FSRA
Financial Services Regulatory Authority of Ontario

Guidance

☑ Interpretation | ☑ Approach | ☑ Information | ☐ Decision

Effective Date: April 1, 2024
Identifier: No. GR0016INT

Information Technology ("IT") risk management

Table 1 presents the applicable sections of the Guidance, organized by regulated entity or individual.

Table 1: Guidance outlined by regulated entity or individual

Regulated entity	Applicable sections	Overview of applicable sector-specific sections
Credentialing Bodies for Financial Planners and Advisors	• All sectors section • Sector-specific Approach for Credentialing Bodies for Financial Planners and Advisors	• FSRA's supervisory approach for assessing IT risk management

Ontario

Credit Unions and Caisses Populaires	• All sectors section • Sector-specific: Interpretation/Approach for Credit Unions and Caisses Populaires	• FSRA's interpretation of IT risk management requirements under the *Sound Business and Financial Practices Rule* and the *Credit Unions and Caisses Populaires Act, 2020* • FSRA's supervisory approach for assessing IT risk management (aligns with the Operational risk and resilience Guidance)
Health Service Providers	• All sectors section	• No sector-specific content
Insurance Agents, Insurance Agencies, Adjusters and Adjusting Firms	• All sectors section • Sector-specific: Approach for Non-Ontario Incorporated Insurance Companies, Insurance Agents, Insurance Agencies, Adjusters and Adjusting Firms	• FSRA's supervisory approach for assessing IT risk management
Loan and Trust companies	• All sectors section	• No sector-specific content

Mortgage Brokerages, Mortgage Agents, Mortgage Brokers, and Mortgage Administrators	• All sectors section • Sector-specific: Approach/Information for Mortgage Administrators, Mortgage Agents, Mortgage Brokerages, and Mortgage Brokers	• Information on how existing Guidance MB0048INF MBRCC's Principles for Cybersecurity preparedness for the Mortgage Brokering Sector aligns with this Guidance and how FSRA will approach non-compliance
Ontario-incorporated Insurance Companies and Reciprocals	• All sectors section • Sector-specific: Interpretation/Approach for Ontario-incorporated Insurance Companies and Reciprocals	• FSRA's interpretation of IT risk management requirements under the *Insurance Act* • FSRA's supervisory approach for assessing IT risk management
Non-Ontario Incorporated Insurance Companies	• All sectors section • Sector-specific: Approach for Non-Ontario Incorporated Insurance Companies, Insurance Agents, Insurance Agencies, Adjusters and Adjusting Firms	• FSRA's supervisory approach for assessing IT risk management

Pension Plan Administrators	• All sectors section • Sector-specific: Interpretation/Approach for Pension Plan Administrators	• FSRA's interpretation of the *Pensions Benefits Act* relating to IT • FSRA's supervisory approach for assessing IT risk management

Purpose and scope

The Financial Services Regulatory Authority's ("FSRA's") IT risk management Guidance ("Guidance") communicates:

- 'Practices[1] for effective IT risk management' under the Information section.
- A process for regulated entities and individuals to notify FSRA[2] in the event of a material IT risk incident under the Approach section.
- Sector-specific Guidance, including interpretations of requirements for Credit Unions and Caisses Populaires ("Credit Unions"), Ontario-incorporated Insurance Companies and Reciprocals ("Insurers"), and Pension Plan Administrators.

This Guidance is applicable to all entities and individuals regulated by FSRA. The Guidance describes practices and desired outcomes for regulated entities and individuals but does not prescribe how to achieve them. This principles-based approach offers regulated entities and individuals the flexibility to achieve the outcomes in a manner that is suitable for the size and nature of their business.

[1] The Practices for effective IT risk management have been developed by FSRA based on national and international standards.
[2] Both the Chief Executive Officer (CEO) of FSRA and FSRA may exercise regulatory authority under the legislation they administer. However, for the purposes of this Guidance, reference will only be made to FSRA as the CEO may delegate authority to FSRA staff, as permitted by s. 10(2.3) of the *Financial Services Regulatory Authority of Ontario Act,* 2016.

This Guidance[3] includes **Interpretation**, **Information**, and **Approach** sections:

- Interpretation Guidance sets out FSRA's interpretation of applicable requirements under its legislative mandate (i.e., legislation, regulation and rules). Non-compliance can lead to enforcement or supervisory action.

- Information Guidance provides information on certain topics such as practices without creating any compliance obligations for regulated entities and individuals.

- Approach Guidance describes FSRA's principles, processes, and practices for supervisory activities and application of FSRA Chief Executive Officer's discretion without creating any compliance obligations for regulated entities and persons.

Outline

The Guidance is segmented in two main sections:

- **All sectors** – Interpretation, Information, and Approach Guidance is applicable to all FSRA regulated entities and individuals. This section contains:

    - Interpretation on existing regulatory requirements

    - Information on 'Practices for effective IT risk management'

    - Approach on 'Notification of material IT risk incidents' to FSRA

- **Sector-specific** – Guidance applicable to FSRA regulated entities or individuals in a specific sector.

[3] This Guidance is being published as combined Interpretation, Approach, and Information Guidance under FSRA's Guidance framework. Each component is labelled for clarity.

As a principles and risk-based regulator, FSRA's regulatory approach differs in accordance with the size and nature of the regulated entities and individuals. While the **'All sectors' section of this Guidance applies to all FSRA regulated entities and individuals**, some regulated entities and individuals have specific sector-specific Guidance. FSRA has made this determination based on the risk posed to consumers, credit union members and pension plan beneficiaries[4], and the risk to the regulated entity/individual or other entities or individuals in the same sector. For some regulated entities and individuals, there is no sector-specific Guidance.

Rationale and background

FSRA defines "IT risk" as the risk of financial loss, operational disruption or damage, or reputational loss resulting from the inadequacy, disruption, destruction, failure, or damage by any means to a regulated entity or individual's IT systems, infrastructure, and data.

IT risk can be external or internal to a regulated entity or individual. IT risk encompasses, but is not limited to, cyber risk. While cyber risk specifically relates to deliberate or accidental breaches of security (e.g., a data breach), IT risk also includes any risk extending from the use of IT (e.g., aging digital infrastructure).

IT risk represents a significant and growing threat to the businesses, operations, and to the stability of FSRA's regulated sectors. Incidents can result in negative impacts[5] to consumers, credit union members and pension plan beneficiaries, which can disrupt confidence in the financial services and pension sectors.

FSRA's focus on IT risk is consistent with FSRA's statutory objects, as set out in the *Financial Services Regulatory Authority of Ontario Act, 2016*, including to:[6]

---

[4] For the purposes of this Guidance, this group will also include the public, policy holders, investors, and other stakeholders.
[5] Negative impacts can include financial losses, breach of privacy and/or confidential information, and a lack of ability to access essential services.
[6] *Financial Services Regulatory Authority of Ontario Act, 2016, S.O. 2016, c. 37, Sched. 8*.

