

5.6 Control assurance from management's perspective

- How leaders assess whether controls are working
- Key control indicators and testing evidence
- Common "paper compliance" failures
- Control maturity vs control effectiveness

UNIT 6 — Third-Party, Cloud and Technology Supply Chain Risk Oversight

Unit Objective: Build a robust governance model for ICT third-party risk, concentration risk, and outsourced critical services.

Sub-units: 6.1 Third-party risk in the central bank environment

- Outsourced ICT services
- Core software vendors and managed service providers
- Cloud hosting, SaaS, telecoms, and cyber tooling providers
- Critical providers in payments, SWIFT, market data, and supervisory platforms

6.2 Governance of outsourcing and cloud adoption

- Pre-contract due diligence
- Materiality assessment and criticality classification
- Approval authorities and risk acceptance
- Security, resilience and legal review requirements

6.3 Contracting and control expectations

- Security clauses, audit rights, incident notification
- Data location, confidentiality, and subcontracting clauses
- Business continuity and disaster recovery requirements
- Exit/transition rights and testing expectations

6.4 Third-party risk monitoring

- Ongoing assurance, attestations and evidence review
- Concentration risk monitoring
- Dependency on hyperscalers and sector-wide common providers

- Performance, incidents and remediation tracking

6.5 Cloud and systemic concentration risk

- Multi-cloud vs single-provider considerations
- Shared responsibility model
- Sovereignty and cross-border data issues
- Operational and geopolitical risk implications

6.6 Exit, substitution and contingency planning

- Exit playbooks
- Recovery from vendor failure or compromise
- Data portability and transition support
- Testing contingency arrangements with providers

UNIT 7 — Incident Management, Crisis Governance and Regulatory/Sector Reporting

Unit Objective: Enable leaders and control functions to oversee cyber incident response, crisis management, escalation and reporting.

Sub-units: 7.1 Cyber incident governance model

- Incident severity classification
- Roles: incident commander, crisis leader, legal, communications, business owners
- Major incident escalation and decision rights
- Coordination between IT, cyber, operations, risk and leadership

7.2 Incident detection to decision-making workflow

- Triage and validation
- Containment, eradication, recovery
- Evidence preservation and forensic support
- Decision-making under uncertainty

7.3 Reporting and notification obligations

- Internal management reporting
- Board and audit committee escalation
- Reporting to supervisors, government, CERTs, law enforcement, payment ecosystem participants
- Cross-border reporting coordination

7.4 Crisis communications

- Executive and board briefing templates
- Communications with banks, FMIs, ministries, media and the public
- Managing misinformation, rumor, and market confidence
- Stakeholder communication sequencing

7.5 Cyber crisis playbooks

- Ransomware affecting payments
- Data integrity compromise in reserves/financial reporting
- Third-party outage affecting critical services
- DDoS and public confidence scenarios
- Insider compromise of privileged systems

7.6 Post-incident review and lessons learned

- Root cause analysis
- Control gap remediation
- Accountability and disciplinary follow-up
- Regulatory and board follow-up actions

UNIT 8 — Cyber Resilience Testing, Assurance and Independent Oversight

Unit Objective: Help participants understand how to design and oversee a meaningful cyber resilience testing and assurance programme.

Sub-units: 8.1 Cyber testing strategy

- Purpose of testing in governance
- Risk-based annual test planning
- Coverage of critical services, technology and third parties
- Mapping tests to impact tolerances and risk appetite

8.2 Types of cyber resilience testing

- Vulnerability scanning and control validation
- Penetration testing
- Red team / threat-led testing
- Purple team exercises
- Backup restore and cyber recovery tests
- Crisis tabletop and executive exercises

8.3 Oversight of testing programmes

- Independence and competence requirements
- Scoping and scenario design

- Tracking findings to remediation
- Reporting to senior management and the board

8.4 Internal audit and second-line assurance

- Audit universe and risk-based audit planning
- Assurance over cyber governance, third-party risk, incident response and resilience
- Continuous monitoring and thematic reviews
- Validation of management assertions

8.5 Metrics of resilience effectiveness

- Mean time to detect / contain / recover
- Patch/vulnerability exposure metrics
- Privileged access and logging coverage
- Third-party remediation aging
- Testing completion and recovery success rates

8.6 Assurance for sector-wide oversight roles

- Assessing cyber resilience of payment systems / FMIs / regulated entities
- Thematic reviews and self-assessment models
- Maturity assessments and benchmarking
- Oversight dialogue and corrective actions

UNIT 9 — Sectoral Cyber Resilience, FMI Oversight, Supervisory Expectations and CBDC/Digital Ecosystem Risk

Unit Objective: Examine the central bank's role in promoting cyber resilience beyond its own walls—across payment systems, supervised institutions, and digital public financial infrastructure.

