Instructions

Title	OSFI technology and cyber incident report – Detailed instructions
Date	January 15, 2025
Sector	Banks Foreign Bank Branches Life Insurance and Fraternal Companies Property and Casualty Companies Trust and Loan Companies

Table of Contents

General instructions

Instructions for incident form sections

- Incident information
- Site location and lines of business affected
- Incident details
- Cyber threat actor details
- Internal and external notifications

General instructions

As per our Technology and Cyber Security Incident Advisory, institutions must report a technology or cyber security incident within 24 hours, or sooner if possible. A list of reporting criteria is available within the Advisory.

Mandatory fields must be completed at a minimum for initial reporting of active/ongoing incidents. Other fields can be completed in subsequent updates when the information becomes available. Mandatory fields are identified with an asterisk (*). For resolved incidents please provide as much information as available.

Information provided can be best estimates, including financial or customer impact, and may not be definitive at the time of reporting. Information provided can also be updated in the post-incident report.

Until the incident is resolved, we expect institutions to provide situation updates, including any short term and long-term remediation action plans and timelines.

Depending on the severity, impact, and velocity of the incident, we may recommend methods and frequency of subsequent updates.

Institutions should submit their incident report to the Technology Risk Division at TRD-DRT@osfi-bsif.gc.ca and their lead supervisor.

Instructions for incident form sections

Incident information

Institution name	Record the legal name of the Federally Regulated Financial Institution.
Incident name or identifier	Record the identifier used internally by federally regulated financial institutions to identify the incident. For example: • INC000001 • CIRT-MAJ-001 • Cyber incident 2024-941 – Account Takeover
Incident report type	The initial submission is the first report submitted by the institution. Once the initial report has been submitted, all subsequent reports should be considered as updates. For updated reports, the same incident name or identifier can be used.
Incident status	An active incident is an incident that is currently ongoing and requires containment or recovery efforts that are not yet effectively implemented. Active incident reports should have as much detail as possible in the incident description field to minimize information requests. Active incidents require regular updates until they have been resolved and closed. A resolved incident is one that has been fully addressed, with all necessary actions taken to mitigate its impact and restore normal operations.
Date, time and time zone the incident occurred	The actual date and time of the incident occurrence, either at the institution or at a third-party. Once the date has been selected, please enter the time and time zone in the designated fields. Please note that the time should be entered in a 24-hour format (YYYY-MM-DD HH:mm).
Date, time and time zone the incident was detected	The actual date and time of the incident detection, either by institution or by a third-party. Once the date has been selected, please enter the time and time zone in the designated fields. Please note that the time should be entered in a 24-hour format (YYYY-MM-DD HH:mm).

Site location and lines of business affected

Where did the incident occur?	Select from the drop-down list the most appropriate entity where the incident occurred. If the incident took place at: • a subsidiary or joint venture partner choose “Institution-Subsidiary” • an institution’s foreign branch, choose “Institution” • a third-party’s subcontractor or fourth party choose “Subcontractor” If “other” is selected, please provide details in the next field.
Third-party, subcontractor, or other details	If the incident originated at a third party or subcontractor, indicate their full legal name.
Business line and service identification	A business line refers to a specific area of operation. For example: • retail banking • capital markets • credit assessment • online services • payment and settlement • wealth management • insurance underwriting • claims settlement • human resource • reinsurance • corporate accounting • customer service Indicate all business lines or services impacted, separated with a comma, and avoid acronyms.
Geographic site or locale affected	If the incident has an impact beyond a single location, provide a list of affected locations or descriptions of the geographical extent of the incident. Also include the names of the countries or jurisdictions that have been affected. Enter the affected sites or locale affected (for example, city, province or state, country, world-wide.

Technology assets affected	A technology asset is a tangible (for example, hardware, infrastructure) or intangible (for example, software, data, information) item that facilitates the delivery of technology services. Please indicate the names of the technology assets affected and indicate whether it is a critical asset. If the function is not apparent from the name, provide a brief description. Expand all acronyms.

