Key risk management expectations across OSFI guidelines

TORYS LLP

	Expectations				Practical insights
	B-13	B-10	E-21	I&S	
Governance	FRFIs should establish a technology and cyber risk management framework (RMF). The framework should set out a risk tolerance for technology and cyber risks and define an FRFI's processes and requirements to identify, assess, manage, monitor and report on technology and cyber risks.	FRFIs should establish a third-party risk management framework (TPRMF) that sets out clear accountabilities, responsibilities, policies and processes for identifying, managing, mitigating, monitoring and reporting on risks relating to the use of third parties.	FRFIs should put in place an "appropriately robust structure" to delineate their key practices of operational risk management. The form of this structure will depend on the FRFIs' business model and risk profile.	FRFIs should put in place adequate policies and procedures to protect themselves against threats to their integrity or security, including foreign interference.	B-13, B-10 and E-21 all set the expectation that FRFIs will create and implement risk-based frameworks. In recognizing that there is no "one-size-fits-all approach" for managing risks created by technologies, OSFI recognizes that compliance with its guidance will require FRFIs to make numerous risk-based decisions that reflect "the unique risks and vulnerabilities that vary with an FRFI's size, the nature, scope, and complexity of its operations, and risk profile". Since all four guidelines are intended to help FRFIs consider risk mitigation based on their acceptable, considered risk profile, it makes sense for FRFIs to align all of their policies to a consistent, cohesive risk profile. In applying the guidelines, FRFIs should note that taking an action to mitigate a risk in one area (e.g., B-10) may lessen the overall risk assessment under B-13. FRFIs should determine their risk tolerance as a whole before drafting policies and negotiating third-party agreements.

	Expectations				Practical insights
	B-13	B-10	E-21	I&S	
Assessing risk	*Assessing a technology's risk level:* FRFIs should maintain a current and comprehensive asset management system, or inventory, that catalogues technology assets throughout their life cycle, including assets owned or leased by an FRFI, and third-party assets that store or process FRFI information or provide critical business services. The asset management system, or inventory, should be supported by 1) processes to categorize technology assets based on their criticality and/or classification; and 2) documented interdependencies between critical technology assets, where appropriate.	*Assessing a vendor's risk level:* Prior to entering a third-party arrangement, FRFIs should identify and understand the third party's risks, including their information management, data, cyber security and privacy practices, as well as their risk management program, including assurance that significant performance, legal and regulatory requirements are aligned. FRFIs are required to assess third-party arrangements regularly, with higher-risk and more critical arrangements subjected to more frequent and rigorous assessment and more robust risk management.	*Assessing the operational risk:* FRFIs should have a framework for operational risk management that sets forth mechanisms for identifying and managing operational risk, which includes inadequate or failed internal processes and systems.	*Assessing I&S risks:* FRFIs should ask themselves and their vendors: Are persons of good character? Are persons promoting a culture that values compliance, honesty and responsibility? Are persons' actions subjected to sound governance? Are persons' actions being verified to ensure they comply with regulatory expectations, laws and codes of conduct?	In conducting a risk assessment of the relevant technology, FRFIs will need to consider multiple overlapping factors, such as accountability for the management of the technology asset (including, for example, the management of changes, patches and releases), integration of systems, subcontracting, concentration risk of the third party and technology, cybersecurity risk, etc. FRFIs should consider using OSFI's *Cyber Security Self-Assessment* to analyze a technology's cyber risk. In all cases, the assessment should also be informed by legal and regulatory requirements, as well as industry standards. For example, an artificial intelligence system designated as "high risk" under legislation such as the proposed federal *Artificial Intelligence and Data Act* (AIDA) will likely be considered high risk during a B-13 or B-10 assessment.

