FSRA
Financial Services Regulatory Authority of Ontario

Guidance

☒ Interpretation | ☒ Approach | ☒ Information | ☐ Decision

Effective Date: TBD
Identifier: No. GR0016INT

Proposed Information Technology ("IT") Risk Management

This guidance applies to all FSRA regulated entities and individuals. Table 1 can be used to navigate the guidance to determine which sections are applicable to a particular regulated entity or individual.

Table 1: Guidance outlined by Regulated Entity or Individual

Regulated Entity (alphabetical order)	Applicable Sections	Sector-Specific Section outline
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

Regulated Entity (alphabetical order)	Applicable Sections	Sector-Specific Section outline
Credit Unions	• All Sectors Section • Sector-Specific Interpretation/Approach for Credit Unions	• FSRA's interpretation of IT risk management requirements under the Sound Business and Financial Practices Rule and the CUCPA • 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

Regulated Entity (alphabetical order)	Applicable Sections	Sector-Specific Section outline
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

Regulated Entity (alphabetical order)	Applicable Sections	Sector-Specific Section outline
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

All sectors

Purpose and scope

This guidance communicates:

- 'Practices[1] for Effective IT Risk Management'
- A process for regulated entities and individuals to notify FSRA[2] in the event of a material IT risk incident.
- 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.

This guidance includes Information, Approach, and Interpretation sections:

- Information Guidance – Provides information on certain topics such as practices without creating any compliance obligations for regulated entities and persons.
- 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.
- Interpretation Guidance – Sets out FSRA's requirements under its legislative mandate (i.e. legislation, regulation and rules). Non-compliance can lead to enforcement or supervisory action.

Outline

The guidance is segmented in two main sections:

- **All Sectors** – Interpretation/Information/Approach guidance 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 regulated entities or individuals in a specific sector

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 additional sector-specific guidance. FSRA has made this determination based on the risk posed to consumers, 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 business, operations and stability of FSRA's regulated sectors, and can result in negative impacts[3] to consumers[4]. This can disrupt confidence in the financial services and pension sectors.

FSRA's focus on IT risk is consistent with FSRA's statutory objects to:[5]

- 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

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")[6].

Failure to comply with such requirements is likely to result in consumer harm. 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; or 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 regulated entities and individuals to ensure 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:
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 later 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 and the board of directors.

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

Desired Outcomes:

- Regulated entities and individuals have policies, procedures and controls in place to adequately protect, detect, respond, recover, and learn from IT risk incidents.
- Regulated entities and individuals that rely heavily on technology to operate and provide products and services to the public articulate their IT risks appetite and tolerance.[7]

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 handled and stored properly 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[8]

Desired Outcomes:

- IT risks for outsourced and co-sourced functions 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.

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 of IT risk incidents is minimalized.
- 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.
- 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 possible 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 the direct notification by the regulated entity or individual, or through other channels (e.g., complaint, media report, etc.), it will determine whether to activate **FSRA's Protocol for IT Risk Incidents**. In some instances, FSRA may determine that activation of the Protocol for IT Risk Incidents is not warranted.

When reporting an IT risk incident, regulated entities or individuals can notify FSRA at ITriskinbox@fsrao.ca using the 'FSRA IT Risk Incident Report'. 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 subsequently notifying FSRA.

For the **mortgage brokering sector,** this guidance, including the Practices for Effective IT Risk Management, the IT Risk Incident Report and the Protocol for IT Risk Incidents are consistent with 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.

Material IT risk incident

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 its consumers.

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

- results in significant operational disruptions to business systems and functions

- significantly disrupts the consumers' 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
- could potentially 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

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.

See Appendix 1 for examples of material IT risk incidents.

Activation of FSRA's protocol for IT risk incidents

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

As FSRA becomes aware of an IT risk incident, either through the direct notification by the regulated entity or individual, or through other channels (e.g., complaint, media report…etc.) it

will determine whether to activate FSRA's Protocol for IT Risk Incidents. In some instances, FSRA may determine that activation of the Protocol for IT Risk Incidents is not warranted.

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

- a complete understanding and knowledge of the extent of the incident, including if any confidential data has been breached and what information was accessed
- 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 consumer harm
- a complete understanding and knowledge of the safeguards that have been put in place to ensure the regulated entity or individual is protected from similar incidents

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

Protocol for IT risk incidents - Three phase protocol

Incident response typically proceeds in phases similar to the pattern below:

Phase 1: Receive a notification from the regulated entity or individual detailing the immediate 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 IT Risk Protocol 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, services and consumers. 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 level / frequency of involvement with a regulated entity or individual, and its determination to activate the IT Risk Protocol, 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
- 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[9], 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

FSRA also reviews if credentialing bodies 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[10].