- regulate and generally supervise the regulated sectors
- contribute to public confidence in the regulated sectors
- promote high standards of business conduct
- protect the rights and interests of consumers
- foster strong, sustainable, competitive and innovative financial services sectors
- promote good administration of pension plans
- protect and safeguard the pension benefits and rights of pension plan beneficiaries
- promote and otherwise contribute to the stability of the credit union sector in Ontario

All sectors

Interpretation – All sectors

Comply with existing requirements

Regulated entities and individuals must comply with existing requirements related to IT risk and the protection of personal information. This includes, but is not limited to, the requirements contained within the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), as applicable. Failure to comply with such requirements is likely to result in harm to consumers, credit union members and pension plan beneficiaries.

Consequently, FSRA considers compliance with existing applicable requirements related to IT risk, and the protection of personal information, as a factor that can impact:

- the assessment of a licensee's suitability to obtain or renew a licence
- incorporating with FSRA as a credit union or insurance company

- registering with FSRA
- being approved or maintaining status as a credentialing body for financial planners and advisors

Information – All sectors

This section is applicable to all regulated entities and individuals.

Practices for effective IT risk management

The following ‘Practices for effective IT risk management’ describe industry accepted practices for effective management of IT risk. FSRA expects all regulated entities and individuals to follow the practices for effective IT risk management. FSRA will consider adherence to these practices and their desired outcomes when supervising, and during licence issuance and renewal.

Note for FSRA regulated individuals operating within a regulated entity (for insurance and mortgage broker sectors only):

While some regulated individuals are responsible for managing the IT risks of their business, others are employees or contractors of a FSRA regulated entity which are ultimately responsible for managing risk in this area (e.g., insurance agents/adjusters employed by or contracted with an insurer, and mortgage agents and brokers working for a brokerage). The latter of these regulated individuals are still responsible for conducting themselves in a manner consistent with the spirit of the practices for effective IT risk management and their desired outcomes.

For example, while regulated individuals that are employees or contractors of a regulated entity will not be responsible for developing a risk management strategy, a good practice would be to follow the strategy established by the regulated entity.

Practice 1: Governance – The regulated entity or individual has proper governance and oversight of its IT risks

Desired outcomes:

- IT risks are effectively governed by regulated entities and individuals.
- Clear responsibilities for the management of IT risks are assigned to an individual or individuals with sufficient seniority and expertise.
- Accountability of IT risk oversight rests with Senior Management (in some instances, the licensee) and the board of directors (if applicable).

Practice 2: Risk management – The regulated entity or individual relies on industry accepted practices to effectively manage its IT risks

Desired outcomes:

- For applicable regulated entities, board oversight of the entity's IT risk management activities is effective.
- Regulated entities and individuals have strategies and frameworks in place to effectively manage IT risk.

Practice 3: Data management – The regulated entity or individual uses industry accepted strategies to effectively manage and secure confidential data

Desired outcomes:

- Confidential data overseen by regulated entities and individuals is secure.
- Confidential data is appropriately handled and stored in a manner that maintains data quality, integrity, availability, and privacy.

Practice 4: Outsourcing – The regulated entity or individual effectively manages the IT risks associated with any outsourced or co-sourced activity, function, and service[7]

Desired outcomes:

- IT risks for outsourced and co-sourced activities, functions and services are properly identified, assessed, and managed.
- Accountability and ownership for any outsourced or co-sourced function is maintained by regulated entities and individuals.

[7] This encompasses all activities, services and arrangements undertaken by a party external to the regulated entity or individual's business. This includes all third-party service provides and activities that are co-sourced.

Practice 5: Incident preparedness – The regulated entity or individual is prepared to effectively detect, log, manage, resolve, recover, monitor, and report on IT incidents in a timely manner

Desired outcomes:

- The impact and likelihood of IT risk incidents is minimized.
- Regulated entities and individuals learn from previous incidents to better prevent future incidents.

Practice 6: Continuity and resiliency – The regulated entity or individual is prepared to ensure the continuity of their IT assets and their ability to deliver critical services during and following an incident

Desired outcomes:

- Regulated entities and individuals maintain the availability of financial services.
- Regulated entities and individuals are operationally resilient.

Practice 7: Notification of material IT risk incidents – The regulated entity or individual notifies its regulator(s) in the event of a material IT risk incident (see notification of material IT risk incidents section)

Desired outcomes:

- Regulated entities and individuals are transparent to FSRA regarding material IT risk incidents.
- Through notification, regulated entities and individuals assist FSRA in identifying high risk areas in a timely manner that can help prevent future incidents.

Approach – All sectors

Notification of material IT risk incidents

Effective IT risk management practices for regulated entities and individuals include notifying regulatory authorities as soon as is reasonable, which normally falls within 72 hours or sooner[8], after determining that an IT risk incident is material. FSRA will maintain confidentiality of any incidents reported by regulated entities and individuals to the extent allowed by the law.

When FSRA becomes aware of an IT risk incident, either through direct notification (e.g., via the IT Risk Incident Notification Form) by the regulated entity or individual, or through other channels (e.g., complaint, media report, etc.), FSRA will determine whether to activate its **protocol for IT risk incidents** (as described below). This means that in some instances, FSRA will consider notification of the incident sufficient and determine that activation of the protocol for IT risk incidents is not warranted.

[8] For Credit Unions and Ontario-incorporated Insurance Companies and Reciprocals, 72 hours is considered the maximum amount of time before notifying FSRA.

When reporting an IT risk incident, regulated entities or individuals can notify FSRA by:

- Emailing the 'IT Risk Incident Notification Form' to the ITriskinbox@fsrao.ca email address.
- Uploading the 'IT Risk Incident Notification Form' and any other supporting documentation to the Incident Notification Portal.
- Direct contact with relationship manager (if applicable), or Pension Officer/Analyst.

To reduce burden on regulated entities or individuals that are required to submit multiple incident reports, FSRA will also accept being notified with a comparable form issued by another financial services regulator.

A good practice for regulated individuals that are employees or contractors of a regulated entity is to report any incident to that regulated entity. Regulated entities can make the determination if a breach is material, and, if so, subsequently by notifying FSRA.

For the **Mortgage Brokering sector,** this Guidance, including the Practices for effective IT risk management, the IT Risk Incident Notification Form and the Protocol for IT risk incidents are consistent with the Mortgage Broker Regulators' Council of Canada Principles for Cybersecurity Preparedness for the Mortgage Brokering Sector Guidance (MBRCC Guidance). Following this Guidance will satisfy the MBRCC Guidance and in areas of inconsistency this Guidance will take priority.

