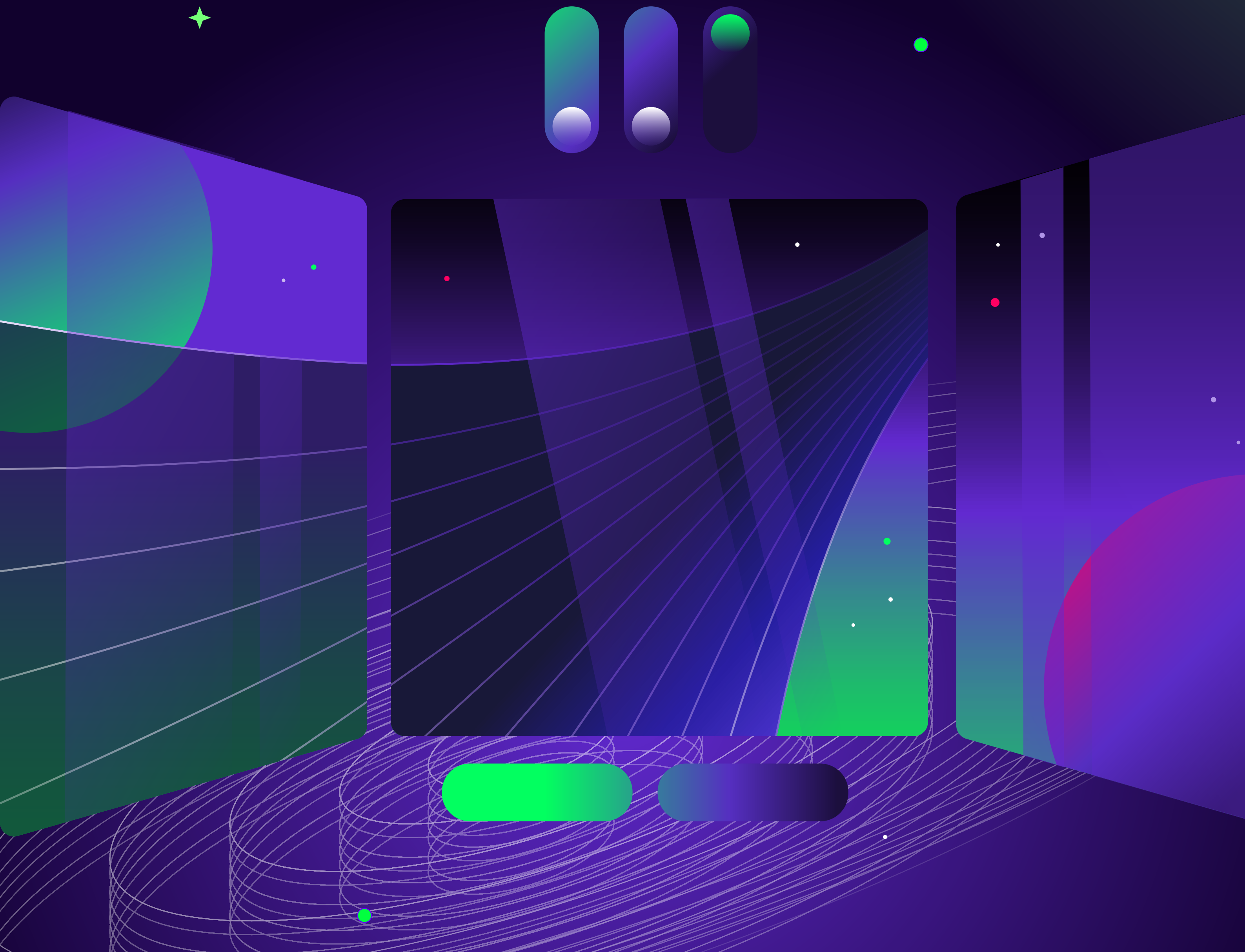
CYERA

GUIDE

Supporting Operational Risk Management and Resilience for Federally Regulated Financial Institutions

How Cyera maps to OSFI's Guideline E-21



Guideline E-21, issued by the Office of the Superintendent of Financial Institutions (OSFI), establishes expectations for managing operational risk and ensuring resilience across federally regulated financial institutions (FRFIs).