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.

Credit Unions – Interpretation and Approach

Interpretation

Credit Unions – FSRA's interpretation of IT risk management requirements under the Sound Business and Financial Practices Rule (“SBFP Rule")

Credit unions 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 within 48 hours.

Sound IT risk management reflects the effectiveness of a credit union'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.[11] The Board is required to periodically review and approve an IT Risk Management Framework (IRMF) and 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.[12]

Senior Management is responsible for:

- developing, updating, and implementing the IT related policies, processes, and systems used to manage IT risk effectively at all decision levels and ensuring that it is understood among staff, third parties, and other relevant stakeholders[13]
- establishing and governing the respective roles and responsibilities necessary to effectively identify, assess, manage, and oversee IT risk[14]
- measuring the credit union's IT risk profile in relation to the Board-approved risk appetite and tolerance and presenting to the Board to confirm alignment[15]

Governance structures with well-defined accountabilities and responsibilities, reporting lines, and decision-making authorities support the management of IT risks. Credit unions must establish an organizational structure where IT risk management activities are conducted by IT Operational

Management[16] (first line of defence), are reviewed and challenged by IT Risk Management[17] (second line of defence), and independent assurance is then provided by Internal Audit[18] (third line of defence), facilitating effective IT governance, oversight and risk management.

Non-compliance with this guidance could lead to supervisory or enforcement action. This may include requiring remediation and enhanced reporting by the credit union, the issuance of a compliance order or placing the credit union under supervision or administration in accordance with the *Credit Unions and Caisses Populaires Act, 2020* (CUCPA 2020)[19].

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

Approach

FSRA takes a risk-based approach to the supervision of IT risk. FSRA's supervisory activities consider all the outcomes of the Practices for Effective IT Risk Management, in its assessments and exercises appropriate supervisory judgment when evaluating the policies, processes, and practices established by the regulated entity to effectively manage IT risk.

FSRA's ‘Risk Based Supervisory Framework' (“RBSF") Guidance[20] sets out FSRA's processes and practices for supervising credit unions and assessing their risk. Its primary focus is to determine the impacts of current and potential future events, both internal and external, on the risk profiles of credit unions.

FSRA uses the RBSF to assess risk and identify imprudent or unsafe business practices and/or misconduct which may impact consumers, in order to be able to intervene on a timely basis. IT risk is a factor FSRA considers in developing the overall risk assessment of credit unions under the RBSF. Credit unions will be assessed in accordance with the RBSF to determine their Overall Risk Rating (ORR).

The management of IT risk is also a factor in assessing a credit union's operational risk and resilience, as described in the ‘Operational Risk and Resilience Guidance' (link when published).

FSRA has the ability to make inquiries, conduct supervisory assessments and collect information from credit unions relating to IT risk. FSRA will take into consideration whether credit unions have achieved the desired outcomes outlined in this guidance, including notifying FSRA within 48 hours in the event of a material IT risk incident, in assessing whether an entity has satisfied its requirements outlined under the Interpretation section.

FSRA will reference the criteria articulated in this Approach when assessing the application of the Practices for Effective IT Risk Management and their desired outcomes. The criteria act as a guide to FSRA's supervisory assessments and are not intended to be an exhaustive or prescriptive list. FSRA will take the credit union's size, complexity, and risk profile into consideration in its assessment.

Criteria used to assess practice 1: Governance

- The board has approved the regulated entity's documented approach to IT risk management (e.g., frameworks, policies, risk appetite, tolerances, and limits).
- Senior management has ensured that a board-approved IT strategy is documented and implemented, and that it aligns with the regulated entity's overall strategy and demonstrates appropriate investment and resource allocation to safeguard the IT assets of the credit union.
- The board has ensured an appropriate organizational structure is established and resources (both people and financial) are available to effectively manage IT risk.
- Senior management has ensured that adequate training is provided to promote enterprise-wide awareness of IT risk.
- The board receives appropriate and timely information (e.g., audit reports, quarterly reporting, incident reporting) to effectively oversee and assess the management of IT risk by the credit union.