For **Pension Plan Administrators**, this Guidance, including the Practices for effective IT risk management, the IT Risk Incident Notification Form and the Protocol for IT risk incidents are consistent with the Canadian Association of Pension Supervisory Authorities' ("CAPSA") guideline on cyber risk for Pension Plans. Following this Guidance will satisfy the CAPSA guideline and in areas of inconsistency this Guidance will take priority.

Material IT risk incident

Regulated entities and individuals should notify FSRA only when an IT risk incident is “material”. What constitutes a material incident is to be determined by the regulated entity or individual based on the impact to their business, its operations, and to its consumers, credit union members, or pension plan beneficiaries.

Regulated entities and individuals (excluding Pension Plan Administrators)

Indicators that a material incident has occurred could include, but are not limited to, the following (for all regulated entities and individuals excluding pension plan administrators). If the incident:

- results in significant operational disruptions to business systems and functions
- significantly disrupts the consumers/members’ ability to access essential services for a prolonged period
- impacts a third-party provider to the extent that it has significant impacts on the regulated entity or individual
- breaches internal risk appetite or thresholds
- requires non-routine measures or resources
- results in the exposure of a large amount of confidential data
- is recurring and could have a significant impact on a cumulative basis
- is reported to Senior Management or the board of directors
- is reported to another regulator, a law enforcement agency, the Office of the Privacy Commissioner, etc.
- results in a claim for cyber insurance

- results in or will likely result in negative media attention that could damage the reputation of the regulated entity/individual or the sector for which they operate

- is likely to negatively affect other entities or individuals regulated by FSRA, or it is an incident that is likely to reoccur with other entities or individuals regulated by FSRA

Pension Plan Administrators

Indicators that a material incident has occurred could include but are not limited to the following for pension plan administrators. If the incident:

- disrupts the operations of the pension plan to an extent that the plan can no longer be effectively administered

- is likely to negatively affect other entities or individuals regulated by FSRA, or it is an incident that is likely to reoccur with other entities or individuals regulated by FSRA

- compromises confidential plan member data

- impacts the ability of the administrator to pay benefits

All regulated entities and individuals

If the regulated entity or individual is unsure if an IT risk incident is material, regulated entities and individuals can contact FSRA through the ITriskinbox@fsrao.ca email address, or through their relationship manager (if applicable), or Pension Officer/Analyst.

FSRA has the authority to request information from its regulated entities and individuals through the various statutes that it administers. FSRA may request information from regulated entities and individuals, either targeted or sector wide, to verify that it is receiving timely information on material IT risk incidents.

Activation of FSRA's Protocol for IT risk incidents

FSRA's decision to activate the Protocol for IT risk incidents

The protocol outlines FSRA's expected engagement with the regulated entity or individual to monitor the actions taken in investigating and responding to the incident. The engagement is continuous[9], until FSRA has:

- An adequate understanding of the extent of the incident, including if any confidential data has been breached and what information was accessed.
- Confirmation that impacts have been addressed, including, but not limited to:
    - Confirmation that any corrupted information has been restored and/or that the incident has been mitigated or contained.
    - Confirmation that all systems are back online and fully functional.
    - Confirmation that all affected stakeholders, including clients and relevant privacy regulators, have been notified, and reasonable steps have been taken by the regulated entity or individual to limit harm to consumers, credit union members and pension plan beneficiaries.
- An adequate understanding of the safeguards that have been put in place to ensure the regulated entity or individual is protected from similar incidents.

As FSRA becomes aware of an IT risk incident, either through direct notification by the regulated entity or individual, or through other channels (e.g., complaint, media report, etc.), FSRA will determine whether to activate its protocol for IT risk incidents. In some instances, FSRA may determine that activation of the protocol for IT risk incidents is not warranted.

[9] It may also be determined early in the process that the incident does not require further information and FSRA will deactivate the protocol.

FSRA will maintain confidentiality of incidents reported to the extent allowed by the law.

Protocol for IT risk incidents - Three phase protocol

FSRA will typically follow the following approach to respond to incidents:

Phase 1: Receive a notification from the regulated entity or individual detailing the available information regarding the incident, including what has been done to recover and respond, and what additional actions are planned.

Phase 2: Once FSRA has determined that the Protocol for IT risk incidents should be activated, FSRA establishes contact with the regulated entity or individual. The regulated entity or individual provides FSRA with regular updates on the impact of the incident to operations and services, as well as any impact to consumers, credit union members or pension plan beneficiaries. The information requested by FSRA will depend on the nature of the incident.

Phase 3: FSRA receives the regulated entity or individual's plan to prevent a similar incident in the future.

FSRA's determination to activate the Protocol for IT risk incidents, and its level / frequency of involvement with a regulated entity or individual, reflects the nature of the IT risk incident, as well as the size and nature of the regulated entity or individual.

Sector-specific

This section contains Guidance appliable to regulated entities or individuals in specific sectors.

- Credentialing Bodies
- Credit Unions and Caisses Populaires
- Mortgage Brokers, Mortgage Agents, Mortgage Administrators and Mortgage Brokerages

- Non-Ontario Incorporated Insurance Companies, Insurance Agents, Insurance Adjusters, Adjuster Firms, and Insurance Agencies
- Ontario-incorporated Insurance Companies and Reciprocals
- Pension Plan Administrators

For regulated entities and individuals that are not included in this section, please refer to the All sectors section which is applicable to all FSRA regulated sectors.

Credentialing Bodies for Financial Planners and Advisors

Approach

Under FSRA's 'Financial Professionals Title Protection – Administration of Applications' Guidance[10], Credentialing Bodies ("CBs") for Financial Planners and Advisors are required to demonstrate that they meet certain prescribed standards. Approved CBs must demonstrate that they have:

- Safety and security measures, which ensure that information technology systems and electronic data are protected.
- Processes and procedures in place to mitigate any disruption in operations.

[10] Financial Professionals Title Protection - Administration of Applications.

FSRA also reviews if CBs have:

- An IT strategy which includes measures for hardware, software and data protection including:
    - strong IT controls in place to protect its electronic data
    - policies that ensure strong passwords are in place for electronic devices, the use of Anti-virus software and firewalls electronic data back-up and the use of off-side / cloud storage
- a business continuity plan to minimize any service disruption
- IT electronic data back-up
- off-site / cloud storage

IT risk comprises part of FSRA's principles and risk-based approach to the supervision of CBs, as outlined in FSRA's 'Financial Professionals Title Protection – Supervisory Framework' Guidance.[11]

FSRA may conduct thematic examinations based on IT risk, and this Guidance will be used to assess whether CBs have met the prescribed conditions outlined in the 'Administration of Applications' Guidance.

