Office of the Superintendent of Financial Institutions Canada
Bureau du surintendant des institutions financières Canada

Strengthening Third Party Risk Management

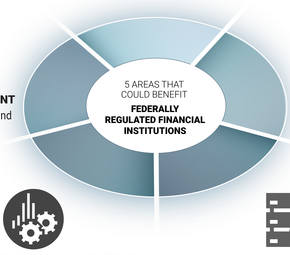
The financial sector today is an interconnected ecosystem of entities, both regulated and non-regulated. Third party risk is frequently cited by Federally Regulated Financial Institutions (FRFIs) as a top or key risk due to increasing FRFI engagement with and reliance on third parties.

In a study conducted in 2019-20 among a subset of FRFIs*, OSFI identified 5 focus areas that can contribute to the effective management of third party risk.

* TOTAL NUMBER OF SURVEY RESPONDENTS: 55 FRFI (47% FROM DEPOSIT TAKING INSTITUTIONS AND 53% FROM INSURANCE)

RISK ASSESSMENT
Comprehensive frameworks to evaluate risk and refresh these assessments

CLOUD RISK MANAGEMENT
Risk identification and mitigation



MONITORING AND INCIDENT MANAGEMENT
Regular monitoring and reporting of risk

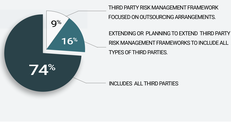
CONTINUITY OF CRITICAL OPERATIONS
Interdependencies identified and tested

DATA SECURITY AND ACCESS
Security standards established and tested

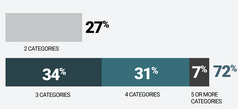
1 RISK ASSESSMENT

Prudent risk management involves focusing on the highest risks at certain providers while providing adequate oversight for providers with lower risk profiles. Developing risk management frameworks with a range of risk categories can help FRFIs more effectively manage the risk from third parties.

Third Party Risk Coverage



Number of categories (e.g., Critical, Moderately High Risk etc.) used by FRFIs for Risk Assessment



2 MONITORING AND INCIDENT MANAGEMENT

Establishing a process to regularly monitor risks against desired standards and measures can help FRFIs identify more effectively whether and when a third party is creating risk. Evaluating third parties solely on service delivery may cause a FRFI to overlook signs of increasing risk. For example, monitoring elevated residual risks as identified in the due diligence process can help FRFIs assess whether remedial actions are timely or mitigating controls are effective.

36% INDICATED THAT THEY MAINTAINED A WATCHLIST, i.e., A LIST OF THIRD PARTIES IDENTIFIED FOR ENHANCED MONITORING

REASONS CITED TO MAINTAIN A WATCHLIST

- RECENT INCIDENTS AT THE THIRD PARTY
- CRITICALITY AND SIGNIFICANCE TO THE FRFI'S OPERATIONS
- ELEVATED RISKS OF FINANCIAL, OPERATIONAL, OR REPUTATIONAL DAMAGE TO THE FRFI.

TOTAL OF 185 REPORTED THIRD PARTY WATCHLIST ITEMS

166 90% FROM DEPOSIT TAKING INSTITUTIONS INSTANCES OF THIRD PARTIES ON THEIR WATCHLISTS

19 10% FROM INSURANCE INSTITUTIONS

3 DATA SECURITY AND ACCESS

Lack of adequate controls and monitoring of third party access, storage and use of FRFI information may expose FRFIs to higher risk of data breaches and loss of confidentiality. Security risk assessments are the first step in protecting FRFI data as these can aid FRFIs understanding if the risk is being sufficiently managed by the third party.

4 CONTINUITY OF CRITICAL OPERATIONS

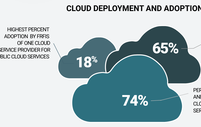
Identifying critical third party dependencies and conducting joint exercises with these parties can help reinforce recovery processes, communication channels, authority levels and the trust relationships necessary to work cohesively and collaboratively through a disruption.

Respondents with management of critical third parties in scope of the study (17)

5 CLOUD RISK MANAGEMENT

Cloud adoption has moved past proof of concept testing and towards an established or emerging practice of assessment and onboarding at FRFIs. While managing Cloud services is a shared responsibility between the FRFI and the Cloud service provider, developing Cloud specific standards may enable FRFIs to increase interoperability and optimize Cloud adoption while operating within the FRFI's risk appetite and tolerances.

CLOUD DEPLOYMENT AND ADOPTION

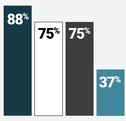


14 AVERAGE NUMBER OF SIGNIFICANT CLOUD DEPLOYMENT FOR BANKING SECTOR

9 AVERAGE NUMBER OF SIGNIFICANT CLOUD DEPLOYMENT FOR INSURANCE SECTOR

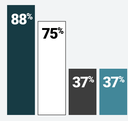
Respondents with Cloud Risk Management in scope of the study (8)

CLOUD ADOPTION CHALLENGES



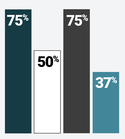
- 88% Effective management of cloud migrations
- 75% Lack of understanding of internal process for cloud management
- 75% Portability
- 37% Lack of available skillsets to use and support cloud implementations

CHALLENGES IN CLOUD COMPUTING OPERATIONS



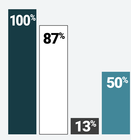
- 88% Protection of sensitive data both in transit and at rest
- 75% Controls to prevent, detect and respond in timely manner to unauthorized access
- 37% Controls relating to administration of console system access and encryption key management
- 37% Controls to ensure appropriate isolation from third parties against intentional or inadvertent security incidents

CLOUD STANDARDS, RISK MANAGEMENT, AND ASSURANCE ACTIVITIES



- 75% Have established governance frameworks for oversight of cloud alignment with the FRFI strategy and assessment and acceptance of risk
- 50% Do not have requirements for security log integrity, log access management, cloud specific data encryption or data governance controls
- 75% Have had the adequacy of cloud service providers' assurance of information security and other controls assessed by Internal Audit.
- 37% Reported differences in their approach to auditing and sampling of cloud services as compared to traditional audits

CLOUD AVAILABILITY AND EXIT STRATEGY



- 100% Indicated that the high availability and disaster recovery requirements are managed by the CSP
- 87% Reported coordination of recovery activities as an area lacking role clarity
- 13% Have developed an exit strategy for cloud service providers
- 50% Have a cloud exit strategy in development

Canada