	Expectations				Practical insights
	B-13	B-10	E-21	I&S	
Managing risks	*Managing technology risks:* FRFIs should put processes and procedures in place for change and release management, patch management, incident and problem management. They should also develop service and capacity standards and processes to monitor operational management of technology, ensuring business needs are met.	*Managing vendor risks:* Throughout the duration of the third-party arrangement, FRFIs should establish and maintain appropriate measures to protect the confidentiality, integrity and availability of records and data. FRFIs should enter into written arrangements that set out the rights and responsibilities of each party. FRFIs' agreements with third parties should encompass the ability to deliver operations through disruption, including the maintenance, testing, activation of business continuity and disaster recovery plans, and ultimately transition services.	*Managing operational risks:* FRFIs should establish a formalized process for mitigating controls when FRFIs undertake significant changes. This involves planning, directing and controlling the day-to-day operations of significant processes and identifying and managing the inherent operational risks in products, activities, processes and systems.	*Managing I&S risk:* FRFIs should manage I&S risk through 1) effective monitoring, control, and reporting procedures; 2) identifying, and reporting deficiencies to senior management; and addressing such deficiencies. Such policies and procedures' effectiveness should be demonstrable and assessed on a regular basis, including when the FRFI identifies new threats or becomes aware of new information.	All four guidelines require that FRFIs mitigate risks created by technology and, if applicable, third-party vendors, by ensuring that there is an operational framework to respond to such risk. In this operational framework, an incident management plan or business continuity plan, for example, should be: 1) adequately and regularly tested to ensure that it is practically workable; 2) preventative and reactive; 3) set out in writing; and 4) responsive to material changes in the arrangement. All four guidelines require that FRFIs manage how material changes are handled. There are a variety of ways to manage changes in practice, such as setting out a detailed change management process, triggering termination grounds or triggering transition service obligations following material changes. When setting up appropriate processes within the organization, cybersecurity vulnerabilities are a key consideration. Organizational (e.g., training and awareness, participating in information-sharing amongst industry actors, etc.), technical (extended detection and response tool, 24/7 monitoring, threat hunting, etc.) and legal measures (template contracts, negotiation playbooks, and internal policies) should be included in this respect.

	Expectations				Practical insights
	B-13	B-10	E-21	I&S	
Performance and incident management	FRFIs should effectively detect, log, manage, resolve, monitor and report on technology incidents and minimize their impacts. FRFIs should respond to, contain, recover and learn from cyber security incidents impacting their technology assets, including incidents originating at third-party providers.	FRFIs should have documented processes in place to effectively identify, investigate, escalate, track and remediate incidents (service and security) to ensure risk levels are kept within an FRFI's risk tolerance.	While E-21 does not expressly deal with incident management, managing operational risks is vital to the ongoing functioning of such incident management plans. E-21 requires that operational risk management frameworks should be designed to permit the collection of information in specific areas. This can be particularly useful in areas such as system breaches or inadequacies (whether indicative of isolated instances of rogue behaviour or wider systemic problems).	The intensity of defences established should be proportional to the likelihood of threats and the severity of impact to the FRFI and their employees, clients and other stakeholders should the technology asset be compromised. Detected incidents and events, including those deemed not to meet the threshold of reporting to OSFI or other authorities, should be documented and inventoried by FRFIs.	FRFIs should ensure that their internal processes and procedures, as well as their vendor arrangements, allow them timely access to accurate and comprehensive information about the performance of their assets and security, such as through technical (e.g., access to systems or logs) or legal measures (e.g., ongoing due diligence, audit rights). In addition, FRFIs should review their vendors' and their own incident response processes and practices and ensure alignment. They should also ensure that their agreements with third parties include provisions relating to 1) notification (including triggers and deadlines); 2) prompt cooperation (including clear expectations relating to information sharing); 3) oversight over the investigation and mitigation measures, including appropriate escalations; and 4) if applicable, responsibility for notification of individuals whose information may be impacted by the incident, including reporting to relevant authorities, such as to OSFI under the *Technology and Cyber Security Incident Reporting Advisory*.