IIROC OCRCVM
Investment Industry
Regulatory Organization
of Canada
Organisme canadien de
réglementation du commerce
des valeurs mobilières

Fundamentals of Technology Risk Management

TABLE OF CONTENTS

Executive Summary

Who should read this guidance?

The guide will be useful to mainly small and medium-sized IIROC firms

Are firms required to follow this guidance?
No. Firms are not required to follow this guidance. This guide provides some helpful information to IIROC firms on how to begin building a technology risk management program.

What will you learn?
Significant reliance on technology brings risks to the firm related to security and confidentiality, integrity and accuracy, sustainability and availability, and effectiveness and efficiency. Firms need to manage the entire spectrum of technology risk in order to build operational resilience.

Are there any important considerations?
Governance is at the centre of effective technology risk management. Those charged with governance should work with the management team to develop and oversee the firm's technology strategy and risk management program.

1. How to use the Guide

This Guide was developed as a high-level document, through independent research, discussions and consultations with various firms[1]. The objective of this guide is to help mainly small and medium-sized IIROC firms take the first steps towards assessing and managing technology risk. For larger IIROC firms, technology risk management is generally incorporated within a formalized enterprise risk management (ERM) framework that includes an internal audit function to validate the firm's governance, risk and controls.

This document outlines general principles of risk management and some recommended controls but does not stipulate a framework or rule requirement that firms must follow. Firms should consider retaining the services of risk management and technology risk experts to design and implement a risk management plan that is customized to the firm's unique circumstances, business model and stakeholders.

[1] The Cybersecurity and Technology Advisory Group (CTAG) is comprised of a select group of executives and technology and security professionals from various small and medium-sized IIROC firms from across the country.

For more information on some widely accepted technology risk management frameworks, refer to Appendix A "Guides and References".

2. Overview

The definition of technology and what technology encompasses keeps evolving. At its most basic, technology incorporates the following components:

- Networks, devices and infrastructure
- Software and applications
- Data and information, including the technology used to store and protect the information
- Human resources like developers, users, support staff and all other individuals involved in the operation and use of the technology
- Processes, i.e., the automated and manual procedures involved in the operation of the technology

Technology risk is the business risk associated with the deployment of and reliance on technology and automation at a firm. This could represent a substantial business risk which, if not appropriately managed, has the potential to seriously damage the firm and its future viability.

While IIROC does not have specific rules around technology risk management *per se*, the use of technology by firms could impact an IIROC firm's compliance with IIROC rules. IIROC's Financial & Operations Compliance (FINOPS) currently does a high-level assessment of the firm's technology risk and incorporates it into the overall risk score of the firm[2].

[2] The FINOPS risk model incorporates several factors and is assessed relative to the overall industry. Changes in the risk rating of one factor alone may not necessarily impact the final FINOPS risk score of a firm.

This guide discusses the general principles of managing technology risk in the following sections:

3: Importance of Technology Risk Management

Role of technology at firms and risks involved

4: Process of Managing Technology Risk

Steps to evaluate technology risk

5: Principles of Technology Risk

Explanation on the four pillars of technology risk

6: Technology Controls

Baseline technology controls by risk categories

7: Risk Register

Register that incorporates aforementioned concepts

8: Importance of Governance

Role of governance in managing technology risk

3. Importance of Technology Risk Management

All IIROC firms rely on technology and automation in some form or another. Technology can be essential and help offset the risks traditionally associated with manual involvement in many ways including the following:

- Enhancing customer experience
- Increasing efficiency
- Increasing accuracy
- Reducing costs
- Enhancing employee engagement

However, reliance on technology brings its own set of risks. Firms have traditionally dealt with the risks of technology usage on a case-by-case basis, i.e., by implementing specific application or process controls. This solution by itself, i.e. without a technology risk management plan, is generally not sufficient anymore because of:

- Pervasiveness of and dependence on automation and technology in all aspects of business, and the interdependence and interconnectivity of these technologies

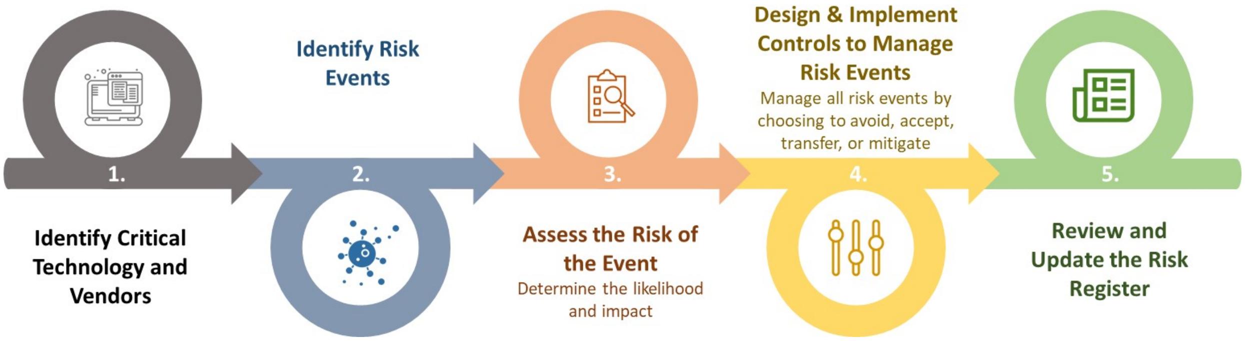
- Growth of big data
- Development of new rules and regulations around information protection and privacy
- Evolution and proliferation of cyber threats
- Adoption of cloud technologies
- Acceleration of technology adoption and automation brought about by the pandemic including implementation of work from home and remote access services, communications technology, and electronic acceptance and delivery of documentation
- Growth of large fintech companies and vendors that provide services and technology solutions in various forms (Platform as a Service (PaaS), Software as a Service (SaaS), etc.)