Criteria used to assess practice 2: Risk management

- Senior management is responsible for ensuring the establishment of an independent risk oversight function or person(s) to ensure the operations of the credit union operate in compliance with the board-approved approach to IT risk management.
- Senior management, with the appropriate subject-matter expertise and IT risk knowledge, is accountable for the regulated entity's IT operations and for implementing the board-approved approach to IT risk management.

- The risk oversight function/person(s) within the credit union has developed an enterprise-wide approach to the management of IT risk, which includes the following elements:
    - The credit union's board-approved IT risk appetite, tolerances and limits.
    - Policies and procedures which enable the regulated entity to:
        - 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 when appropriate (e.g., through insurance).
        - Monitor – develop and implement processes to monitor threats on a regular basis and provide adequate reporting to the board or senior management.
        - Respond – develop processes which allow entities to respond in an effective and timely manner if an incident occurs.
    - A process to review and respond to recommendations from auditors or other external examiners.
    - A process to report to the board regularly and consistently on the credit union's performance against its IT risk appetite.

The credit union has established IT risk management policies and procedures that commensurate with the entity's size, complexity, and risk profile, including but 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.

Criteria used to assess practice 3: Data management

The credit union:

- Has policies and procedures to identify and classify (according to type of information) the credit union'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 for monitoring for data risk management incidents (e.g., discovery scans).
- Conducts regular testing of data management controls and develop 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.

Criteria used to assess practice 4: Outsourcing

The credit union:

- Has criteria for the evaluation and selection of vendors as well as a process to assess the ongoing performance of vendor IT controls.
- Performs a third-party risk assessment prior to contracting/procurement.
- Assesses third-party arrangements/third-party partners (“TPPs") for risk levels and criticality.

- Includes the rights to audit and access information in its third-party contracts.
- Has a process or mechanism (e.g., attestation) to ensure vendor accountability for and compliance with the regulated entity's IT risk management policies and procedures.
- Has a process for classifying critical vendors as part of the credit union's broader technology continuity and resiliency plan (see Practice 6).
- Has cloud-specific requirements, which align with the credit union's broader IT strategy and risk appetite.
- Assesses risk of incidents and data leakages when outsourcing to cloud computing service providers (“CSPs") are utilized.
- Identifies, investigates, escalates, tracks, and ensures remediation of the incidents at its TPPs.
- Established an exit plan in the event the third party experiences a major, negative event (e.g., bankruptcy, catastrophic outage or loss of key individuals).

Criteria used to assess practice 5: Incident preparedness

The credit union:

- Has a process 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 with third parties.
- 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 early warning indicators and identify areas of IT vulnerability and triggers of system disruption.

- Conducts regular vulnerability assessments of its IT assets at network, systems, and applications levels. Vulnerabilities and threats are assessed and ranked according to the severity of the threats.
- 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.
- Performs periodic testing and exercises (e.g., tabletop exercises) to assess incident response plans and capabilities, including with TPPs.
- Has processes for ensuring issues are resolved in a timely manner and that post-incident reviews and root cause analyses are conducted.
- Identifies current or emerging threats proactively, using threat assessments to evaluate threats and assess IT risk.
- Adopts recognized industry standards on incident preparedness.
- Has developed and implemented an IT risk policy, which incorporates a detect, log, manage, resolve, recover, monitor and report approach.
- Regularly and consistently reports to senior management and the board on material IT risk incidents.

Criteria used to assess practice 6: Continuity and resiliency

The credit union:

- Maintains an inventory of all IT assets that support business processes or functions.
- Assigns a classification (e.g., risk profile, criticality to the entity) 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 internally as well as with third-party providers.

- Has project management and change management policies and procedures, which ensure the timely completion of IT projects and limit 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 entity will continue to deliver services if critical services are disrupted:
    - 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.

Criteria used to assess practice 7: Notification of material IT risk incidents

The credit union:

- Has a process for assessing what constitutes a material IT risk.
- Notifies FSRA in the event of all material IT risks.
- 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. 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.

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 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 contains the principle of ‘Protection of Personal and Confidential Information'.

Guidance	Relevant expectations from guidance
	FSRA released guidance for consultation[32] 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 framework in rating and underwriting of automobile ("ORM Guidance")[33]	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 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 ensuring that IT risks are being effectively managed through all of its distribution channels and outsourced functions.

Ontario-Incorporated Insurance Companies and Reciprocals – Interpretation and Approach

Interpretation

Ontario-Incorporated Insurance Companies and Reciprocals – FSRA's Interpretation of the *Insurance Act* relating to IT risk

This section outlines FSRA's interpretation of the *Insurance Act* as it relates to the Principles for effective IT Risk Management.

