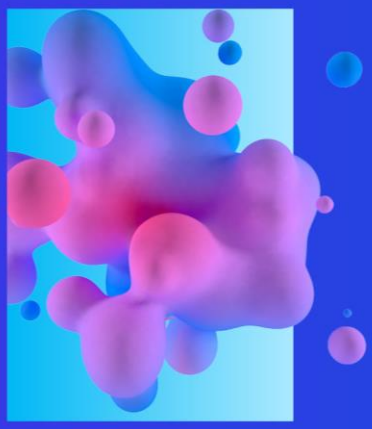
KPMG

Supply Chain Governance and Cyber Risk Management

Regulatory changes to B-10 guideline from OSFI



Organizations are increasingly reliant on third party vendors for driving financial and operational efficiencies, realizing competitive advantages, and to support the growth of the business. The growing dependence on third parties has introduced new risks for organizations, and emphasized the importance of managing risks associated with existing relationships, to effectively manage any potential significant reputational and operational impact due to the compromise of such third parties.

Findings from KPMG's Third Party Risk Management 2022 Outlook

Increasing prevalence of cyber threat actors compromising supply chains to target the organizations is apparent, with the organizations struggling with effectively managing third party risks. Trends highlight:

Global events

63% say that since Covid-19, the organization is not continuously focused on improving the effectiveness of their Third Party Risk Management (TPRM) capabilities.

Fourth parties

79% of the organizations stated that the management of risks associated with the fourth parties across the supply chain still needs improvement.

Business continuity

77% felt that their organization lacks business continuity capabilities to manage any potential disruption to business arising from a third party incident.

Technology

59% flag that the technology made available to the organization does not provide adequate visibility needed to gauge the third party risk across the entire supply chain.

Changing Regulatory Landscape

The regulatory landscape is evolving and Canadian regulators are taking action and introducing new requirements from a third party cyber risk management perspective. Recent revision of B-10 guidelines from OSFI are prime examples, where the revised guidelines place increased focus on supply chain governance and risk management programs. This also accounts to considerations from B-13 guidelines on third party risk management that have now been moved to the revised B-10 guidelines from OSFI. Key changes to B-10 guideline from OSFI, and the associated impact, is summarized in the table below:

Principle Changes	Current Guideline B-10	Revised Draft Guideline B-10
Expanded Scope	Applies to outsourcing arrangements	Applies to third-party arrangements
Widened Risk Lens	Focus on outsourcing risk	Focus on third-party risk and related risks
Enhanced Risk Focus	Reliance on contractual provisions to manage risk	Emphasis on governance and risk management programs
Modernized Guidance	Legal language, dated guidance style	Reorganized and streamlined, sets clear outcomes & principles

Source: OSFI Guideline B-10 Open Letter to FRFIs

For recent B-13 guideline updates and how to navigate the technology & cyber risk landscape, please see our report.

Five focus areas based on changes to B-10

Third Party Governance Framework

Establishing a third-party governance framework 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 facilitates robust management of third party relationships.

Formalized and defined third party governance structures enables the organizations to oversee, monitor and manage the effectiveness and maturity of the TPRM program. Buy-in at the C-Suite level can drive timely completion of necessary initiatives such as developing policies and standards, creating dashboards that report on the risks and performance metrics, and designing a target operating model that considers the people, processes and technologies. Awareness and training on third party security should be facilitated to ensure practices are consistently followed.

Supply Chain Management focused on Risk

Third party relationships should be managed commensurate with risk introduced by such relationships to the organization. Identification of level of risk introduced, empowers the organization with tailoring the risk management activities to each third party relationship. A third party risk management program, supported by a robust criteria for assessing risk associated with third parties enables the organization with:

- Gauging the risk prior to entering the third party relationship and throughout the lifecycle of the relationship
- Conduct due-diligence relative risk and criticality of the third party
- Assess the risks associated with organization's fourth parties

Contract Management

All third party relationships of the organization should be supported by a formalized contract or agreement, that outlines the rights and responsibilities for organization and the third party stakeholders. Contract management for third parties support comprehensive governance over such relationships. Some key areas that can be covered within the contracts are outlined below:

- Data security including what data needs to be protected and controls to facilitate the protection, responsibilities of each party around management of security of data, liability of data compromise and notifications of data breach, etc.
- Management of applicable regulatory requirements, the relationship is subjected to
- Managing compliance with terms, conditions and service level agreements, included within the contract, including resiliency

Business Continuity Planning and Testing

Organizations should establish contingency plans to support continuity of business in case of disruption of third party operations. Requirements around availability of third party services should be formalized within the contracts. Key area around business continuity planning include, but are not limited to:

- Formalized plans to ensure recovery and continuity of organization's services, within reasonable time
- Testing of such plans in collaboration with third party to ensure all involved stakeholders are aware of their responsibilities

Monitoring and Reporting

Organizations should continuously monitor its third parties to ensure compliance of services being delivered with terms and conditions laid out within the contract with such party. Monitoring of third parties should be conducted in accordance with risk associated with third parties, as well as their criticality to the business. Further, organizations should report on identified cyber incidents at third parties, to ensure business resiliency.

Continuous monitoring of third parties enables the organization to confirm that the risk associated with such relationships, is within acceptable level. Formalized metrics to assess and report on risks additionally support prompt action by management around investigation, escalation and remediation of the incident.

Contact us

Adil Palsetia
Partner, Cyber Security
apalsetia@kpmg.ca

Aniket Dharap
Manager, Cyber Security
aniketdharap@kpmg.ca