The *Financial Professionals Title Protection Act, 2019* ("FPTPA") and FSRA's Rule 2020-001 – Financial Professionals Title Protection ("FPTP Rule") permit FSRA to revoke a CB's approval if it is not in compliance with the FPTPA, the FPTP Rule, or the terms and conditions of its approval.

[11] Financial Professionals Title Protection - Supervisory Framework.

Credit Unions and Caisses Populaires

Interpretation

FSRA's Interpretation of IT risk management requirements under Rule 2021-001 Sound Business and Financial Practices (the *"SBFP Rule"*).

Credit Unions and Caisses Populaires ("CUs") must achieve the desired outcomes of the practices for effective IT risk management in order to satisfy requirements in the *SBFP Rule*. This includes notifying FSRA of any material IT risk incident **as soon as is reasonable, and no later than 72 hours after determining that an IT risk incident has occurred**.

Sound IT risk management reflects the effectiveness of a CU's Board and Senior Management in administering the Credit Union's portfolio of products, activities, processes, and systems, resulting in reduced frequency and impact of IT risk events.

The Board is responsible for establishing the necessary IT strategies and governance structures, overseeing and approving the credit union's IT risk management program, as well as ensuring that there are adequate resources to carry out its IT risk management activities.[12] The Board is required to periodically review and approve an IT risk management framework and other supporting frameworks (e.g., third-party risk management framework) or similar construct according to its size, complexity, and risk profile, which will include its IT risk appetite, tolerance, and limits.[13]

[12] *Rule 2021-001 Sound Business and Financial Practices, s. 5(4) [SBFP RULE].*
[13] Ibid at s. 5(2), 5(3)(h).

Senior Management is responsible for implementing the IT risk framework (or equivalent) as approved by the board. This includes:

- developing, updating, and implementing IT related policies used to manage IT risk, including clearly-defined roles and responsibilities of management, employees, and third parties, and ensuring that they are understood by all relevant stakeholders[14]

- implementing systems and processes that allow for the effective identification, measurement, and management of IT risk[15]

- monitoring the CU's IT risk profile in relation to the board-approved risk appetite and associated limits and providing regular reporting to the board to confirm alignment[16]

Governance structures with well-defined accountabilities and responsibilities, reporting lines, and decision-making authorities support the management of IT risks. CUs must establish an organizational structure where IT risk management activities are conducted by operational management[17] (first line of defence), are reviewed and challenged by risk management[18] (second line of defence), and independent assurance is then provided by internal audit[19] (third line of defence).

Non-compliance with the requirements of this Guidance could lead to supervisory or enforcement action. This may include requiring remediation and enhanced reporting by the credit union, issuing compliance orders, and/or placing the credit union under supervision or administration in accordance with the *Credit Unions and Caisses Populaires Act, 2020* (CUCPA 2020).[20]

The management of IT risk is also a factor in assessing a Credit Union's operational risk and resilience. FSRA's operational risk and resilience Guidance includes an interpretation of the *SBFP Rule* and has Guidance related to IT risk. This Guidance and the operational risk and

---

[14] Ibid at s. 6(1)(i), s. 6(2)(iii).
[15] Ibid at s. 6(1)(i).
[16] Ibid at s. 5(3)(i)(g).
[17] Ibid at s. 15(2)(iv), s. 15(2)(v).
[18] Ibid at s. 10(9)(i)(a)-(b), s. 10(11) and s. 12(1)(i).
[19] Ibid at s. 11(2).
[20] *Credit Union and Caisses Populaires Act, 2020, S.O. 2020, C. 36, Sched 7, ss. 230 and 233 [CUCPA 2020].*

resilience Guidance should be considered together when credit unions develop their IT risk policies, processes, and procedures.

Approach

Processes and practices

FSRA's Risk Based Supervisory Framework for Credit Unions ("RBSF-CU") sets out FSRA's approach for the supervision and assessment of CUs. Its primary focus is to determine the impacts of current and potential future events, both internal and external, on the risk profiles of CUs.

FSRA uses the RBSF-CU to identify imprudent or unsafe business practices that may impact members, customers and depositors of CUs and will intervene on a timely basis if warranted. FSRA will exercise supervisory judgement and assess the most important risks posed by CUs to supervisory objectives and the extent to which CUs can identify, assess, and manage these risks as well as achieve resilience.

FSRA's supervisory activities consider whether the outcomes described below have been achieved through an assessment of a CU's IT risk management framework and the extent to which it has been implemented effectively by management through policies, processes, systems and associated controls. The characteristics referenced for each of the outcomes are indicators of effectiveness that act as a guide for FSRA's supervisory assessments and are not intended to be an exhaustive or prescriptive list.

Practice 1: Governance

Outcomes:

- IT risks are effectively governed at the CU.
- Accountability for the effective management of IT risk rests with the CU's Board of Directors.
- Responsibility for the management of IT risk is delegated appropriately within the CU.

The following are examples but not an exhaustive list of characteristics that support the achievement of these outcomes:

- The Board has approved a documented IT strategy that is aligns with the CU's overall strategy and demonstrates appropriate investment and resource allocation to safeguard the IT assets of the CU.

- The Board has approved the CU's enterprise-wide approach to IT risk management (e.g., frameworks, policies, risk appetite, tolerances, and limits).

- The Board has articulated an appropriate organizational structure and ensured that sufficient resources (both financial and non-financial) are available to effectively manage IT risk.

- The Board has approved thresholds for the escalation and reporting of IT risk, including a clear and reasonable definition of what constitutes a material IT risk incident.

Practice 2: Risk management

Outcome

- Board oversight of the CU's IT risk management activities is effective.

The following are examples but not an exhaustive list of characteristics that support the achievement of this outcome:

- Senior Management has implemented policies, processes, systems, and controls that are commensurate with its size and complexity for operational management, risk management, and internal audit to ensure that the CU operates in a manner that aligns with the Board-approved approach to IT risk management. Areas of coverage may include, but are not limited to:

    - information and records management, data storage, and maintenance

    - data classification and access

  - third party risk management
  - cloud-specific requirements
  - cybersecurity
  - project and change management

- The Board receives regular reporting on the extent to which the CU's operations are aligned with the IT risk management framework, including exposures relative to the approved risk appetite, and there are processes in place to escalate risks, issues, and events outside of the cadence of regular reporting.

- The risk management function/person(s) within the CU has developed an enterprise-wide approach to the management of IT risk, which includes the following elements:

  - The CU's Board-approved IT risk appetite, tolerances and limits articulate an enterprise-wide approach to the management of IT risk, which includes the CU's risk appetite.

