

OSFI B-13 self-assessment

Groupe Conseil GRD. Official source: OSFI Guideline B-13, Technology and Cyber Risk Management (effective January 1, 2024): <https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/technology-cyber-risk-management>

How to use: for each expectation, tick Compliant, Partial or Non-compliant and note the evidence (document, report, screenshot). The statements below are OSFI's section titles from B-13 with their section number; OSFI's official text prevails. The "Useful Microsoft tools" line is a Groupe Conseil GRD suggestion, not an OSFI requirement.

Domain 1. Governance and risk management

Outcome (OSFI): "Technology and cyber risks are governed through clear accountabilities and structures, and comprehensive strategies and frameworks." Useful Microsoft tools: Secure Score, MCSB.

Section	B-13 expectation (OSFI section title)	Compliant	Partial	Non-compliant	Evidence
1.1.1	Senior Management accountability is established	☐	☐	☐	
1.1.2	Appropriate structure, resources and training are provided	☐	☐	☐	
1.2.1	Strategy is proactive, comprehensive and measurable	☐	☐	☐	
1.3.1	RMF is well-aligned and continuously improved	☐	☐	☐	
1.3.2	RMF captures key elements	☐	☐	☐	

Domain 2. Technology operations and resilience

Outcome (OSFI): "A technology environment that is stable, scalable and resilient. The environment is kept current and supported by robust and sustainable technology operating and recovery processes." Useful Microsoft tools: Defender for Cloud, emergency access accounts.

Section	B-13 expectation (OSFI section title)	Compliant	Partial	Non-compliant	Evidence
2.1.1	Architecture framework ensures technology supports business needs	☐	☐	☐	
2.1.2	Architecture is comprehensive	☐	☐	☐	
2.2.1	Technology asset management standards are established	☐	☐	☐	
2.2.2	Inventory is maintained and assets are categorized	☐	☐	☐	
2.2.3	Inventory records and manages technology asset configurations	☐	☐	☐	
2.2.4	Standards for safe disposal of technology assets are established	☐	☐	☐	
2.2.5	Technology currency is continuously assessed and managed	☐	☐	☐	
2.3.1	Technology projects are governed by an enterprise-wide framework	☐	☐	☐	
2.4.1	SDLC framework guides system and software development	☐	☐	☐	

Section	B-13 expectation (OSFI section title)	Compliant	Partial	Non-compliant	Evidence
2.4.2	Security requirements are embedded throughout the SDLC	☐	☐	☐	
2.4.3	Integration of development, security and technology operations	☐	☐	☐	
2.4.4	Acquired systems and software are assessed for risk	☐	☐	☐	
2.4.5	Coding principles provide for secure and stable code	☐	☐	☐	
2.5.1	Changes to technology assets are conducted in a controlled manner	☐	☐	☐	
2.5.2	Segregation of duties controls against unauthorized changes	☐	☐	☐	
2.5.3	Changes to technology assets are traceable	☐	☐	☐	
2.6.1	Patches are applied in a timely and controlled manner	☐	☐	☐	
2.7.1	Incidents are managed to minimize impact on affected systems and business processes	☐	☐	☐	
2.7.2	Incident management process is clear, responsive and risk-based	☐	☐	☐	
2.7.3	Processes are established to investigate, resolve and learn from problems	☐	☐	☐	
2.8.1	Technology service performance is measured, monitored and regularly reviewed for improvement	☐	☐	☐	
2.8.2	Technology infrastructure performance and capacity are sufficient	☐	☐	☐	
2.9.1	Disaster recovery program is established	☐	☐	☐	
2.9.2	Key dependencies are managed	☐	☐	☐	
2.9.3	Disaster recovery scenarios are tested	☐	☐	☐	

Domain 3. Cyber security

Outcome (OSFI): "A secure technology posture that maintains the confidentiality, integrity and availability of the FRFI's technology assets." Useful Microsoft tools: multifactor authentication, PIM, audit log.

Section	B-13 expectation (OSFI section title)	Compliant	Partial	Non-compliant	Evidence
3.0	Confidentiality, integrity and availability of technology assets is maintained	☐	☐	☐	
3.1.1	Security risks are identified	☐	☐	☐	
3.1.2	Intelligence-led threat assessment and testing is conducted	☐	☐	☐	
3.1.3	Vulnerabilities are identified, assessed and ranked	☐	☐	☐	
3.1.4	Data are identified, classified and protected	☐	☐	☐	
3.1.5	Continuous situational awareness and information sharing are maintained	☐	☐	☐	
3.1.6	Threat modelling and hunting are conducted	☐	☐	☐	
3.1.7	Cyber awareness is promoted and tested	☐	☐	☐	

Section	B-13 expectation (OSFI section title)	Compliant	Partial	Non-compliant	Evidence
3.1.8	Cyber risk profile is monitored and reported on	☐	☐	☐	
3.2.1	Secure-by-design practices are adopted	☐	☐	☐	
3.2.2	Strong and secure cryptographic technologies are employed	☐	☐	☐	
3.2.3	Enhanced controls and functionality are applied to protect critical and external-facing technology assets	☐	☐	☐	
3.2.4	Cyber security controls are layered	☐	☐	☐	
3.2.5	Data protection and loss prevention security controls are implemented	☐	☐	☐	
3.2.6	Security vulnerabilities are remediated	☐	☐	☐	
3.2.7	Identity and access management controls are implemented	☐	☐	☐	
3.2.8	Security configuration baselines are enforced and deviations are managed	☐	☐	☐	
3.2.9	Application scanning and testing capabilities are employed	☐	☐	☐	
3.2.10	Physical access controls and processes are applied	☐	☐	☐	
3.3.1	Continuous, centralized security logging to support investigations	☐	☐	☐	
3.3.2	Malicious and unauthorized activity is detected	☐	☐	☐	
3.3.3	Cyber security alerts are triaged	☐	☐	☐	
3.4.1	Incident response capabilities are integrated and aligned	☐	☐	☐	
3.4.2	Cyber incident taxonomy is defined	☐	☐	☐	
3.4.3	Cyber security incident management process and tools are maintained	☐	☐	☐	
3.4.4	Timely response, containment and recovery capabilities are established	☐	☐	☐	
3.4.5	Forensic investigations and root cause analysis are conducted, as necessary	☐	☐	☐	

OSFI also publishes an official Technology and cyber risk management self-assessment tool, linked from the B-13 page.

Need help with your self-assessment? Request a quote: info@grdinc.ca, 514 291-9003.