The management of technology risk can be vital to the survival of a business. As such, all firms should consider developing a technology risk management plan that takes into consideration its unique business model and stakeholders, and accordingly how best to manage the risks. Through an effective technology risk management plan, firms can focus on which key changes to make in order to significantly decrease their overall risk exposure.

4. Process of Managing Technology Risk[3]

Technology risk is typically seen as a non-financial risk or a component of operational risk. Unlike financial risks (e.g. credit risk, market risk, etc.) where firms can choose their level of risk exposure, technology risk cannot be eliminated.

Generally, firms should consider developing a process to manage risk:


1.
Identify Critical Technology and Vendors
2.
Identify Risk Events
3.
Assess the Risk of the Event
Determine the likelihood and impact
4.
Design & Implement Controls to Manage Risk Events
Manage all risk events by choosing to avoid, accept, transfer, or mitigate
5.
Review and Update the Risk Register

[3] While this section speaks specifically to managing technology risk, this process can also be used to manage all other types of risks at the firm.

An effective process would not only involve the technology, risk or compliance staff, but across the organization as well. They use the technology, are most familiar with how the technology works, and rely on it to perform their functions. Ultimately, firms should consider having the risks and controls reviewed by the executive management and the Board to ensure that the critical technology and vendors, and high-risk events are identified, accurately assessed, and appropriately managed.

When conducting this process, it is important to be realistic and practical:

- Too much optimism in assumptions makes this exercise fruitless and will leave the firm, clients and other stakeholders exposed to high-risk events. On the other hand, too much pessimism will make it hard for firms to effectively and efficiently prioritize management of higher risk events.
- Complete mitigation or elimination of risk is not possible because of how pervasive and entrenched technology and automation are in a firm’s business. The achievable goal to aim for is managing the risk, i.e., reducing the impact or likelihood of a high risk event to a level that the firm can accept[4].

4.1 Identify critical technology and vendors

The first step is to itemize a list of all the technology being used at the firm, who and which business area uses it, and for what purpose. This will help determine the critical technology that the firm uses and relies on, which is a key first step. The following are potential areas for firms to consider:

a. The list should be filled out by the business line staff and technology staff to inventory all technology being used at the firm. Refer to Appendix B for a high-level summary of areas where technology is generally used in the investment industry.

b. In order to effectively manage the risk, the identification should also incorporate

  i. How the firm is accessing the technology. For example, is the firm developing it, is it white-labeled/licensed directly, or does the firm access it through a vendor, and

  ii. What the underlying technology is.

4.2 Identify risk events

The next step is to identify the high risk events, i.e. things that could go wrong, and how they could go wrong by listing threats and threat vectors (refer to section 5)

a. What could go wrong (i.e., identify threats) – This is a list of the potential incidents that could make the technology, the vendor or its output unreliable, unavailable, unsecure or ineffective.

b. How could it go wrong (i.e., identify threat vectors and actors) – This a list of the ways in which the potential incidents could occur. It may be helpful to categorize them based on whether they

[4] General risk management principles dictate that firms should determine what their risk tolerance and risk appetite is in order to effectively manage risks. This is separate from the IIROC requirement for all firms to set RAC-based limits for significant functions and activities that use capital ([IIROC Rule 4112-4116]).

are internal and external threats, and further by accidental or intentional. Any controls designed will then depend on the source of the threat.

Firms that are starting out with this process may find it helpful to brainstorm a list of possible threats with the business line users and technology staff. This may help to identify those risk events that have a higher impact and likelihood.

4.3 Assess the risk of the event

Firms should consider assessing the seriousness of risk events based on a combination of its likelihood and impact. This helps identify those risk events that need the most urgent attention. Note that this assessment will differ for each firm based on how they are structured, their business model, their stakeholders and their strategic goals.

4.3.1 Likelihood

When assessing the likelihood of an event occurring, it helps to base the assessment on the range of probable outcomes. For example, the likelihood of the event occurring could be:

- Rare,
- Unlikely,
- Possible,
- Likely, or
- Very Likely.

4.3.2 Impact

When assessing the impact of an event occurring, it is again helpful to base the assessment on the range of significance. For example, if the event were to occur, its impact could be:

- Insignificant,
- Minor,
- Moderate,
- Major, or
- Significant or Material.

Accordingly, the firm should consider who will be impacted and the nature and amount of impact:

- Who would be impacted?

  Who are the stakeholders that rely on the technology or its output – for example, which staff, departments or business functions, clients, regulators, service relationships, etc. would be impacted if the risk event were to occur?

- What would be the business impact?

What would the risk event cost the firm if it were to occur? Some examples include:

- Lost revenues / customers
- Business downtime
- Financial costs to recover / respond / replace / remediate / redress
- Lost reputation
- Legal or contractual liability (e.g., because of missed deadlines or inability to meet service delivery obligations)
- Compliance and regulatory liability

4.4 Design and implement controls to manage risk events

Once the likelihood and impact of a risk event have been determined, the next step would be to sort them in descending order, from those events that have the highest likelihood and highest impact to those assessed as having the lowest likelihood and lowest impact. Accordingly, controls to manage the risk events would be prioritized such that:

a. Risk events with a combined assessment of high likelihood and high impact, which are the high technology risks to the firm, would be the key area of focus to design and implement sufficient and appropriate controls to manage these risk events.

b. Those risk events with a combined assessment of low likelihood and low impact are given the least attention and resources. There may be no need to focus on controls other than to ensure that their assessment of likelihood and impact is accurate and does not increase.

For each of these events, the general technique that firms should consider applying to manage risks is to avoid, accept, transfer or mitigate risk.

- **Avoid**

  This technique advocates avoiding or getting rid of the technology if the likelihood of an event is high or possible and its impact is significant or material. Keep in mind that eliminating technology that has been fully implemented or has been in use for a while may be difficult and expensive. In such cases, "Accept" may be a better alternative..

- **Accept**

  This technique advises firms to leave it alone or do nothing. This is a viable option where the firm's assessment of the risk of the event is determined to be rare or unlikely to occur, and of insignificant or minor impact.

