

RISK AND RESILIENCE BOOTCAMP





GOVERNANCE, AUDIT, AND COMPLIANCE BASICS

This section is an introduction to governance, audit and compliance
A later module will do a deep dive
Topics introduced

- Governance at the organizational level
- The role of the audit function
- Compliance at the regulatory level



GOVERNANCE

- How leadership directs, oversees, and holds IT accountable for supporting business goals, managing risk, and complying with laws
- In practice
 - *Sets direction:* Board and executives set risk appetite and resilience objectives
 - *Evaluates:* Review reports, audits, metrics
 - For example: KRIs, KPIs, BIAs, recovery tests
 - *Monitors:* Ensure controls are working and improvements are made
- ISACA's COBIT model:
 - Governance objectives are Evaluate, Direct, Monitor (EDM)
 - Oversight examiners expect banks to provide evidence of these activities

AUDIT

- Independent review that verifies whether controls and processes are working as intended
- Types of audits in banking IT:
 - Internal audit: continuous review of IT risk and resilience processes
 - External audit/regulatory exams
 - For example: OCC, FDIC, or Federal Reserve reviews of IT risk governance and resilience testing
- DRI best practice alignment:
 - Post-incident assessments and regular resilience plan exercises are “mini-audits” of readiness
- An audit is feedback and assurance that governance processes are real, not just on paper

COMPLIANCE

- Demonstrating that IT risk and resilience practices follow laws, regulations, and industry standards
- In US banks, this includes:
 - Regulators: OCC, FDIC, Federal Reserve, FFIEC (exam guidance)
 - Standards: NIST CSF, ISO 27001, PCI DSS, SOX (ITGCs)
 - Banking expectations:
 - Business Continuity Plans (BCPs),
 - Disaster Recovery Plans (DRPs),
 - Vendor risk management
 - Evidence of annual testing and updates.

COMPLIANCE

- ISACA guidance:
 - Align IT risk management with enterprise risk management (ERM) and regulatory obligations
- DRI guidance:
 - Ensure BCPs/DRPs are tested, documented, and regularly improved

INTERRELATIONSHIPS

- Governance sets the rules
 - Tone at the top, appetite, accountability
- Compliance enforces the rules
 - Ensures the organization is following the applicable laws and frameworks
- Audit verifies the rules
 - Ensures controls are effective and that evidence is available
- Together, they create a resilience loop
 - Leadership defines objectives
 - Teams execute and maintain controls
 - Auditors validate, regulators examine
 - Feedback cycles back into governance decisions

WHAT REGULATORS DO

- Set the rules (prudence and conduct)
 - Capital/liquidity, governance, operational resilience, cybersecurity, disclosures, fair dealing
- Supervise and examine
 - Ongoing reviews of controls, testing, and governance
 - Issue findings and identify areas where remediation is necessary
- Enforce
 - Fines, consent orders, restrictions when rules are broken

WHAT REGULATORS DO

- Monitor systemic risk
 - Risks that could threaten the stability of an entire system, not just a single organization
- Protect consumers/investors
 - Ensure products are fair, disclosures are clear, and complaints are handled
- Ensure market integrity
 - Prevent manipulation/abuse in trading and derivatives other markets
- Enable orderly failure
 - Plan for resolution so critical services continue if an organization fails

IT BANK REGULATION

- Complicating the discussion of regulation in bank IT systems are the overlapping areas of regulation related to IT systems
- Financial industry regulators
 - Organizations that regulate financial services
 - Their regulations are not IT specific
 - For example: audit requirement and record keeping
 - Generally implemented by IT which supplies the supporting infrastructure
- Technology regulators
 - Not concerned specifically with banking, but focuses on general IT issues
 - For example: system security or data privacy and integrity
- These are not disjoint classifications

IT BANK REGULATION

- This is not going to be an exhaustive discussion
 - The regulatory landscape constantly adapts to new products, services, technologies, threats and market shifts
- Quick partial roll call of industry regulators
 - Safety & soundness / banking
 - Federal Reserve (FRB), Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC)
 - Securities & markets:
 - Securities and Exchange Commission (SEC)
 - Derivatives:
 - Commodity Futures Trading Commission (CFTC)

IT BANK REGULATION

- Quick partial roll call of industry regulators (cont)
 - Consumer financial protection:
 - Consumer Financial Protection Bureau
 - Self-regulation (brokers)
 - Financial Industry Regulatory Authority (FINRA)
 - States
 - e.g., NYDFS (New York) sets influential cyber/resilience rules
 - Systemic oversight
 - Financial Stability Oversight Council (FSOC) coordinates across agencies

IT BANK REGULATION

- Relevance to IT risk and resilience teams
 - Regulators expect to be able to review document risk mitigation controls
 - Regulators require resilience to be designed, tested, and evidenced, not just documented
 - Operational resilience requirements
 - Define critical services, set disruption tolerances (RTO/RPO/MTPD), run realistic exercises, and fix gaps
 - Cybersecurity and incident governance goals
 - Detect, respond, and notify on time
 - For example: 36-hour bank incident notifications
 - Manage third-party risk
 - Contract for resilience
 - For example: RTO/RPO, testing rights, notification windows and monitor vendors/fintechs continuously
 - Governance and reporting
 - Require metrics (KRIs), issues, and remediation status
 - Evidence must be retrievable on demand