Sub-units: 9.1 Central bank as overseer, supervisor and catalyst

- Cyber resilience as a financial stability issue
- Central bank coordination with supervisory authorities and government
- Sector-wide information sharing and exercises
- Macroprudential perspective on cyber risk

9.2 Oversight of payment systems and FMIs

- FMI cyber resilience principles
- Oversight expectations for critical payment infrastructures
- Operational resilience of RTGS and settlement ecosystems
- Third-party and concentration risk in FMIs

9.3 Supervisory perspectives on cyber risk in banks and financial institutions

- Governance and ICT risk expectations
- Incident reporting and materiality
- Outsourcing and third-party oversight
- Testing and evidence expectations
- Data quality and regulatory reporting integrity

9.4 CBDC / digital currency ecosystem cyber governance

- CBDC threat landscape
- Identity, wallet, API, settlement and offline risks
- Key management and cryptographic resilience
- Third-party and ecosystem governance
- Public trust and resilience implications

9.5 Sector-wide crisis coordination and financial stability

- Coordinating systemic response to cyber incidents
- Liquidity, payments, and market confidence considerations
- Crisis escalation across public authorities
- Recovery of critical sector services

UNIT 10 — Board Reporting, Maturity Improvement and Cyber Governance Transformation

Unit Objective: Translate all course content into an actionable improvement roadmap and governance transformation plan.

Sub-units: 10.1 Cyber governance maturity models

- Capability maturity concepts
- Baseline, target state and gap analysis
- Prioritization criteria for central banks

10.2 Board and executive dashboards

- KRIs, KPIs and KCI design
- What to report monthly, quarterly, and ad hoc
- Heat maps, trend reporting and risk narratives
- Warning indicators for board attention

10.3 Budgeting and investment prioritization

- Risk-based cyber investment decisions
- Building the business case for resilience
- Prioritizing people, tooling, architecture and recovery capabilities

10.4 Policy, roadmap and programme management

- Multi-year cyber resilience roadmap
- Ownership, milestones and governance checkpoints
- Remediation portfolio management
- Quick wins vs structural reforms

10.5 Culture, training and accountability

- Executive cyber awareness
- Specialized training for control functions and critical operations teams
- Accountability mechanisms and performance expectations
- Building a challenge culture

10.6 Capstone project workshop

- Develop a central bank cyber governance improvement plan
- Present governance, risk, resilience and oversight enhancements
- Prioritize actions for 12, 24 and 36 months

Five-Day Training Schedule

5-Day Intensive Schedule: Cybersecurity Governance and Risk Oversight for Central Banks

Day	Session / Theme	Key Topics Covered	Practical Activities	Expected Outputs
Day 1	**Module Block 1: Cyber Governance Foundations**	**Unit 1:** Cybersecurity governance in central banks; board and executive accountability; governance models; policies; committee structures. **Unit 2 (Part A):** cyber threat landscape, central bank attack surfaces, adversaries, systemic risk drivers.	**Icebreaker mapping exercise:** participants map cyber responsibilities across their central bank. **Group discussion:** "What makes central bank cyber risk different from commercial bank cyber risk?" **Case study 1:** governance failure in a critical public-sector financial institution.	Draft governance responsibility map; list of central bank-specific cyber risk drivers; governance gap notes.
Day 2	**Module Block 2: Risk Framework, Appetite and Critical Services**	**Unit 2 (Part B):** threat intelligence and emerging risk. **Unit 3:** cyber risk framework, risk appetite, risk register, assessment methodology, treatment and reporting. **Unit 4:** critical services, crown jewels, BIA, dependency mapping, impact tolerance.	**Workshop 1:** build a cyber risk appetite statement for a central bank. **Group work:** identify crown-jewel assets and critical services for payments, reserves, supervision, and currency operations. **Case study 2:** ransomware and data integrity attack affecting a payment system and supervisory data platform.	Draft cyber risk appetite statement; critical service map; sample risk register entries; impact tolerance matrix.
Day 3	**Module Block 3: Control Oversight and Third-Party Risk**	**Unit 5:** control domains—identity, privileged access, data integrity, logging, vulnerability management, backup resilience, secure change. **Unit 6:** cloud and third-party governance, concentration risk, contracting, exit planning, oversight.	**Control challenge lab:** participants review a mock board dashboard and identify hidden control weaknesses. **Group exercise:** assess a cloud outsourcing proposal for a central bank payment platform. **Case study 3:** third-party compromise causing operational disruption at a financial authority.	Control oversight checklist; third-party due diligence scorecard; key contract clause checklist; third-party concentration risk heat map.
Day 4	**Module Block 4: Incident Governance, Crisis Management and Testing**	**Unit 7:** incident governance, escalation, reporting, crisis communications, playbooks, post-incident review. **Unit 8:** resilience testing strategy, red team/tabletop/recovery testing, internal audit and second-line assurance, resilience metrics.	**Simulation / tabletop exercise:** "Major cyberattack on the central bank RTGS and reserve management environment." Participants play roles as governor, CISO, CRO, legal counsel, communications head, payment systems director, and supervisor. **Workshop:** design an annual cyber resilience testing plan.	Crisis escalation log; incident decision matrix; executive communications draft; resilience testing calendar; post-incident action register.