- **Transfer**

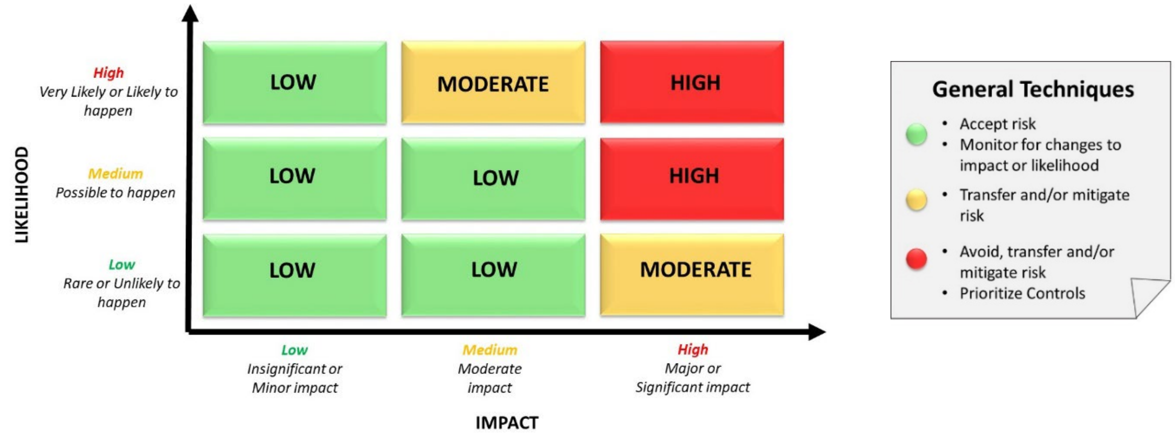
  This technique involves sharing, transferring or offsetting the risk to another party. Examples of methods used to transfer risk are through insurance and outsourcing relationships. Note that there are costs associated with transferring the risk and which, by itself, may not be sufficient. Certain risks like regulatory, compliance, legal and reputational risk may not be transferrable.

- **Mitigate**

  This technique involves the firm designing and implementing general and specific controls to reduce the likelihood and impact of a risk event occurring. For areas where acceptance, avoidance and transference of risks is not sufficient or possible, controls need to be implemented to manage the specific higher risk event.

4.4.1 Risk Management Matrix

While there are several methods available depending on the size of the organization and number of business lines, in general, the following matrix demonstrates how a specific risk event can be managed.



LIKELIHOOD	*Low* *Insignificant or Minor impact*	*Medium* *Moderate impact*	*High* *Major or Significant impact*
High *Very Likely or Likely to happen*	LOW	MODERATE	HIGH
Medium *Possible to happen*	LOW	LOW	HIGH
Low *Rare or Unlikely to happen*	LOW	LOW	MODERATE

IMPACT

General Techniques

🟢
- Accept risk
- Monitor for changes to impact or likelihood

🟡
- Transfer and/or mitigate risk

🔴
- Avoid, transfer and/or mitigate risk
- Prioritize Controls

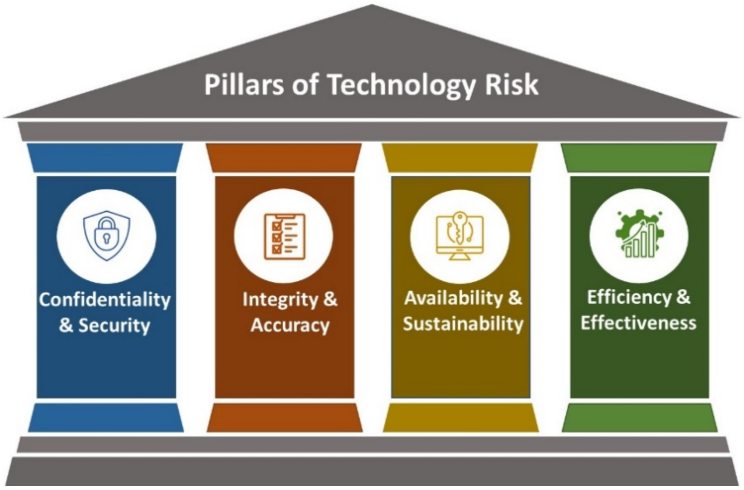
4.5 Review and update the risk register

Firms should consider compiling the list of all risk events, the risk assessment, and the controls in a document or a "risk register" and making sure that the risk register is regularly reviewed and updated. The frequency of the review would depend on the firm's business model, characteristics and whether significant changes to IT have been introduced. Refer to section 7 for more information.

5. Principles of Technology Risk

When implementing a technology risk management plan and thinking about risk events, it is important to understand the principles of technology risk.

Accordingly, the four pillars of technology risk to consider are confidentiality and security, integrity and accuracy, availability and sustainability, and efficiency and effectiveness.


Pillars of Technology Risk
Confidentiality & Security
Integrity & Accuracy
Availability & Sustainability
Efficiency & Effectiveness

5.1 Confidentiality & Security

Confidentiality refers to the need to designate and enhance protection over sensitive information all through its life cycle, i.e., from its collection or creation through to its final disposition and removal from the entity's control. Confidentiality is distinguished from privacy in that privacy applies to information specifically protected by and subject to privacy legislation, for example, personal identifiable information. For purposes of this guidance, privacy and confidentiality have been treated as synonymous.

Security refers to the need for overall protection of both information and technology from unauthorized access, inappropriate disclosure, and other damage that could compromise the availability, integrity, confidentiality, and privacy of the information or technology.

5.2 Integrity & Accuracy

Integrity and Accuracy refers to the need for systems processing, vendor services and data to achieve the aim or purpose for which they were implemented, contracted or collected, respectively. This means ensuring completeness, validity, accuracy, timeliness, and authorization of processing and/or the output being generated.

5.3 Availability & Sustainability

Availability and sustainability refers to the need for continuous access and for the technology and/or its output, and vendor services to be available as designed or contracted. This also includes the ability to recover from applicable risk events.