Incident details

Incident category	A technology incident is any disruption or failure of technology assets that affects business operations or services. A cyber incident is any incident involving unauthorized access or malicious activity targeting information systems, data, or networks, often with the intent to steal, disrupt, or damage technology assets.
Incident result	The incident result is the outcome or adverse impact of the incident on the organization's technology assets and operations. This reflects how the incident affected the confidentiality, availability, or integrity of services, systems, or data. A "compromise" is an incident result when data, systems, or users are compromised because of data exposure, account takeover, or privileged access to systems gained by unauthorized entities for example. A "degradation" is an incident result when a service or application operates at diminished capacity, such as slow responses to queries or delays in processing. An "outage" is an incident result when a service or function is unavailable or offline.

Incident type

An incident type describes how a technology asset has been determined and observed to be deteriorated.

An incident type can also indicate a threat vector or attack technique, such as phishing and malware, used by a threat actor which leads to an incident result (degradation, outage, or compromise).

Select the best match from the list below.

Account takeover

> An incident where an unauthorized party gains access to a user or customer account.

Application issue

> Flaws or failures in software application layer that have resulted in performance issues, vulnerabilities, or other operational problems.

Data loss or exposure

> The unauthorized access, disclosure, misuse, or destruction of information, often resulting in a breach of privacy or loss of critical data.

Denial of service

> The unavailability of a service or application due to overwhelming traffic from coordinated and possibly multiple malicious sources.

Infrastructure issue

> Flaws and failures within an underlying infrastructure technology system adversely affecting operational functionality. For example, failures in servers or network, hardware, operating systems, virtualization, middleware, database, and data centres causing degradation and outage.

Malware or ransomware

> An incident involving the use of malicious software designed to damage, disrupt, or gain unauthorized access to technology assets such as viruses, trojans, worms, and ransomware.

Phishing

> A deceptive attempt, usually through email, to trick individuals into revealing sensitive information, such as passwords or credit card numbers, by impersonating a trustworthy entity.

Unauthorized access

> When a malicious entity gains access to an internal system or data. This can include threat actors gaining access to a database or client computer.

Other

> Provide details in the incident description field below.

Incident severity or priority	The severity or priority levels represent the incident classification levels based on the potential impact of the incident. Institutions should use their internal assessment processes to ascertain the potential impact, with Severity 1, Priority 1, or Critical being the highest level of impact. If internal categories exceed the 4 tiers, select an option as close to the level as possible.
Incident description	The incident description should provide any additional information that is not captured in the previous fields and provide more context surrounding the incident, its detection, impacts, affected internal and external parties, planned remedial actions, and lessons learned. Information can include incident details, such as: • detection method • known direct and indirect impacts • affected internal and external parties • actions completed and pending • estimated timelines to resolve incident or to implement enhancements or controls • any planned or implemented workarounds in place for active incidents.
Breach of recovery point objective (RPO) or recovery time objective (RTO)	RTO refers to the maximum allowable time to restore systems, services, or data following an incident. RPO refers to the maximum amount of data loss that can be tolerated, measured in time. It defines the point in time to which data must be restored after an incident. If “under assessment” is selected during an initial report, please confirm RTO/RPO breach in a subsequent update.
Activation of business continuity plans (BCPs) or disaster recovery plans (DRPs)	BCPs are the procedures to maintain essential operations during and after an incident, disruption, or crisis. DRPs are a set of policies and procedures for restoring systems and data after a disaster or major incident. If “under assessment” is selected during an initial report, please confirm BCP/DRP activation in a subsequent update.