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".

Ontario-incorporated insurance companies and reciprocals must achieve the outcomes of the Practices for Effective IT Risk Management, to ensure compliance with Subsection 437(3) of the *Insurance Act*. This includes notifying FSRA of any material IT risk incident within 48 hours.

FSRA monitors compliance with Subsection 437(3) of the *Insurance Act* as it relates to IT risk management. Ontario-incorporated insurance companies and reciprocals that fail to demonstrate compliance with this guidance in regard to their procedures for handling and safeguarding of investments may face supervisory or enforcement action.[34]

Approach

FSRA takes a risk-based approach to the supervision of IT risk. FSRA's supervisory activities consider all the outcomes of the Practices for Effective IT Risk Management, in its assessments and exercises appropriate supervisory judgment when evaluating the policies, processes, and practices established by the regulated entity to effectively manage IT risk.

FSRA's “Risk Based Supervisory Framework for Ontario-Incorporated Insurance Companies and Reciprocals" (“RBSF-I") Guidance (final link needed when published) sets out FSRA's processes and practices for supervising Ontario-incorporated insurance companies and reciprocals and assessing their risk. Its primary focus is to determine the impacts of current and potential future events, both internal and external, on the risk profiles of Ontario-incorporated insurance companies and reciprocals.[35]

FSRA uses the RBSF-I to assess risk and identify imprudent or unsafe business practices and/or misconduct which may impact consumers, in order to be able to intervene on a timely basis. IT risk is a factor FSRA considers in developing the overall risk assessment of credit unions under the RBSF-I. Regulated entities will be assessed in accordance with the RBSF-I to determine their Overall Risk Rating (ORR).

FSRA has the ability to make inquiries, conduct supervisory assessments and collect information from Ontario-incorporated insurance companies and reciprocals relating to IT risk. FSRA will take into consideration whether Ontario-incorporated insurance companies and reciprocals have achieved the desired outcomes outlined in this guidance, including notifying FSRA within 48 hours in the event of a material IT risk incident, in assessing whether an entity has satisfied its requirements outlined under the Interpretation section.

FSRA will reference the criteria articulated in this Approach when assessing the application of the Practices for Effective IT Risk Management and their desired outcomes. The criteria act as a guide to FSRA's supervisory assessments and are not intended to be an exhaustive or prescriptive list. FSRA will take the regulated entity's size, complexity, and risk profile into consideration in its assessment.

Criteria used to assess practice 1: Governance

- The board has approved the regulated entity's documented approach to IT risk management (e.g., frameworks, policies, risk appetite, tolerances, and limits).
- Senior management has ensured that a board-approved IT strategy is documented and implemented, and that it aligns with the regulated entity's overall strategy and demonstrates appropriate investment and resource allocation to safeguard the IT assets of the regulated entity.
- The board has ensured an appropriate organizational structure is established and resources (both people and financial) are available to effectively manage IT risk.

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

- The board receives appropriate and timely information (e.g., audit reports, quarterly reporting, incident reporting) to effectively oversee and assess the management of IT risk by the regulated entity.

Criteria used to assess practice 2: Risk management

- Senior management is responsible for ensuring the establishment of an independent risk oversight function or person(s) to ensure the operations of the regulated entity operate in compliance with the board-approved approach to IT risk management.

- Senior management, with the appropriate subject-matter expertise and IT risk knowledge, is accountable for the regulated entity's IT operations and for implementing the board-approved approach to IT risk management.

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

    - The entity's board-approved IT risk appetite, tolerances and limits.

    - Policies and procedures which enable the regulated entity to:

        - 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 when appropriate (e.g., through insurance).

        - Monitor – develop and implement processes to monitor threats on a regular basis and provide adequate reporting to the board or senior management.

        - Respond – develop processes which allow entities to respond in an effective and timely manner if an incident occurs.

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

- A process to report to the board regularly and consistently on the regulated entity's performance against its IT risk appetite.

The regulated entity has established IT risk management policies and procedures that commensurate with the entity's size, complexity, and risk profile, including but 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.

Criteria used to assess practice 3: Data management

The regulated entity:

- Has policies and procedures to identify and classify (according to type of information) the regulated entity'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 for monitoring for data risk management incidents (e.g., discovery scans).
- Conducts regular testing of data management controls and develop 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.