5.4 Efficiency & Effectiveness

Efficiency refers to the need for the technology or vendor to produce the desired result in a timely and inexpensive manner.

Effectiveness refers to the need for the technology or vendor to be the best possible solution to achieve the firm's strategic goals and objectives.

Assessing the effectiveness of a technology or vendor should be done before determining whether it is efficient.

6. Technology Controls

This section highlights some key dimensions that can be considered, where applicable, for key technology risk categories[5] and some baseline controls that can be implemented where the area has been determined to be high likelihood and high impact. The controls listed in this section are not exhaustive. Firms should design and implement customized controls taking into consideration its unique business model, strategy and risk assessment.

6.1 Information and data management

This area outlines some baseline controls around information being collected, created, processed and/or stored, and disposed. All four pillars of technology risk apply in developing controls around information and data management particularly around data identified as essential and confidential.

Context	Controls
INFORMATION INVENTORY	
What does it mean? *Identifying all interaction with essential and confidential data, and where the data resides.* Why is it important? • *To ensure there is no confidential or private data that is inadvertently unsecured or unprotected* • *To ensure compliance with privacy legislation*	➢ Map out all data touchpoints at the firm, i.e., where information is collected, created, processed, used, or stored ➢ Maintain and review a log detailing where different types of data are stored (e.g., database and server locations, cloud data centres, shared folders, USB drives, paper documents) ➢ Establish and document process for handling privacy enquiries and complaints ➢ Ensure handling of confidential and private information complies with all applicable privacy regulation which can include providing clear

[5] Refer to IIROC's Best Practices Guide and Cyber Governance Guide for more detailed guidance on managing security risks.

Context	Controls
	notification to clients and individuals on the use, processing and storage of their personal information and obtaining consent where required by law [6]
ACCESS MANAGEMENT[7]	
What does it mean? *Restricting access to information based on the principle of least privilege, i.e. that access to technology and information should be limited to what is needed for the individual to perform their job.* Why is it important? • *To protect against a breach of a user's login credentials* • *To limit the impact of a breach, whether accidental or intentional, of a user's login credentials*	➢ Create user hierarchy policies detailing access requirements and approvals ➢ Control user access with elevated privileges and include monitoring alerts when an administrator account is added or removed ➢ Grant, remove or adjust access as part of the user onboarding and off-boarding process in a timely manner ➢ Implement strong password management policies including password complexity, limits to password attempts, and limits to password reuse ➢ Review access rights at regular intervals for each device, system or application including for inactive accounts, monitoring anomalous or irregular access attempts, and deactivated accounts ➢ Verify the authenticity of the users logging into applications at regular intervals ➢ Enforce multi-factor authentication, screen locks, timed log-outs, and other authentication measures for accessing confidential data ➢ Encrypt data files that store passwords
DATA LOSS PREVENTION	
What does it mean?	➢ Establish policies to identify and classify essential and confidential data (i.e., personally identifiable

[6] In Canada, privacy regulation is governed by the Privacy Act, PIPEDA and amended by the Digital Privacy Act, and provincial private sector privacy laws in BC, Alberta and Quebec.

[7] These controls are related to device management, and systems and applications management.

Context	Controls
Identifying and protecting essential and confidential information. Why is it important? - *To ensure that confidential and private data are always treated securely* - *To help firms secure confidential and private data in the most efficient manner (i.e. costs, time and resources)* - *To ensure compliance with privacy legislation* - *To limit the impact of a data breach*	information), and for the backup, retention and recovery of application programs and data ➢ Track the movement of essential and confidential data through and out of the firm ➢ Create and implement a data retention policy ➢ Train users continuously to ensure they understand how to securely handle confidential information
DATA INTEGRITY	
What does it mean? *Ensuring the accuracy and completeness of the information being generated.* Why is it important? - *To ensure that data needed for key functions can be relied upon* - *To ensure that a technology malfunction or incorrect output can be detected and corrected*	➢ Establish procedures to review reports being generated to ensure accuracy ➢ Establish accountability and responsibility structures to identify who is responsible for accuracy and completeness of reports where other businesses or functions rely on the integrity of the reports to discharge their responsibilities[8]
THREAT MONITORING	
What does it mean?	➢ Monitor for anomalous transactions including unusual user transactions, user behavior (e.g.,

[8] Individuals registered with IIROC that have designated regulatory responsibilities such as supervisors, chief financial officers, chief compliance officers, etc. need to understand their role in the firm's responsibility and accountability structure for ensuring that the information they are relying on is accurate and complete.

Context	Controls
Monitoring malicious activity and threats. Why is it important? • *To protect from and detect malicious external attempts to gain unauthorized access to technology or data* • *To detect malicious insider attacks* • *To enable firms to promptly respond to attacks and limit the damage and impact*	large number of downloads, streaming media), network and systems activity (e.g., high volume of network traffic, unsuccessful login attempts, logins after work hours), and other irregular activities ➢ Establish and implement policy to collect, analyze, monitor and review security events and audit logs ➢ Maintain a 24/7 security services group/division ➢ Monitor threat landscape including subscribing to threat intelligence information services

6.2 Device management

This area outlines some baseline controls around management of hardware and devices being used to conduct the various business activities and operations of the firm. Security, sustainability and efficiency are the important technology risk pillars when developing controls around managing devices that the firm uses.