Day	Session / Theme	Key Topics Covered	Practical Activities	Expected Outputs
Day 5	**Module Block 5: Sectoral Oversight and Capstone**	**Unit 9:** cyber resilience oversight of FMIs, supervised institutions, sector coordination, CBDC ecosystem risk. **Unit 10:** board reporting, maturity improvement, cyber transformation roadmap.	**Capstone project:** each group designs a **Central Bank Cyber Governance & Risk Oversight Improvement Plan**. **Presentation to mock board panel** with Q&A and challenge session. **Peer review and facilitator feedback.**	Capstone presentation; 12/24/36-month roadmap; board dashboard prototype; prioritized cyber governance reform plan.

Detailed Practical Components

A. Group Work Exercises

The course should include at least **5 structured group exercises**:

Group Exercise 1 — Cyber Governance Responsibility Mapping

Participants map:

- Board responsibilities
- Executive management responsibilities
- CISO / CRO / CIO / Internal Audit roles
- Business owner accountability for payments, reserves, supervision, and currency operations
- Escalation lines and committee structure

Group Exercise 2 — Risk Appetite and Tolerance Workshop

Participants draft:

- Cyber risk appetite statement
- Tolerance thresholds for outages, data integrity compromise, third-party dependency, and incident escalation
- Examples of board reporting triggers

Group Exercise 3 — Critical Service and Crown Jewel Mapping

Participants identify:

- Top 10 critical services
- Crown-jewel assets and data stores
- Interdependencies with vendors, telecoms, FMIs, and commercial banks
- Recovery priorities and impact tolerances

Group Exercise 4 — Third-Party Risk Review

Participants review a hypothetical outsourcing of:

- Payment switching infrastructure
- Cloud-based supervisory analytics platform
- Managed SOC or managed identity service
They assess due diligence, concentration risk, contractual safeguards, and exit planning.

Group Exercise 5 — Capstone Governance Transformation Plan

Participants produce a full roadmap with:

- Governance changes
- Risk management enhancements
- Control and testing priorities
- Crisis management improvements
- Reporting and oversight model

B. Case Studies to Include

IBSF to use **4–6 case studies** across the week. Recommended examples:

Case Study 1 — Governance Failure in a Public Financial Institution
Focus: unclear accountability, weak challenge from board, inadequate cyber investment, no tested recovery plan.

Case Study 2 — Ransomware Affecting a Payment and Settlement Environment
Focus: critical service disruption, public confidence, escalation, coordination with banks and government, recovery prioritization.

Case Study 3 — Third-Party / Cloud Provider Compromise
Focus: outsourcing oversight, concentration risk, incident notification failures, contractual weaknesses, exit limitations.
Case Study 4 — Data Integrity Attack on Supervisory or Financial Stability Data
Focus: decision-quality risk, reporting inaccuracies, forensic validation, communications and public trust.

Case Study 5 — Insider Privileged Access Abuse in Treasury / Reserves Systems
Focus: access governance, segregation of duties, monitoring, disciplinary escalation, audit response.

Case Study 6 — CBDC / Digital Payments Cyber Incident Scenario
Focus: ecosystem risk, wallet/API compromise, cryptographic key protection, third-party dependency, public communications.