Criteria used to assess practice 4: Outsourcing

The regulated entity:

- Has criteria for the evaluation and selection of vendors as well as a process to assess the ongoing performance of vendor IT controls.

- Performs a third-party risk assessment prior to contracting/procurement.

- Assesses third-party arrangements/third-party partners (“TPPs") for risk levels and criticality.

- Includes the rights to audit and access information in its third-party contracts.

- Has a process or mechanism (e.g., attestation) to ensure vendor accountability for and compliance with the regulated entity's IT risk management policies and procedures.

- Has a process for classifying critical vendors as part of the regulated entity's broader technology continuity and resiliency plan (see Practice 6).

- Has cloud-specific requirements, which align with the regulated entity's broader IT strategy and risk appetite.

- Assesses risk of incidents and data leakages when outsourcing to cloud computing service providers (“CSPs") are utilized.

- Identifies, investigates, escalates, tracks, and ensures remediation of the incidents at its TPPs.

- Established an exit plan in the event the third party experiences a major, negative event (e.g., bankruptcy, catastrophic outage or loss of key individuals).

Criteria used to assess practice 5: Incident preparedness

The regulated entity:

- Has a process 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 with third parties.
- 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 early warning indicators and identify areas of IT vulnerability and triggers of system disruption.
- Conducts regular vulnerability assessments of its IT assets at network, systems, and applications levels. Vulnerabilities and threats are assessed and ranked according to the severity of the threats.
- 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.
- Performs periodic testing and exercises (e.g., tabletop exercises) to assess incident response plans and capabilities, including with TPPs.
- Has processes for ensuring issues are resolved in a timely manner and that post-incident reviews and root cause analyses are conducted.
- Identifies current or emerging threats proactively, using threat assessments to evaluate threats and assess IT risk.
- Adopts recognized industry standards on incident preparedness.
- Has developed and implemented an IT risk policy, which incorporates a detect, log, manage, resolve, recover, monitor and report approach.

- Regularly and consistently reports to senior management and the board on material IT risk incidents.

Criteria used to assess practice 6: Continuity and resiliency

The regulated entity:

- Maintains an inventory of all IT assets that support business processes or functions.
- Assigns a classification (e.g., risk profile, criticality to the entity) 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 internally as well as with third-party providers.
- Has project management and change management policies and procedures, which ensure the timely completion of IT projects and limit 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 entity will continue to deliver services if critical services are disrupted:
    - 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.

Criteria used to assess practice 7: Notification of material IT risk incidents

The regulated entity:

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

- Notifies FSRA in the event of all material IT risks.
- 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 and 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.[36] In order to adequately protect plan members' rights and benefits, and to effectively administer the pension plan, administrators must consider and mitigate IT risks

As is set out in the PBA, administrators must ensure that any personal information sent electronically must use 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)."[37]

Failure to follow the Practices for Effective IT Risk Management to properly protect their assets, operations and the confidential information of their plan members will likely result in a breach of sections 22 (1) and 30.1 (2) of the PBA.

Approach

FSRA has issued ‘Pension Plan Administrator Roles and Responsibilities Guidance', which details for pension plan administrators their roles and responsibilities.[38] 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 part of this process, administrators will need to demonstrate that they have considered IT risks.

Administrators will need to 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,[39] and other CAPSA Guidelines as applicable. In addition, administrators will need to demonstrate 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.

Effective date and future review

This guidance is effective **June 2023** (TBC) and will be reviewed no later than **June 2027** (TBC)**.**

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.

Appendix 1 – Examples of IT risk incidents

Table 2 - Examples of material IT risk incidents (not an exhaustive list)

Scenario	Example
Cyber Attack	• The regulated entity or individual's IT systems have been compromised by an external hacker; confidential data may/may not have been exposed.
Internal Data Breach	• An employee or contractor has either purposefully or unintentionally caused the exposure of confidential data.
Ransomware Attack	• The regulated entity or individual is unable to access an internal system unless a ransom is paid to an extorter.
Internal Systems Malfunction	• An IT update, aging digital infrastructure, or other incident results in the shutdown of one of the regulated entity or individual's key systems for a prolonged period; ability to provide essential services to consumers may/may not be impacted.
Third-Party Incident	• An IT risk incident occurs at a third-party and the regulated entity or individual is notified that confidential data has been compromised or there may be a prolonged disruption to services.

Appendix 2 – IT Risk Notification Form

FSRA's IT Risk Notification Form provides direction to regulated entities and individuals of useful information to provide FSRA in notifying FSRA in the event of a material IT risk incident.