Context	Controls
PHYSICAL AND ENVIRONMENTAL SECURITY	
What does it mean? *Physically securing areas where technology assets are located.* Why is it important? • *To protect physical technology and hardware from accidental, intentional or environmental damage*	➢ Establish physical access controls, surveillance technology and other security controls to prevent and detect unauthorized access to sensitive locations (e.g., server rooms) ➢ Protect server room/data center from environmental threats and hazards (e.g., fire and water damage) ➢ Require identification for all employees, contractors and visitors ➢ Obtain and review the data center vendor's audit report (refer to Appendix C) and validate that appropriate physical access controls are in place at the data center

Context	Controls
MANAGEMENT OF FIRM-OWNED DEVICES AND SERVERS	
What does it mean? *Managing risks associated with physical technology assets.* Why is it important? • *To ensure that there aren't any devices that are unprotected or unsecure, and are therefore, vulnerable to unauthorized access* • *To protect and secure all devices from malicious external threats to data or applications within the device* • *To protect confidential and private information on all devices from accidental breaches due to loss of device* • *To ensure that the device is functioning efficiently and is compatible with all critical systems and applications* • *To ensure that essential information on the device is backed up*	➢ Maintain an updated list of all of devices that details the location, when the last maintenance check was performed, and who has possession of the respective assets. ➢ Establish policies for the acceptable use of devices including requirements to shut down or lock devices when not in use, and a mobile device management plan ➢ Establish baseline configurations for hardware that can only be altered with a formal change request ➢ Restrict users from accessing unsecure sites and applications, and from disabling security solutions on devices ➢ Deploy anti-malware applications on all technology (specifically, devices, servers, business critical systems and applications) ➢ Encrypt devices that collect, process, use, or store confidential information ➢ Implement tools to wipe data remotely on all missing or stolen devices ➢ Establish and implement end of life policies for devices (i.e., ensure that obsolete or decommissioned devices are wiped clean and securely disposed of) ➢ Document and implement policies for server backups and offline availability
BRING YOUR OWN DEVICE (BYOD)	
What does it mean? *Managing risks associated with personal-owned devices that are used to access essential and confidential information and critical systems and applications.*	➢ Document formal BYOD policies which outline how users can use their personal devices to access firm systems and information ➢ Maintain a list of all personal-owned devices being used to access firm information

Context	Controls
Why is it important? • *To protect and secure all personal devices from malicious external threats to firm data or applications being accessed on the device* • *To protect firm-related confidential and private information on all personal devices from accidental breaches due to loss of device* • *To ensure that essential business data and output on the personal device is backed up*	➢ Enforce access to confidential data and applications on personal mobile devices via a secured isolated sandbox or container ➢ Implement remote-wipe capability in case of loss of device
NETWORK SECURITY	
What does it mean? *Protecting and monitoring internal and external networks for security risks* Why is it important? • *To protect and secure all networks from malicious external threats to technology and information on the network* • *To detect unauthorized access to networks from external or internal actors*	➢ Automatically block attempted access by unregistered devices to internal networks ➢ Scan for unauthorized devices or systems on the network ➢ Install firewalls to protect connections from external threats ➢ Establish detection rules that limit access to trusted sites and deny communications from known malicious IP addresses ➢ Create guest access to networks for visitors or temporary contractors with restrictions on access
EXTERNAL STORAGE DEVICES / REMOVABLE MEDIA	
What does it mean? *Managing the risks associated with external storage devices and removable media.* Why is it important? • *To protect and secure confidential and private information data on removable storage devices from loss, theft or misuse*	➢ Encrypt external storage devices (e.g., external hard drives and USBs) ➢ Lock down ports on firm-owned devices – limit usage only to firm-approved devices ➢ Limit user actions (e.g., read-only, download only, etc.) permitted to be performed on the devices

Context	Controls
• *To protect devices and networks from being infected by malware through removable media*	

6.3 Systems and application management

This area outlines some baseline controls around all applications and software used in various business activities and operations. Security, integrity, sustainability and efficiency are the important technology risk pillars to consider when developing controls around managing the software and applications that the firm uses.

Context	Controls
SOFTWARE INVENTORY	
What does it mean? *Managing risks associated with software assets, systems and applications.* Why is it important? • *To ensure that all systems or applications, and the data being accessed, are protected and secure from unauthorized access and malicious downloads* • *To ensure that there aren't any systems or applications that are unprotected or unsecure, and are therefore, vulnerable to unauthorized access* • *To detect and prevent unauthorized or unplanned changes or access to systems or applications which could cause business disruptions, losses or breaches*	➢ Maintain an inventory of software and applications, review it at least annually, and update it as required ➢ Establish a request/approval process for acquisition and installation of software ➢ Detect and block unauthorized changes or installations of software ➢ Establish baseline configurations for software that can only be updated with a formal change request
PATCH AND VULNERABILITY MANAGEMENT	
What does it mean?	➢ Implement automated patch management and software update solutions

Context	Controls
Establishing patch and vulnerability practices Why is it important? • *To ensure that all systems or applications, and the data being accessed, are protected from security issues and vulnerabilities* • *To ensure that all critical systems or applications will continue to be operational and supported by the developer to address and correct any issues or problems*	➢ Test material patches before applying them to systems and/or software ➢ Prioritize and track missing patches across all environments (including, test and production environment) ➢ Manage end-of-life or end-of-support issues (i.e., take action to replace or update before the product support or warranty expires)
MONITORING PERFORMANCE AND OUTPUT INTEGRITY	
What does it mean? *Monitoring the functioning and output of systems and applications* Why is it important? • *To ensure that critical systems and applications continue to function effectively and meet the needs of the users* • *To ensure critical systems and applications produce the right output as needed* • *To detect system malfunctions or issues with output* • *To ensure that critical systems and applications continue to be applicable if there are changes in user needs, in other*	➢ Establish and monitor risk and performance metrics for key technology and applications based on the needs of the business owners and the strategic vision of the firm ➢ Review the integrity of the information being generated to ensure the system is producing accurate and complete information ➢ Ensure that the systems and technology being used for recordkeeping purposes meet all applicable legislative and regulatory requirements[9] ➢ Ensure that surveillance activities encompasses all communications technology being used[10] ➢ Review APIs and other interfaces between the different systems and applications for completeness and accuracy

[9] IIROC rules stipulate minimum books and records and audit trail requirements most of which are outlined in [IIROC Rule 3800]. Firms also need to ensure compliance with NI 23-101 and [IIROC Rule 7201-7205].