Impact scope – Service delivery	If the incident has impacted the ability to deliver a service, select the level of impact identified by the institution from the drop-down list. The rating is from none through low, moderate, high to critical. If service delivery impact is under assessment, please provide the assessed rating in a subsequent update.
Impact scope – (Loss of) Sensitive information	If the incident includes exposure or loss of sensitive data, select the level of impact identified by the institution from the drop-down list. The rating is from none through low, moderate, high to critical. If sensitive data impact is under assessment, please provide assessed rating in a subsequent update.
Impact scope – Media or public sentiment	Describe any reporting, statements or sentiment arising from mainstream or social media channels. Enter the current level of media or public discourse resulting from the incident.
Estimated financial impact or financial risk (in CAD)	This represents the estimated total cost for the incident response effort, plus remediation (including remediation for clients). If financial impact is under assessment, please provide the estimated cost in a subsequent update.
Estimated number of impacted users, clients, or transactions	Provide the estimated number of employees, clients, or transactions impacted by the incident.
Estimated recovery timeframe	If the incident is ongoing or still active, please provide best estimate of date and time when the incident will be resolved or is expected to be resolved.
Incident duration	Please provide the total duration for resolved incidents. This should be measured from the incident occurrence to the return to normal operations. Indicate the time in units of days, hours, and minutes.
Incident recurrence	If the incident is related to a previous incident, please provide the reference(s) to the previously reported incident(s). If incident recurrence relation is under assessment, please provide assessment result in a subsequent update.

Incident root cause	The root cause of an incident is the underlying factor that must be addressed to prevent a reoccurrence of the chain of events that led to the incident. If the root cause is known at the time of reporting, select the appropriate one. Provide additional details including (but not limited to): cause of the issue, failed controls resulting in the incident, and planned improvements to prevent incident reoccurrence in the root cause description field. If the root cause is under assessment, provide the root cause information in subsequent updates or in the post-incident report submission. The incident root cause descriptions are as follows: Capacity management Issues arising from systems being overwhelmed due to excessive, non-malicious, user demand or IT resource (for example, memory, CPU, virtualizations, servers, storage etc.) limitations. Configuration error Incidents resulting from incorrect or improper settings within technology assets. Deficient process Issues arising from inadequate or inefficient procedures, steps, instructions, or workflows. Design flaw Problems originating from flaws or weaknesses in the architectural design of technology solutions. Facilities or physical security Incidents stemming from unauthorized access or physical breaches of secure locations (for example, data center, server rooms, offices, housing critical technology assets.) Failed redundancy Incidents occurring when backup or redundancy mechanisms, such as failover to an alternate site, fail to provide continuity during system disruptions. Faulty equipment Technology asset failures due to malfunctioning hardware or software components. Human error Incidents caused by mistakes or oversight made by individuals while using technology. Natural disaster Incidents caused by extreme natural events like earthquakes, floods, or hurricanes disrupting hardware and infrastructure. Outdated technology asset Incidents arising from using outdated or unsupported technology assets, leaving

Cyber threat actor details

Threat-actor tactics, techniques, and procedures (TTP) (cyber incidents)	TTPs describe the behavior of a threat actor. A tactic describes a threat actor behavior at the highest-level. Techniques give a more detailed description of it, and procedures are the lowest level detailed actionable steps. Where applicable, include known details about the threat actor's behavior, including vulnerabilities exploited and threat-actor attribution.
Indicators of compromise (IoC)– Hash, URL, email, IP, etc.	Indicators of compromise are essentially evidence or trace of malicious activities or behaviour left behind by a threat-actor. Where applicable, provide any known technical or non-technical indicators, including any references (for example, NVD, CVE) to exploited vulnerability. These could include unusual actions, IP addresses, URLs, mail header fields or file hashes. For example: • unusual or unknown login location or login time • Hxxps://malicious.url.example/page.asp • CVE-2024-01283 • IPv4 or IPv6 address • badsender@malicious.domain[.]example • 44d88612fea8a8f36de82e1278abb02f

Internal and external notifications

Senior management notification	Select from the drop-down list whether senior management (executives, board members, etc.) have been notified of the incident. If the senior management has been notified enter the actual date and time of notification. Once the date has been selected, please enter the time and time zone in the designated fields. Please note that the time should be entered in a 24-hour format (YYYY-MM-DD HH:mm).
Other regulatory or supervisory notification	Enter the name(s) of the notified regulatory or supervisory entity within the free-text field.
Law enforcement or security agency notification	Enter the name(s) of the notified law enforcement or security agency within the free-text field.
Cyber insurance notification or claim submission	Indicate whether insurance or cyber-insurance providers have been notified or a claim has been filed as a result of the incident.

Footnotes

* Mandatory field