IT Risk Notification Form

Contact Information

Name of Regulated Entity or Individual:

Type of Regulated Entity or Individual (drop-down menu):

Where Incident Occurred (drop-down menu, including regulated entity/individual, intermediary, third party, other (please specify))

Incident Lead's Name:	Incident Lead's Position:
Incident Lead's Email:	Incident Lead's Phone Number:

Incident name / identifier:

Date and Time Incident Occurred (calendar):	Date and Time Incident Discovered/Detected (calendar):	Date and Time Incident Assessed to be Material (calendar):

Incident Information

Type of Incident (check-list, check all that apply):

Examples include: Cyber Breach, Internal Data Breach, Ransomware Attack Internal Systems Malfunction, Third-Party Incident, Other (Please Specify)

Has the incident been resolved?	If yes, indicate when the incident was resolved (calendar)	If no, please estimate when the incident is anticipated to be resolved (calendar)

Has the incident resulted in the exposure of confidential data? Yes/No/Unsure

If yes, please provide details on the severity of the exposure of confidential data, including the number of impacted people, the nature of the confidential data (indicate if full severity is not known at this time, in which case provide a best estimate):

On a scale of 1-10 please rate the severity of the incident (drop-down):

Has the incident resulted in significant operational disruptions to business systems and functions: Yes/No

If yes, have operations returned to normal?: Yes/No	If no or unsure, please indicate when operations are anticipated to return to normal (calendar)

Please provide details of the full IT risk incident (including current state of incident, direct/indirect impacts, type of systems impacted, primary method used to identify the incident,

procedure and steps used (or plan to use) to respond and recover, known or suspected causes, plan to prevent future incidents)

Effective Date: [TBD]

---

[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.

[3] Negative consumer impacts can include financial losses, breach of privacy and/or confidential information, and a lack of ability to access essential services.

[4] For the purposes of this guidance, the term consumers will also include the public, policy holders, credit union members, pension plan beneficiaries, investors and other stakeholders.

[5] *Financial Services Regulatory Authority of Ontario Act*, 2016 s. 3 [FSRA Act]

[6] *The Personal Information Protection and Electronic Documents Act*

[7] Risk appetite refers to the type and amount of risk an organization is willing to accept in pursuit of its objectives. Regulated entities and individuals are expected to use their own judgement to determine if they rely heavily on technology.

[8] 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.

[9] FSRA Approach Guidance: Financial Professional Title Protection – Administration of Applications

[10] FSRA Interpretation/Approach Guidance: Financial Professionals Title Protection – Supervisory Framework

[11] Rule 2021-001 Sound Business and Financial Practices, s. 5(4) [SBFP RULE].

[12] Ibid at s. 5(2), 5(3)(h).

[13] Ibid at s. 6(1)(i), s. 6(2)(iii).

[14] Ibid at s. 6(1)(i).

[15] Ibid at s. 5(3)(i)(g).

[16] Ibid at s. 15(2)(iv), s. 15(2)(v).

[17] Ibid at s. 10(9)(i)(a)-(b), s. 10(11) and s. 12(1)(i).

[18] Ibid at s. 11(2).

[19] *Credit Union and Caisses Populaires Act*, 2020, S.O. 2020, C. 36, Sched 7, ss. 230 and 233 [CUCPA 2020].

[20] FSRA Approach Guidance: Risk Based Supervisory Framework

[21] Mortgage Broker Regulators' Council of Canada (MBRCC) - Principles for Cybersecurity Preparedness

[22] FSRA Information Guidance: 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

[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

[28] Office of the Superintendent of Financial Institutions Guideline - 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'.

[30] FSRA Approach Guidance: Fair Treatment of Customers in Insurance

[31] Canadian Insurance Services Regulatory Organizations (CISRO) - Principles of Conduct for Intermediaries.

[32] FSRA Interpretation/Approach Guidance: Proposed Principles of Conduct for Insurance Intermediaries

[33] FSRA Information Guidance: Operational Risk Management Framework in Rating and Underwriting of Automobile Insurance

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

[35] FSRA Approach Guidance - Proposed Insurance Prudential Supervisory Framework

[36] *Pension Benefits Act*, R.S.O. 1990, c. P.8, s. 22 (1) [PBA]

[37] Ibid at 30.1 (2)

[38] FSRA Interpretation Guidance - Pension Plan Administrator Roles and Responsibilities

[39] CAPSA Guideline 4. Pension Plan Governance Guideline