[10] IIROC has rules around surveillance and retention of client communication. Refer to IIROC Notice 11-0349 *Guidelines for the review, supervision and retention of advertisements, sales literature and correspondence* and [IIROC Rule subsection 1201(2) and IIROC Rule 3600]).

Context	Controls
connected systems and applications, and in legal or regulatory requirements • *To ensure that the critical systems and applications currently being deployed are the most effective and efficient solutions available*	➢ Obtain and review Service Organization Control (SOC 2) reports for key technology and applications at least annually (refer to Appendix C for a comparison of the different SOC reports)
SOFTWARE DEVELOPMENT LIFE CYCLE	
What does it mean? *Managing risks associated with software that is developed at the firm at every stage of the development life cycle.* Why is it important? • *To protect and detect unauthorized, accidental or unplanned changes to the programming and code* • *To ensure that any changes to the programming and code are tested before implementation or going live so that there are no conflicts with connected applications or devices, and that it is producing the right output* • *To ensure that critical systems and applications are continuing to generate the accurate output* • *To ensure that systems and applications are amended on a timely basis if there are changes in user needs, in configurations of other connected systems and applications, and in legal or regulatory requirements* • *To ensure that the developed solution continues to be the most effective and efficient solutions available*	➢ Establish standards and secure coding practices for software developers based on industry frameworks ➢ Perform security testing on all post-design (before implementation or installation) phases for every application ➢ Perform independent code reviews ➢ Update applications based on experiences gained, technological innovations and emerging threats ➢ Perform static code analysis and remediate vulnerabilities identified

6.4 Process management

This area outlines some baseline controls around all processes; in particular, those that have a direct impact on the security, integrity, availability and efficiency of technology.

Context	Controls
DOCUMENT AND FLOWCHART BUSINESS PROCESSES	
What does it mean? *Understanding and documenting how technology is integrated in the different business operations.* Why is it important? • *To identify if there are manual processes that can be effectively and efficiently automated* • *To ensure that processes necessary to the proper functioning of critical technology are appropriately managed, supervised and backed-up*	➢ Document flowcharts and process narratives to understand how technology is integrated in the different business operations ➢ Identify and address areas of automation and manual procedures separately
MONITOR EFFICACY OF BUSINESS PROCESSES	
What does it mean? *Monitoring the performance of business processes.* Why is it important? • *To ensure that all business processes and inputs necessary to the operation of critical technology are working as planned* • *To ensure that issues with business processes can be identified for correction* • *To ensure that all key processes are adequately supervised and controlled*	➢ Establish efficiency and effectiveness metrics for performance of business functions and activities ➢ Review the performance of functions against metrics at regular intervals to determine if changes need to be made ➢ Identify areas of weakness (e.g., higher rate of failures where procedures are manually performed, areas of heightened fraud risk, etc.) ➢ Review flowcharts and process narratives at regular intervals to ensure they are being followed, and evaluated for improvements ➢ Document management's response to address the issues

6.5 Change management

This area encompasses controls around changes to technology and related processes that are effectively rolled out. This area is often ignored but has the potential to cause significant losses if not properly managed. Implementing change to significant technology or vendors should take into consideration all four technology risk pillars.

Context	Controls
POLICIES AND PROCEDURES	
What does it mean? *Maintaining a plan to guide the implementation of key changes to critical technology or vendors.* Why is it important? • *To ensure that the adoption of new or updated critical technology increases effectiveness and efficiency* • *To ensure that critical technology changes and implementations are operationalized seamlessly* • *To minimize business disruptions, delays, costs, and errors from implementing significant changes to critical technology*	➢ Document and implement change management processes to cover key considerations such as strategic alignment, budget management, management of risks, planned timelines, communication, stakeholder management, and cultural changes ➢ For significant technology or vendor conversions, flowchart all business functions, processes, devices, systems and applications and ensure that the plan addresses all changes ➢ Develop metrics to measure the success and efficacy of proposed changes ➢ Ensure experienced personnel are responsible for leading and monitoring the change management, and continuously improving the process ➢ Assign the responsibility of signing off, and ongoing monitoring of, automated functions to registered personnel
BOOKS AND RECORDS SYSTEMS CONVERSIONS[11]	
What does it mean?	➢ Conduct an audit before conversion/implementation to assess readiness as it relates to critical vendors, business functions, systems and applications, and

[11] These are IIROC's expectations when firms undergo a conversion of their significant books and records systems. Firms that are undergoing significant system conversions should report the proposed change to IIROC as outlined in IIROC Notice 10-0060 *Reporting of Changes to Business Models* [IIROC Rule 2246(2)].

Context	Controls
Managing risks from conversions or implementations of significant systems and applications that impact regulatory recordkeeping requirements. Why is it important? • *To ensure compliance with regulatory requirements* • *To prevent data loss during migration* • *To minimize business disruptions and losses*	information that will be impacted prior to going live ➢ Ensure that all applicable documentation, service agreements, and policies and procedures are updated ➢ Update the business continuity plan to incorporate the new system ➢ Conduct an audit after conversion/implementation to ensure that the system is working as designed and that all data, connecting systems and functions have been accurately and completely migrated and replicated

6.6 Vendor management

This area outlines some baseline controls around management of critical vendors. The use of outsourced vendors could add significant risk across all four pillars of technology risk[12].

Context	Controls
VENDOR DUE DILIGENCE	
What does it mean? *Validating and approving critical vendors* Why is it important? • *To ensure that the vendor is reputable and will be able to deliver critical technology or services as and when needed* • *To ensure that the vendor can meet the firm's performance standards*	➢ Document policies and procedures pertaining to managing vendor risks and performance including business case, vendor search, vendor risk assessment, legal review, and a signed contract ➢ Conduct ongoing review of all vendors and their services and consider the information, systems and processes involved ➢ Assign an executive to manage relationships and arrangements with critical vendors ➢ Assess vendors for potential information and security risks before entering into a contract (e.g.,

[12] IIROC issued Notice 14-0012 in 2014 to provide guidance on *Outsourcing Arrangements*. The principles discussed here are substantially the same as those reflected in the IIROC Notice.