  - Policies and procedures which enable the CU to manage its IT risks:

    - **Identify and measure** – Take steps on a recurring basis to effectively understand, analyze, and assess vulnerabilities to IT risk.

    - **Mitigate** – Determine appropriate steps to protect against identified threats, establish controls (preventative and detective) and security measures, and transfer risk (e.g., through insurance) when appropriate.

    - **Monitor** – Develop and implement processes to monitor risks/threats on a regular basis and provide adequate reporting to the Board and Senior Management.

    - **Respond** – Develop processes which allows the CU to respond in an effective and timely manner in the event of an incident.

- A process to review and respond to recommendations from auditors or other external third parties.

- A process to report to the Board regularly and consistently on the CU's performance against its IT risk appetite.

- Senior Management has ensured that adequate training is provided to promote enterprise-wide awareness of IT risk.

Practice 3: Data management

Outcomes

- Confidential data overseen by regulated entities and individuals is secure.

- Data is appropriately handled and stored in a manner that maintains data quality, integrity, availability, confidentiality, and privacy.

The following are examples but not an exhaustive list of characteristics that support the achievement of these outcomes:

The CU:

- Has policies and procedures to identify and classify (according to type of information) the CU's data.

- Has policies, procedures, and controls to ensure authorized access to data sources and environment (e.g., multi-factor authentication, segregation of duties, and principles of least privilege).

- Has procedures (i.e., discovery scans) for identifying data risk management incidents.

- Conducts regular testing of its data management controls and develops a process for addressing deficiencies and implementing recommendations.

- Has adequate and robust data governance processes and procedures to ensure:

- data is fit-for-purpose
- data is being collected and stored in a transparent manner
- data quality and integrity is maintained
- data has clearly defined ownership

- Has a process to ensure compliance with relevant legislative requirements in addition to the sector statutes (e.g., PIPEDA) and to report on material compliance breaches to Senior Management, the Board, FSRA and other applicable regulators.

Practice 4: Outsourcing

Outcomes:

- The Board clearly retains risk management accountability when functions or processes have been outsourced.

IT risks for outsourced and co-sourced activities, functions, and services are properly identified, assessed, and managed.

The following are examples but not an exhaustive list of characteristics that support the achievement of these outcomes:

The CU:

- Has criteria for the evaluation and selection of third-party providers (“TPPs”) as well as a process to assess the ongoing performance of TPP IT controls.
- Performs a third-party risk assessment prior to contracting/procurement.
- Has a methodology to assess the risk level and criticality of third-party arrangements/TPPs.

- Includes the rights to audit and access information in its third-party contracts.
- Has a process or mechanism to confirm a TPP's responsibility to comply with the CU's IT risk management policies and procedures.
- Has a process or mechanism to periodically test a TPP's compliance with the CU's IT risk management policies and procedures.
- Has cloud-specific requirements, if applicable, which align with the CU's broader IT strategy and risk appetite.
- Assesses risk of incidents and data leakages when outsourcing to cloud computing service providers are utilized.
- Identifies, investigates, escalates, tracks, and ensures remediation of the incidents at its TPPs.
- As appropriate, has established an exit plan (if appropriate) in the event the third party experiences a major, negative event (e.g., bankruptcy, catastrophic outage or loss of key individuals).

Practice 5: Incident preparedness

Outcomes:

- There is a consistent understanding of roles and responsibilities in the event of an IT incident.
- The impact and likelihood of IT risk incidents is minimized.
- Regulated entities and individuals learn from previous incidents to better prevent future incidents.

The following are examples but not an exhaustive list of characteristics that support the achievement of these outcomes:

The CU:

- Has a documented process within IT risk policies to detect, log, manage, resolve, recover, monitor and report on IT incidents.
- Defines and documents roles and responsibilities of relevant internal and external parties to support effective incident response.
- Performs periodic testing of incident management processes, including table-top exercises, and includes third parties in these exercises as appropriate.
- Conducts periodic independent reviews of incident management process and controls to ensure their effectiveness.
- Prioritizes incidents based on their impacts on the entity generally and IT services specifically.
- Has a process for escalating incidents internally to the appropriate level of authority (e.g., Senior Management or the Board) and developing internal and external communications actions, as applicable.
- Has processes for ensuring issues are resolved in a timely manner and that post-incident reviews and root cause analyses are conducted.
- Adopts the relevant recognized industry standards on incident preparedness.
- Reports to Senior Management and the Board on material IT risk incidents.

Practice 6: Continuity and resilience

Outcome:

- CUs are operationally resilient and services remain available in the event of a crisis.

The following are examples but not an exhaustive list of characteristics that support the achievement of this outcome:

The CU:

- Maintains an inventory of all IT assets that support business processes or functions.
- Assigns a classification (e.g., risk level, criticality) to IT assets and manage and monitor assets throughout their life cycle.
- Continuously monitors the currency of software and hardware assets used to support business processes.
- Proactively mitigates and manage risks stemming from unpatched, outdated or unsupported assets, and replace or upgrade assets before maintenance expires or end-of-life is reached.
- Has service level agreements between key stakeholders internally as well as with third-party providers.
- Has project management and change management policies and procedures, which ensure that project risks are appropriately managed and that changes are effectively implemented in a timely manner with minimal disruptions to service delivery.
- Has a Disaster Recovery Plan (“DRP”), which aligns with the entity’s broader Business Continuity Plan (“BCP”) and articulates how the CU will continue to deliver services if critical services are disrupted. The DRP, among other things:
    - Establishes the accountabilities and responsibilities within DRP for the availability and recovery of IT services including recovery actions.
    - Tests the disaster recovery scenarios to promote learning, continuous improvement and IT resilience.
    - Reviews critical third party's DRP practices and test results.

Practice 7: Notification of material IT risk incidents

Outcomes:

- CUs have a consistent understanding of what constitutes a material IT risk incidents.
- Through notification, regulated entities and individuals assist FSRA in identifying high risk areas in a timely manner in order to help prevent future incidents.

The following are examples but not an exhaustive list of characteristics that support the achievement of these outcomes:

The CU:

- Has a process and clear thresholds for assessing what constitutes a material IT risk.
- Has documented processes and assigned responsibility for notifying FSRA in the event of a material IT risk incident.
- Systematically learns and improves its risk mitigation efforts following a material IT risk incident.

Mortgage Brokers, Mortgage Agents, Mortgage Administrators and Mortgage Brokerages

Information/Approach

The Mortgage Broker Regulators' Council of Canada ("MBRCC")'s 'Principles for Cybersecurity Preparedness for the Mortgage Brokering Sector' (Principles for Cybersecurity Preparedness)[21] outline outcomes that regulated entities and individuals are expected to achieve to ensure "cybersecurity preparedness". FSRA has released Information Guidance[22] that adopts the MBRCC Principles for Cybersecurity Preparedness into FSRA's regulatory framework. It also established FSRA's 'Market Conduct Protocol for Cybersecurity' for mortgage brokerages and administrators to follow in the event of a cybersecurity incident.