It is designed to ensure that institutions can continue delivering critical operations through disruption, and that they anticipate, withstand, respond to, and recover from adverse events such as cyberattacks, system failures, third-party outages, and data breaches.

The Guideline applies to all FRFIs—banks, insurers, trust and loan companies, and branches—on a proportionate, risk-based basis, according to their size, complexity, and interconnectedness.

Guideline E-21 is structured around three desired **outcomes:**

01 Operational risk management practices support operational resilience.

02 Operational risks are managed within approved risk appetite and limits.

03 Critical operations continue to be delivered through disruptions

Each outcome is tied to specific **principles** and **management expectations** across four main domains:

01 Governance

02 Operational Risk Management

03 Operational Resilience

04 Key Risk Areas that Strengthen Resilience

01 Domain 1 – Governance

The purpose of this domain is to ensure clear accountability, documentation, and oversight for operational risk management and resilience across senior management, business units, and independent assurance functions.

Principle 1: Senior management must ensure effective frameworks, scenario testing, defined roles, adequate resources, and escalation processes are in place to identify, assess, and address operational deficiencies.

How Cyera Helps

Cyera enhances governance through:

- **Data visibility to support accountability:** Providing a unified view of sensitive and business-critical data to clarify ownership and accountability across teams.
- **Reporting and escalation support:** Automated reports and dashboards aligned with OSFI's governance expectations provide timely, accurate reporting to management and boards.
- **Control validation:** Continuous visibility into policy adherence for data handling and access supports independent assurance and compliance functions.

02 Domain 2 – Operational Risk Management

The purpose of this domain is to maintain an **enterprise-wide framework** for identifying, assessing, monitoring, and reporting on operational risks.

Principle 2: Establish an operational risk management framework (ORMF) that defines risk appetite, policies, taxonomies, and controls

Principles 3: Maintain a documented and forward-looking operational risk appetite integrated with enterprise risk frameworks.

Principles 4: Identify and assess operational risks using tools such as risk and control assessments, key risk indicators (KRIs), operational event data, and scenario analysis.

Principles 5: Continuously monitor and report to detect control weaknesses and potential breaches of risk appetite

How Cyera Helps

Cyera's platform supports these principles through:

- **Risk identification and assessment:** Automatically discovering and classifying sensitive data, enabling identification of data-related operational risks.
- **KRIs and metrics:** Providing measurable indicators such as exposure levels, data policy violations, or risky third-party data flows.
- **Event monitoring:** Integrating with SIEM/SOAR and cloud platforms to contextualize incidents with data-specific risk insights.
- **Scenario analysis inputs:** Enabling simulation of data loss or unauthorized access impacts across business units to test resilience and response.

03 Domain 3 – Operational Resilience

The purpose of this domain is to ensure that **critical operations continue through disruption,** supported by mapping dependencies and vulnerabilities, defining disruption tolerances, and scenario testing.

Principle 6: Identify and map critical operations, dependencies, and vulnerabilities.

Principles 7: Define tolerances for disruption—the maximum downtime or loss a firm can withstand.

Principles 8: Conduct scenario testing to validate the ability to deliver critical operations under severe but plausible scenarios such as cyber incidents, power outages, or third-party failures.

How Cyera Helps

Cyera directly supports operational resilience by:

- **Mapping dependencies:** Building an end-to-end map of data flows, systems, and third-party connections supporting critical operations.
- **Tolerance setting:** Quantifying which data assets are mission-critical, enabling definition of data-centric disruption tolerances and recovery priorities.
- **Scenario testing:** Providing impact modeling for data loss, exposure, or corruption scenarios to evaluate operational continuity
- **Incident readiness:** Delivering forensic visibility into affected data and users during exercises or real events, accelerating recovery and lessons learned.