Context	Controls
• *To ensure that the vendor can meet the firm's security standards* • *To ensure that the vendor will be responsive to issues and agile to changes in user needs, and legal or regulatory requirements* • *To ensure vendor can provide their products or services effectively and efficiently*	assess cybersecurity posture, conduct independent cybersecurity assessments, assess risk related to use of subcontractors, etc.) ➢ Obtain proof of certifications, audit reports, customer testimonials, compliance reports from key regulators, audited financial statements, and conduct other background checks to ensure that the vendor is reputable and viable
VENDOR ONBOARDING	
What does it mean? *Establishing process steps to onboard new approved vendors.* Why is it important? • *To ensure clear communication and documentation of rights and responsibilities* • *To protect the firm from costs and risks associated with the vendor* • *To ensure vendors are granted access to only those systems and applications and data that they need*	➢ Obtain a signed agreement[13] that incorporates and articulates, among other things, ○ roles and responsibilities, ○ ownership of information and technology, ○ performance and security standards, including obtaining audit/SOC reports without material exceptions, and the consequences of breaches, ○ clauses for indemnification or pre-approval of material sub-contractors, ○ clauses for notification of significant changes at the vendor that would impact the firm, ○ termination clauses, including timelines and responsibilities for retention and destruction of confidential and proprietary information, ○ compensation, and ○ a Non-Disclosure Agreement (NDA)

[13] For cloud services providers, refer to ISO/IEC 19086-1 *Cloud Computing Service Level Agreement Framework* the international standard, which provides guidance on establishing a service level agreement.

Context	Controls
	➢ Create a vendor onboarding checklist which incorporates all aspects of vendor management ➢ Map and identify all the information and technology that vendors will be given access to ➢ Communicate metrics and standards that the vendor needs to meet and the process of escalating material breaches
MONITORING PERFORMANCE AND RISKS OF VENDORS	
What does it mean? *Monitoring the vendor and their service.* Why is it important? • *To ensure that the vendor can continue to deliver critical technology or services effectively and efficiently, as and when needed* • *To ensure that the vendor is meeting the firm's performance standards (i.e. that the firm is able to detect and correct any issues with performance)* • *To ensure that the vendor is meeting the firm's security standards (i.e. that the firm is able to detect and protect against any security issues or threats)* • *To ensure that the vendor is responding to issues being escalated* • *To ensure that any risks to the firm from changes to vendors, technology or processes are identified and mitigated*	➢ Regularly review vendor performance in accordance with established metrics ➢ Regularly review vendor security controls including obtaining attestations pertaining to use of the firm's confidential and private data ➢ Review the vendor based on feedback from the business function, news releases, technological innovations, financial information, and changes in the industry or regulation ➢ Obtain and review a Service Organization Control (SOC 2) Type 2 report at a minimum annually (refer to Appendix C for a comparison of the different SOC reports) and assess the risk and action plan for material exceptions ➢ Have regular touchpoints with critical vendors to discuss any breaches of performance or security standards, and if changes are being considered that would impact the firm or the vendor ➢ Escalate material issues identified in the monitoring of the vendor, their performance, or security
INCORPORATING VENDORS INTO THE BUSINESS CONTINUITY PLAN (BCP)	
What does it mean?	➢ Implement a firm-wide backup plan for all critical vendors

Context	Controls
Maintaining backup plans for critical vendors. Why is it important? • *To minimize business disruptions and costs if a critical vendor is unable to deliver technology or services as and when needed*	➢ Plan and test a replacement strategy with other vendors or workaround business processes in the event of a sudden or unexpected failure of the vendor to deliver services ➢ Obtain and review the vendor's BCP to ensure that they have backup plans to continue to deliver services in the event of incidents or disasters
OFF-BOARDING VENDORS	
What does it mean? *Establishing process steps when changing or terminating vendor relationships.* Why is it important? • *To ensure that the firm is protected from security issues at the vendor after the relationship has terminated*	➢ Implement controls to delete data and remove access once a vendor contract is terminated or expired ➢ Obtain attestation from the vendor that all firm information is deleted from their own and their sub-contractors' possession

6.7 Business continuity, incident response, and disaster recovery

This area outlines some baseline controls to ensure the availability and sustainability of critical technology and information. The controls would include having an actionable and practical plan to respond and recover from incidents, and ensure that business functions that rely on core and critical technology and related processes can sustain if the technology is unable to function for short or extended periods of time.

Context	Controls
BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING[14]	
What does it mean?	➢ Document a Business Continuity Plan (BCP) to address technology risks which identifies the key business functions, technology and information,

[14] [IIROC Rule 4711-4714] requires that firms establish a business continuity plan (BCP) and to test it frequently.

Context	Controls
Maintaining a Business Continuity Plan (BCP) to address failures or disruptions of critical technology. Why is it important? • *To minimize business disruptions and costs if a critical technology is unavailable as and when needed*	responsible personnel, expected maximum outage, response plan and timelines, trigger events for the BCP ➢ Ensure individuals responsible for the use and support of critical technology are incorporated into the BCP and back-up individuals are identified, and all are familiar with key aspects of the BCP ➢ Determine the firm's capability to handle increases in client account creations and trading activities, and plan for operational resilience ➢ Maintain and update the employee and key contacts directory ➢ Review and revise the BCP at least annually ➢ Assess the annual budget to focus on emerging risks associated with the industry and their business operations
INCIDENT RESPONSE PLANNING[15]	
What does it mean? *Maintaining an Incident Response Plan to address security risk events.* Why is it important? • *To ensure that the firm can respond quickly when a security incident is detected to limit the scope of an attack and minimize losses*	➢ Document a security incident response plan that addresses a data breach or cybersecurity attack separate from the BCP process ➢ Engage and retain an incident response team of experts including a breach coach, legal counsel, forensics investigators, insurance providers, and crisis communications consultants to deal with possible incidents before they occur ➢ Establish an internal incident response team (including individuals from legal, corporate communications and HR) ➢ Develop a communications plan for reporting security incidents to the public and media, to management and relevant stakeholders, to

[15] Refer to IIROC's Cyber Incident Management Planning Guide for detailed guidance.