Under Principle 8 of the MBRCC's Code of Conduct for the Mortgage Brokering Sector (Code of Conduct),[23] "regulated persons and entities must protect their clients' information. They must use and disclose it only for purposes for which the client has given consent or as compelled by law." FSRA has adopted this Code into its supervision framework for the mortgage broker sector.

MBRCC's 'Code of Conduct' and 'Principles for Cybersecurity Preparedness', as well as FSRA's corresponding Guidance incorporating these into FSRA's regulatory framework, are consistent with the practices for effective IT risk management and desired outcomes of this Guidance. Following this Guidance will satisfy the MBRCC Guidance and in areas of inconsistency this Guidance will take priority.

FSRA can enforce against non-compliance with this Guidance that corresponds to requirements under the *Mortgage Brokerages, Lenders and Administrators Act, 2006* and its regulations.

---

21 Mortgage Broker Regulator's Council of Canada (MBRCC), Principles for Cybersecurity Preparedness.
22 Mortgage Broker Regulators' Council of Canada Principles for Cybersecurity Preparedness for the Mortgage Brokering Sector.
23 Mortgage Broker Regulators' Council of Canada (MBRCC), Code of Conduct for the Mortgage Brokering Sector.

Existing requirements that are applicable to the practices for effective IT risk management and desired outcomes of this Guidance include the duty to establish policies and procedures for both mortgage administrators[24] and mortgage brokerages[25], and the requirement to take precautions to secure records for administrators[26] and brokerages.[27]

This Guidance applies to mortgage brokers, agents, brokerages and administrators. FSRA considers mortgage administrators and mortgage brokerages to be ultimately responsible for ensuring that IT risks are being effectively managed by their licensed representatives and staff or any function outsourced to a third party.

Failure to comply with the Practices for effective IT risk management and their desired outcomes may impact the suitability for both licence issuance and licence renewal.

[24] O. Reg. 189/08, s. 25 (1).
[25] O. Reg. 188/08, s. 40 (1).
[26] O. Reg. 189/08, s. 30-31.
[27] O. Reg. 188/08, s. 47-48.

Non-Ontario incorporated insurance companies, Insurance Agents, Insurance Adjusters, Adjuster Firms, and Insurance Agencies

Approach

This section is applicable to federally incorporated insurance companies, and insurance companies incorporated in other provinces, that are licensed in Ontario. It also applies to insurance agents, insurance adjusters, adjuster firms, and insurance agencies.

See this section of the Guidance for Ontario incorporated insurance companies and reciprocals.

Existing Guidance from other regulators

Insurance companies that are incorporated outside of Ontario may be subject to similar Guidance by another regulator, such as the Office of the Superintendent of Financial Institutions ("OSFI")'s 'Technology and Cyber Risk Management' guideline.[28] The Practices for effective IT risk management and desired outcomes of this Guidance are aligned with OSFI's guideline and similar Guidance by other provincial regulators.[29]

Alignment with other existing Guidance

The Practices for effective IT risk management and their desired outcomes are consistent with Guidance issued by FSRA, and by the Canadian Council of Insurance Regulators ("CCIR") and the Canadian Insurance Services Regulatory Organizations ("CISRO"). This Guidance elaborates

[28] Office of the Superintendent of Financial Institutions, Technology and Cyber Risk Management.
[29] This includes the BC Financial Services Authority's 'Information Security Guideline' and the Autorité des marchés financiers' 'Guideline on Information and Communications Technology Risk Management'.

on Guidance issued by CCIR and CISRO and should not be interpreted as limiting these pieces of Guidance. In areas where there are inconsistencies between CCIR and CISRO Guidance, regulated entities and individuals are expected to follow the FSRA Guidance.

Guidance	Relevant expectations from Guidance
CCIR and CISRO - Conduct of Insurance Business and Fair Treatment of Customers' ("FTC Guidance")	Insurers and intermediaries have safeguards in place and have adopted policies and procedures relating to **the protection of personal information that** "ensure compliance with legislation relating to privacy protection and to reflect best practices in this area." FSRA's has adopted this Guidance[30] to supervise the fair treatment of customers.
CISRO Principles of Conduct for Insurance Intermediaries[31] ("CISRO Principles")	For insurance intermediaries, like agents, adjusters and corporate insurance agencies, the Guidance[32] contains the principle of 'Protection of Personal and Confidential Information'. FSRA released Guidance for consultation[33] for the adoption of the CISRO Principles into its regulatory framework, which outlines FSRA's supervisory and enforcement approach.
FSRA information Guidance – Operational risk management	Only applicable for insurance companies that offer automobile insurance. This Guidance, including the Practices for effective IT risk management and their desired outcomes are consistent and intended to elaborate on FSRA's ORM Guidance. The ORM Guidance outlines

30 Fair Treatment of Customers in Insurance.
31 Canadian Insurance Services Regulatory Organizations (CISRO), Principles of Conduct for Intermediaries.
32 Ibid.
33 Proposed Principles of Conduct for Insurance Intermediaries.

framework in rating and underwriting of automobile ("ORM Guidance")[34]	foundational and sound practices for applying three lines of defence to assist insurers in meeting existing obligations in protection of personal information (practices 1 and 2); for having data governance in place (practice 3); and for insurers to ensure oversight of, and hold accountability for consumer outcomes from, the use of third-party data or services (practice 4).

Supervisory approach

FSRA may conduct thematic reviews of Ontario licensed insurance entities and individuals on management of IT risks based on this Guidance. Where possible, FSRA will coordinate reviews with other CCIR regulators.

FSRA may take supervisory action or enforcement action when non-compliance with Guidance corresponds to existing requirements under the *Insurance Act* and its regulations. Such measures shall include remedies ranging from education and remediation to regulatory discipline and intervention. Failure to comply with this Guidance may impact the suitability of an individual licensee at renewal.

Although this Guidance also applies to insurance agents, insurance adjusters, adjusters, adjusting firms, and insurance agencies, FSRA considers insurers to be ultimately responsible for the fair treatment of customers. This includes ensuring that IT risks are being effectively managed through all of its distribution channels and outsourced functions related to the conduct of insurance business. This responsibility of insurers does not absolve intermediaries of their own responsibilities for which they are accountable.

[34] Operational risk management framework in rating and underwriting of automobile insurance.

