Due diligence checklist: OSFI B-13

Guideline B-13 Technology and Cyber Risk Management. OSFI, Canada.

Regime	OSFI B-13
Regulator	OSFI
Country	Canada
Regulator's page	https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/technology-cyber-risk-management
Prepared	9 November 2026
Current version	https://www.vederca.com/market-scan/due-diligence/ca-b13

What it is

Technology and cyber risk is managed end to end, including risk from technology providers.

Who it applies to

Applies to banks, mutuals and credit unions, insurers and pension and superannuation funds in Canada.

What to ask a vendor, and the evidence to request

#	Ask the vendor for	Evidence to request	Received
1	Security controls, vulnerability management and change management the institution can assess	A description of the security controls, the most recent control testing or penetration test summary, and the policies for vulnerability, change and access management.	
2	Notification of technology and cyber incidents in time for the institution's 24-hour report to OSFI	The incident notification clause and procedure: what counts as an incident, who is told, within what time, and a record of a past notification if one exists.	

In every case

- A named contact at the vendor responsible for this regime, and how the vendor tracks changes to it.
- Which named customers the vendor already serves under this regime, as references you may call.

This checklist is a starting point for a procurement team, not legal advice. Read it with the regulator's own page, your institution's policies and your legal and risk teams; the regime may have changed since the date on this document.