Simulation Exercise Design

Flagship Simulation: "Cyber Crisis at the Central Bank"

Scenario Summary

A sophisticated cyberattack affects:

1. RTGS / payment operations
2. Reserve management support systems
3. A critical third-party cloud-based supervisory data service

Participants are assigned roles:

- Governor / Deputy Governor
- CISO
- CRO / Head of ERM
- CIO / Head of Technology
- Head of Payment Systems
- Head of Reserve Management / Treasury
- General Counsel / Compliance
- Head of Communications
- Internal Audit Observer
- Government / regulator liaison role

Decisions they must make:

- Whether to shut down or isolate payment systems
- Whether to activate manual workarounds
- Whether to communicate immediately to banks and the public
- How to prioritize service restoration
- Whether to invoke crisis management committee and government coordination
- How to classify the incident and what to report externally
- How to manage third-party provider failure and forensic evidence preservation

Simulation outputs

- Situation report
- Executive decision log
- Stakeholder communications plan
- Recovery priorities and service restoration plan
- Immediate remediation and lessons-learned actions

Capstone Project

Capstone Title: Central Bank Cybersecurity Governance & Risk Oversight Improvement Plan

Capstone Task

Each group acts as an advisory team to a central bank governor and board. Using a provided scenario pack, they must produce a **governance and cyber resilience improvement plan** for a central bank facing rising cyber threats, third-party concentration risk, outdated governance arrangements, and weak incident escalation.

Capstone Deliverables

1. Current-state risk summary
2. Governance and accountability redesign

3. Cyber risk appetite and reporting framework
4. Critical service and crown-jewel protection priorities
5. Third-party and cloud oversight enhancement plan
6. Incident governance and crisis management improvement plan
7. Testing and assurance roadmap
8. 12-, 24-, and 36-month implementation roadmap
9. Board dashboard prototype
10. Presentation to mock board panel

Types of Assessments to Expect

A. Diagnostic / Entry Assessment

Conducted at the start to gauge participant baseline.
Examples:

- Short pre-course quiz on cyber governance concepts
- Self-assessment of institutional cyber maturity
- Short questionnaire on current central bank cyber governance arrangements

B. Formative Assessments (during the course)

1. Daily knowledge checks

- 10–15 multiple-choice / short-answer questions
- Quick recap quizzes after each module block

2. Group exercise assessment

Facilitators assess:

- Participation

C. Summative Assessment

1. Final individual assessment

Could include:

- Multiple-choice questions
- Short written answers
- Scenario-based analysis questions
- Board memo / executive briefing draft

Capstone Assessment Criteria

- Relevance to central bank context
- Practicality and realism
- Alignment with international standards
- Governance clarity and accountability
- Risk-based prioritization
- Quality of board reporting and metrics
- Strength of crisis management and resilience recommendations

- Quality of analysis
- Practicality of recommendations
- Ability to connect governance decisions to risk outcomes

3. Case study debriefs

Participants may be asked to submit:

- A one-page board briefing note
- A risk register extract
- A decision memo or escalation recommendation

4. Simulation performance assessment

Assesses:

- Incident prioritization
- Escalation decisions
- Quality of stakeholder communication
- Coordination under pressure
- Recovery decision logic

2. Capstone group assessment

Based on:

- Written improvement plan
- Quality of final presentation
- Ability to defend recommendations under challenge
- Use of metrics, roadmap logic, and governance design

D. Optional Post-Course Assignment

Participants prepare a **Cyber Governance Action Note** for their own institution within 2–4 weeks of the programme, summarizing:

- top five governance gaps,
- top five resilience actions,
- and an executive reporting proposal.

Sample Assessment Mix and Weighting

Assessment Component	Suggested Weight
Pre-course diagnostic quiz	5%
Class participation and engagement	10%
Group exercises and workshop outputs	20%
Case study analyses / briefing notes	15%
Crisis simulation performance	20%
Final individual knowledge test	10%
Capstone project and presentation	20%

.

Suggested Course Materials / Participant Pack

Participants should receive:

- Course handbook / slides
- Cyber governance maturity assessment template
- Sample cyber risk appetite statement
- Board cyber dashboard template
- Third-party due diligence checklist
- Incident severity and escalation matrix
- Crisis communication template
- Cyber resilience testing plan template
- Capstone case pack and scoring rubric