Ontario-incorporated Insurance Companies and Reciprocals

Interpretation

FSRA's Interpretation of IT risk management requirements under the *Insurance Act.*

Ontario-incorporated Insurance Companies and Reciprocals ("Insurers") must achieve the desired outcomes listed for each of the practices for effective IT risk management in order to satisfy the requirements under the *Insurance Act*. Subsection 437(3) of the *Insurance Act* requires that every insurer "institute and record procedures to be followed in the handling and safeguarding of its investments and shall, at all times, ensure strict compliance with those procedures".

This includes notifying FSRA of any material IT risk incident as soon as is reasonable, but no later than 72 hours after determining that an IT risk incident has occurred.

Insurers that fail to demonstrate compliance with this Guidance may face supervisory or enforcement action.[35]

[35] *Insurance Act*, R.S.O. 1990, c. I.8, ss. 441 and 447 [*Insurance Act*].

Approach

Processes and practices

FSRA's Risk Based Supervisory Framework for Ontario-incorporated Insurance Companies and Reciprocals Guidance ("RBSF-I") sets out FSRA's approach for supervision and assessment of Insurers. Its primary focus is to determine the impacts of current and potential future events, both internal and external, on the risk profile of each Insurer.[36]

FSRA uses the RBSF-I to identify imprudent or unsafe business practices and/or misconduct impacting policyholders, beneficiaries, consumers, and stakeholders (including members and subscribers) and will intervene on a timely basis if warranted. FSRA will exercise supervisory judgement and assess the most important risks posed by Insurers to supervisory objectives and the extent to which Insurers can identify, assess, and manage these risks and achieve resilience.

FSRA's supervisory activities consider whether the outcomes described below have been achieved through assessment of an insurer's IT risk management framework and the extent to which it has been implemented effectively by management through policies, processes, systems and associated controls. The characteristics referenced for each of the outcomes are indicators of effectiveness that act as a guide for FSRA's supervisory assessments and are not intended to be an exhaustive or prescriptive list.

Practice 1: Governance

Outcomes:

- IT risks are effectively governed at the Insurer.
- Accountability for the effective management of IT risk rests with the Insurer's Board of Directors.

[36] Risk Based Supervisory Framework for Ontario-incorporated Insurance Companies and Reciprocals.

- Responsibility for the management of IT risk is delegated appropriately within the Insurer.

The following are examples but not an exhaustive list of characteristics that support the achievement of these outcomes:

- The Board has approved a documented IT strategy that is aligns with the Insurer's overall strategy and demonstrates appropriate investment and resource allocation to safeguard the IT assets of the Insurer.

- The Board has approved the Insurer's enterprise-wide approach to IT risk management (e.g., frameworks, policies, and risk appetite, tolerances, and limits).

- The Board has articulated an appropriate organizational structure and ensured that sufficient resources (both financial and non-financial) are available to effectively manage IT risk.

- The Board has approved thresholds for the escalation and reporting of IT risk, including a clear and reasonable definition of what constitutes a material IT risk incident.

Practice 2: Risk management

Outcome

- Board oversight of the insurer's IT risk management activities is effective.

The following are examples but not an exhaustive list of characteristics that support the achievement of this outcome:

- Senior Management has implemented policies, processes, systems, and controls that are commensurate with its size and complexity for operational management, compliance, risk management, and internal audit to ensure that the Insurer operates in a manner that aligns with the board-approved approach to IT risk management. Areas of coverage may include, but are not limited to:

- information and records management, data storage, and maintenance
- data classification and access
- third party risk management
- cloud-specific requirements
- cybersecurity
- project and change management

- The Board receives regular reporting on the extent to which the Insurer's operations are aligned with the IT risk management framework, including exposures relative to the approved risk appetite, and there are processes in place to escalate risks, issues, and events outside of the cadence of regular reporting.

- The risk management function/person(s) within the Insurer has developed an enterprise-wide approach to the management of IT risk, which includes but is not limited to the following elements:
  - A Board-approved and clearly articulated IT risk appetite, tolerances, and limits.
  - Policies and procedures which enable the Insurer to manage its IT risks are sufficiently comprehensive to provide Guidance on approach to:
    - **Identify and measure** – Identifying and assessing risks and vulnerabilities.
    - **Mitigate** – Determining the appropriate steps to protect against identified threats, establish controls (preventative and detective) and security measures, and transfer risk (e.g., through insurance) when appropriate.
    - **Monitor** – Developing and implementing processes to monitor risks/threats on a regular basis and provide adequate reporting to the board and Senior Management.

        - **Respond** – Developing processes which allows the Insurer to respond in an effective and timely manner in the event of an incident.

    - A process to review and respond to recommendations from auditors or other external third parties.

    - A process to report to the Board regularly and consistently on the insurer's performance against its IT risk appetite.

- Senior Management has ensured that adequate training is provided to promote enterprise-wide awareness of IT risk.

Practice 3: Data management

Outcomes

- Confidential data overseen by the Insurer is secure.

- Data is appropriately handled and stored in a manner that maintains data quality, integrity, availability, confidentiality, and privacy.

The following are examples but not an exhaustive list of characteristics that support the achievement of these outcomes:

The Insurer:

- Has policies and procedures to identify and classify the insurer's data.

- Has policies, procedures, and controls to ensure authorized access to data sources and environment (e.g., multi-factor authentication, segregation of duties, principles of least privilege).

- Has procedures for identifying when data is mishandled.

- Conducts regular testing of its data management controls and develops a process for addressing deficiencies.

- Has adequate and robust data governance processes and procedures to ensure:

    - data is fit-for-purpose

    - data is being collected and stored in a transparent manner

    - data quality and integrity is maintained

    - data has clearly defined ownership.

- Has a process to ensure compliance with relevant legislative requirements in addition to the sector statutes (e.g., PIPEDA) and to report on material compliance breaches to Senior Management, the board, FSRA and other applicable regulators.

Practice 4: Outsourcing

Outcomes:

- The Board clearly retains accountability when functions or processes have been outsourced.

- IT risks for outsourced and co-sourced activities, functions, and services are adequately identified, assessed, and managed.

The following are examples but not an exhaustive list of characteristics that support the achievement of these outcomes:

The Insurer:

- Has criteria for the evaluation and selection of third-party providers (“TPPs”) as well as a process to assess the ongoing performance of TPP IT controls.

- Performs a third-party risk assessment prior to contracting/procurement.
- Has a methodology to assess the risk level and criticality of third-party arrangements/TPPs.
- Includes the rights to audit and access information in its third-party contracts.
- Has a process or mechanism to confirm a TPP's responsibility to comply with the insurer's IT risk management policies and procedures.
- Has a process or mechanism to periodically test a TPP's compliance with the insurer's IT risk management policies and procedures.
- Has cloud-specific requirements, if applicable, which align with the insurer's broader IT strategy and risk appetite.
- Assesses risk of incidents and data leakages when outsourcing to cloud computing service providers are utilized.
- Has ensured its TPPs have an established process to manage IT risk incidents, including notification of incidents to the Insurer.
- As appropriate, has established an exit plan, as appropriate, in the event the TPP experiences a major, negative event (e.g., bankruptcy, catastrophic outage, or loss of key individuals).