IT BANK REGULATION

- IT resilience roles responsibilities
 - Translate business impact into targets (RTO/RPO) that can be reviewed
 - Keep evidence ready for examination
 - For example: BIA, test reports, access/backup/restore logs)
 - Run table-tops and technical drills and close action items with owners according to due dates
 - Align change, incident, and third-party processes to regulatory expectations so the bank stays safe, compliant, and trusted

REGULATOR DRILL DOWN

- Practical map of who regulates (or drives) IT operations for US banks
 - What each expects from tech, risk, and resilience teams
- Prudential bank regulators (core examiners)
 - Federal Reserve (FRB), OCC, FDIC:
 - Supervise safety & soundness
 - Assess IT programs using the FFIEC IT Examination Handbook (e.g., the Business Continuity Management booklet)
 - Expect governed RTO/RPO targets, exercises, dependency management, and evidence on demand.
 - 36-hour incident-notification rule (Interagency: FRB/OCC/FDIC):
 - Must notify your primary federal regulator as soon as possible and no later than 36 hours after determining a qualifying "notification incident"
 - Bank service providers must also notify bank customers promptly.
 - Build 24x7 thresholds and comms playbooks

REGULATOR DRILL DOWN

- Prudential bank regulators (cont)
 - Third-party risk (Interagency Guidance / FDIC):
 - Life-cycle oversight of vendors/fintechs
 - Contracts must embed resilience (RTO/RPO, testing rights, incident notice), with ongoing monitoring and exit planning.

24×7 THRESHOLDS

- The bank, and its critical service providers
 - Must define clear triggers that apply around the clock, not just during business hours
 - Determine when an incident becomes serious enough to
 - Escalate internally
 - Notify regulators (e.g., the 36-hour rule)
 - Alert clients or stakeholders
 - Invoke continuity or recovery procedures
 - Examples of 24×7 thresholds:
 - System outage exceeding X minutes
 - Cyber incident affecting customer data
 - Payment failures or transaction delays
 - Critical vendor disruption
 - Data corruption or ransomware event
 - Must be monitored continuously
 - Regulators expect rapid action anytime risk materializes.

COMMUNICATION PLAYBOOKS

- Predefined, documented communication procedures
 - Outlines who to notify, when, how, and in what order during an incident
 - A comms playbook typically defines:
 - Escalation chains, for example: IT → Risk → Legal → Executives
 - Regulator notification steps, for example: which agency, what info, how fast
 - Internal announcements, for example: Ops, security, leadership
 - Customer or partner communications
 - Templates for emails, calls, and regulatory submissions
 - 24×7 contact rosters
 - Playbooks are essential for meeting the 36-hour incident notification rule and demonstrating readiness during examinations

REGULATOR DRILL DOWN

- Prudential bank regulators (cont)
 - Third-party risk (Interagency Guidance / FDIC)
 - Life-cycle oversight of vendors/fintechs
 - Contracts must embed resilience (RTO/RPO, testing rights, incident notice), with ongoing monitoring and exit planning
- Interagency coordination
 - FFIEC (Federal Financial Institutions Examination Council)
 - Not a regulator itself, but its IT Examination Handbook playbook is used by examiners
 - InfoSec, Architecture/Infrastructure/Operations, Business Continuity Management
 - Artifacts and drills are judged against this planning

REGULATOR DRILL DOWN

- Securities/markets
 - SEC
 - Requires disclosure of material cybersecurity incidents within four business days on Form 8-K and annual disclosure of cyber risk management, strategy, and governance
 - FINRA: self-regulator for broker-dealers
 - Rule 4370 requires a written Business Continuity Plan and annual review
 - Relevant if you have a broker-dealer in the group.
- State banking/cyber
 - NYDFS (New York Department of Financial Services)
 - Prescriptive cybersecurity regulation (governance, MFA, testing, incident reporting, BCDR)
 - Widely influential beyond NY

REGULATOR DRILL DOWN

- Global standards
 - Basel Committee: Principles for Operational Resilience
 - Map critical operations, set disruption tolerances, and test through severe-but-plausible scenarios
 - US prudential examiners align to these principles for large banks
- Industry/technical standards
 - NIST Cybersecurity Framework
 - US government guidance that many banks use to structure controls and metrics
 - Regulators expect coherent mappings from bank policies/standards to frameworks like CSF
 - PCI DSS v4.x
 - Regulates protecting payment card data and any systems that could affect it
 - Requires provable controls and testing

REGULATOR DRILL DOWN

- Other regulators
 - There are other aspects of IT that are regulated that are not finance specific
 - These include areas like:
 - Customer rights
 - Privacy and data stewardship
 - Reporting of suspicious activity

Q&A AND OPEN DISCUSSION