04 Domain 4 – Key Areas of Operational Risk Management That Strengthen Resilience

This section links E-21 to other OSFI guidelines and risk domains that reinforce resilience:

4.1 Business continuity risk management – testing and planning for operational disruptions.

4.2 Disaster recovery – especially for technology infrastructure and data failover.

4.3 Crisis management – ensuring effective communication and escalation in response to crises.

4.4 Change management – managing operational risk introduced by organizational or technological change.

4.5 Technology and cyber risk management – referencing Guideline B-13, emphasizing secure, recoverable systems.

4.6 Third-party risk management – referencing Guideline B-10 for oversight of vendors and outsourced functions.

4.7 Data risk management – emphasizing governance, architecture, classification, integrity, confidentiality, and breach response.

How Cyera Helps

Cyera's platform directly supports multiple key areas:

- **Data risk management:** Centralized discovery, classification, and monitoring across data environments fulfill OSFI's expectations for data governance, protection, and breach response.
- **Technology and cyber resilience:** Visibility into at-risk data assets enhances technology risk and disaster recovery planning.
- **Third-party oversight:** Cyera identifies and monitors where external vendors handle sensitive data.
- **Change management:** Automated scanning detects when new systems or changes introduce new data exposure risks.

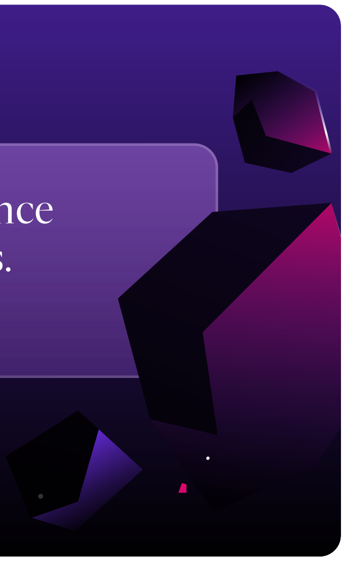
Summary: Compliance Cheat Sheet for OSFI E-21

Cyera helps institutions both prove and improve compliance with OSFI E-21 by delivering continuous, data-driven visibility and control that span the full operational risk lifecycle, from prevention and detection through recovery and learning.

E-21 Requirement	Cyera Capabilities
Principle 1: Roles and responsibilities	Cyera enhances governance by providing unified visibility into sensitive data for clear accountability, delivering timely OSFI-aligned reporting and escalation insights, and continuously validating data-handling controls to support independent assurance and compliance.
Principle 2: Operational Risk Management Framework **Principle 3:** Operational risk appetite defined	Cyera automatically discovers and classifies sensitive data, enabling identification of data-related operational risks.
Principle 4: Identify and assess operational risks	Cyera provides measurable indicators such as exposure levels, data policy violations, or risky third-party data flows.
Principle 5: Continuous monitoring and reporting	Cyera enriches incident monitoring with data-specific risk context and supplies detailed impact insights for scenario analyses that simulate data loss or unauthorized access across business units.
Principle 6: Mapping critical operations, dependencies, and vulnerabilities	Cyera helps you build an end-to-end map of data flows, systems, and third-party connections supporting critical operations.
Principle 7: Define tolerances for disruptio	Cyera helps you quantify which data assets are mission-critical, enabling definition of disruption tolerances and recovery priorities.

E-21 Requirement	Cyera Capabilities
Principle 8: Conduct scenario testing	Cyera helps you model the impacts of data loss, exposure, or corruption to test continuity, while providing forensic insight into affected data and users during exercises or real incidents to accelerate recovery and learning.
Section 4.4: Change management	Cyera detects when new systems or changes introduce new data exposure risks.
Section 4.5: Technology and cyber risk management	Cyera provides visibility into at-risk data assets to enhance technology risk and disaster recovery planning.
Section 4.6: Third-party risk management	Cyera identifies and monitors where external vendors handle sensitive data.
Section 4.7: Data risk management	Cyera provides centralized discovery, classification, and monitoring across data environments to support data governance, protection, and breach response.

See how Cyera can help you embed data-centric intelligence into governance, operations, and cyber security programs. Schedule a demo today at Cyera.com.



CYERA

CYERA.IO