Practice 5: Incident preparedness

Outcomes:

- There is a consistent understanding of roles and responsibilities in the event of an IT risk incident.
- The impact and likelihood of IT risk incidents is minimized.

- Insurers learn from previous incidents to better prevent future incidents.

The following are examples but not an exhaustive list of characteristics that support the achievement of these outcomes:

The Insurer:

- Has a documented process within its IT risk policies to detect, log, manage, resolve, recover, monitor and report on IT incidents.

- Defines and documents roles and responsibilities of relevant internal and external stakeholders to support effective incident response.

- Performs periodic testing of incident management processes, including table-top exercises, and includes third parties is these exercises as appropriate.

- Conducts periodic independent reviews of incident management process and controls to ensure their ongoing effectiveness.

- Prioritizes incidents based on their impacts on the entity generally and IT services specifically.

- Has a process for escalating incidents internally to the appropriate level of authority (e.g., Senior Management or the board) and developing internal and external communication actions, as applicable.

- Has processes for ensuring issues are resolved in a timely manner and that post-incident reviews and root cause analyses are conducted.

- Refers to the relevant recognized industry standards to inform its incident management program.

- Reports to Senior Management and the board on material IT risk incidents.

Practice 6: Continuity and resilience

Outcome:

- Insurers are operationally resilient and services remain available in the event of a crisis.

The following are examples but not an exhaustive list of characteristics that support the achievement of this outcome:

The Insurer:

- Maintains an inventory of all IT assets that support business processes or functions.
- Assigns a classification (e.g., risk level, criticality) to IT assets and manage and monitor assets throughout their life cycle.
- Continuously monitors the currency of software and hardware assets used to support business processes.
- Proactively mitigates and manage risks stemming from unpatched, outdated or unsupported assets, and replace or upgrade assets before maintenance expires or end-of-life is reached.
- Has service level agreements between key stakeholders internally as well as with third-party providers.
- Has project management and change management policies and procedures, which ensure that project risks are appropriately managed and that changes are effectively implemented in a timely manner with minimal disruptions to service delivery.
- Has a disaster recovery plan (“DRP”), which aligns with the entity’s broader business continuity plan (“BCP”) and articulates how the Insurer will continue to deliver services if critical services are disrupted. The DRP, among other things:
    - Establishes the accountabilities and responsibilities within DRP for the availability and recovery of IT services including recovery actions.

- Tests the disaster recovery scenarios to promote learning, continuous improvement and IT resilience.

- Reviews critical third party's DRP practices and test results.

Practice 7: Notification of material IT risk incidents

Outcomes:

- The Insurers has a consistent understanding of what constitutes a material IT risk incident.

- Through notification, regulated entities and individuals assist FSRA in identifying high risk areas in a timely manner in order to help prevent future incidents.

The following are examples but not an exhaustive list of characteristics that support the achievement of these outcomes:

The Insurer:

- Has a process and clear thresholds for assessing what constitutes a material IT risk.

- Has documented processes and assigned responsibility for notifying FSRA in the event of a material IT risk incident.

- Systematically learns and improves its risk mitigation efforts following a material IT risk incident.

Pension Plan Administrators – Interpretation and Approach

Interpretation

FSRA's Interpretation of the *Pensions Benefits Act* ("*PBA*") relating to IT risk.

Pension plan administrators are subject to fiduciary duties under common law as well as prescribed minimum standards in the *PBA*.

The *PBA* requires administrators to act with the care, diligence and skill that a person of ordinary prudence would exercise in dealing with the property of another person. They must also use all relevant knowledge and skill that they possess or, by reason of their profession, business or calling, ought to possess.[37]

As is set out in the *PBA*, administrators "shall not send a document in electronic form if the document contains personal information or any prescribed information, unless the administrator sends the document by way of a secure information system that,

(a) requires the intended recipient to identify themselves prior to accessing the document

(b) complies with any other prescribed conditions, requirements, limitations or prohibitions, including any requirements concerning methods of identification for the purpose of clause (a)[38]

In order to adequately protect plan members' rights and benefits, and to effectively administer the pension plan, administrators must consider and mitigate IT risks.

---

[37] *Pension Benefits Act*, R.S.O. 1990, c. P.8, s. 22 (1) [PBA].
[38] Ibid at 30.1 (2).

Approach

FSRA has issued 'Pension Plan Administrator Roles and Responsibilities Guidance', which details for pension plan administrators their roles and responsibilities.[39] The Pension Plan Administrator roles and responsibilities Guidance notes that administrators are responsible for implementing processes to ensure that plan risks are understood and addressed. As a risk-based regulator, FSRA may take into account IT risks in its assessment of potential risks impacting pension plans.

As part of this process, FSRA would assess whether administrators can demonstrate:

- That they have familiarized themselves with industry accepted practices for plan governance, including the Canadian Association of Pension Supervisory Authorities ("CAPSA") guideline on Pension Plan governance[40] and other CAPSA guidelines as applicable.

- That they have considered the practices for effective IT risk management and their desired outcomes in this Guidance as supporting their consideration of risk management in their plan, in accordance to the size and nature of the plan and any other relevant factors.

This Guidance, including the practices for effective IT risk management, the IT Risk Incident Notification Form and the protocol for IT risk incidents are consistent with the CAPSA guideline on cyber risk for Pension Plans. Following this Guidance will satisfy the CAPSA guideline and in areas of inconsistency this Guidance will take priority.

---

[39] See Pension Plan Administrator responsibilities at Pension Plan Administrator Roles and Responsibilities.
[40] See CAPSA guideline 4. Pension Plan Governance Guideline at Guideline No. 4: Pension Plan Governance Guideline, CAPSA/ACOR.

Effective date and future review

This Guidance is effective **April 1, 2024** and will be reviewed no later than **June 2028.**

About this Guidance

This document is consistent with FSRA's Guidance framework.

As Information Guidance, it describes FSRA's views on certain topics without creating new compliance obligations for regulated persons.

As Interpretation Guidance, it describes FSRA's view of requirements under its legislative mandate (i.e., legislation, regulations and rules) so that non-compliance can lead to enforcement or supervisory action.

As Approach Guidance, it describes FSRA's internal principles, processes and practices for supervisory action and application of Chief Executive Officer discretion. Approach Guidance may refer to compliance obligations but does not in and of itself create a compliance obligation.