Context	Controls
	regulators[16] and privacy commissioners, and to employees ➢ Perform a root cause analysis for significant incidents and conduct a forensics analysis after an incident has been contained
TESTING AND ACTIONING IMPROVEMENTS	
What does it mean? *Performing tests of the BCP and incident response plans* Why is it important? • *To ensure that the BCP and incident response plans are practical and easily operational if they are suddenly triggered* • *To ensure that any issues or gaps are identified and fixed in the BCP and incident response plans*	➢ Perform tests of the BCP and incident response plan at regular intervals to ensure the plans are up to date and effective ➢ Conduct table-top exercises and crisis simulations to validate the plans and ensure that any gaps are addressed ➢ Update the BCP and incident response plans based on lessons learned from the tests ➢ Increase capacity to handle increases of client account creations and trading activities based as necessary

6.8 Human Resource management

This area outlines some baseline controls around human resources to ensure that security risks are managed and that the key individuals needed to develop or maintain the critical technology are hired and retained. This includes ensuring that such key positions are appropriately backed up, cross-trained and supported.

Context	Controls
HUMAN RESOURCE MANAGEMENT	
What does it mean? *Managing technology and security risks associated with employees, contractors and vendors.*	➢ Establish formal security processes for onboarding and off boarding employees, contractors and vendors ➢ Conduct background checks and screening of new hires, contractors, and vendors for security risks

[16] [IIROC Rule 3703] requires that cybersecurity incidents that meet stipulated requirements be reported.

Context	Controls
Why is it important? • *To minimize the likelihood of authorized users, that have access to critical technology and confidential information, causing a security incident or breach* • *To ensure that the firm is aware of attacks or breaches as soon as it happens so that they can take quick action to respond and limit the scope and minimize losses* • *To ensure that firms can prevent threats arising from authorized users* • *To ensure that firms can detect attacks from authorized users*	➢ Define disciplinary processes for non-compliance with security policies ➢ Establish and action a program to identify and manage insider threats ➢ Conduct cybersecurity awareness training for all staff on hiring and at least annually which incorporates how to handle confidential data including personal information, and how to detect threats (e.g., phishing emails) ➢ Establish and communicate the process for employees, contractors and vendors to report security problems and potential issues ➢ Include in the code of conduct a section for confidential information and make the employees, contractors and vendors sign it annually
ATTRACTING AND RETAINING TALENTED EMPLOYEES	
What does it mean? *Maintaining a plan to hire and retain key individuals needed to manage critical technology.* Why is it important? • *To minimize business disruptions and costs associated with unavailability of key employees to manage critical technology* • *To ensure that firms can meet their strategic technology plan, goals and objectives*	➢ Determine the strategic human resource plan for technology and ensure talent recruitment and alignment throughout the organization ➢ Identify key roles and key employees in technology and develop a strategy to retain and or attract the required talent for those roles ➢ Cross-train and backup key employees needed to manage, develop, and use critical technology

7. Risk Register

Firms should consider compiling all of the work done on risks and controls in a risk register.

Below is one example of what the register could look like:

			Principles ***(check all that apply)***				**Likelihood** ***(Check one)***					**Impact** ***(Check one)***					
Business Function	**Name of Technology**	**Risk events**	**C**	**I**	**A**	**E**	**R**	**U**	**P**	**L**	**VL**	**I**	**Min**	**Mod**	**Maj**	**S**	**Mitigating Controls**

Putting the risk register together is not a one-time exercise. The firm's risk management policies and procedures should consider the following:

- The risk register is reviewed at least annually by applicable staff
- Risk events identified as high impact and/or high likelihood are reviewed more frequently to verify that the controls in place are still sufficient and effective to manage the risk
- Certain key triggers require an update or review of the risk register. For example,
    - on procurement of technology or contracting/hiring/management of vendors
    - when circumstances in the industry or the business increase the likelihood or impact of risk events
    - when a change in business process is being implemented
    - when there is a change to IT service providers

8. Importance of Governance

Effective management of technology risk requires the involvement of individuals charged with governance and oversight of strategy at the firm.

As mentioned earlier, technology risk is not just the responsibility of the IT, risk or compliance staff. Effective management of technology risk requires collaboration of individuals from the business lines all the way to the top including the Board of Directors and Executive Management.

The Board of Directors is responsible for governance at a firm. While senior management is responsible for developing a core technology strategy and risk management framework, the Board of Directors is responsible for oversight of senior management and challenging their strategic proposals and implementation plans[17].

The Board of Directors' and senior management's responsibilities as it relates to technology is essentially two-fold:

1. Development and oversight of the strategic technology plan
2. Oversight of technology risk management

8.1 Development and oversight of the firm's strategic technology plan

In an industry where technology is becoming increasingly enfolded within the business, the Board of Directors and senior management of firms should consider not just how much to rely on technology, but what the long term vision is with respect to the adoption and/or development of technology, automation and innovation, and accordingly, what aspects of reliance this form needs to take.

For example, the Board of Directors and senior management should consider:

- whether the firm should be a fintech innovator, or if not, what stage of the technology adoption process to be engaged in, and in which business functions or areas, i.e. whether building technology is part of the firm's core competencies in any business function or whether to rely on other vendors
- emerging technologies and their potential for disruption to the business and industry
- whether the firm has the resources to achieve its strategic technology plan
- whether to incorporate the firm's technology and innovation vision in marketing and public affairs
- reviewing ongoing technology projects to ensure that they are implemented on time, within the budget, and aligned with the overall strategy of the firm

8.2 Oversight of technology risk management

The Board of Directors and senior management should ensure that high risk events are being properly identified and appropriately managed[18].

For example, as it pertains to technology risk, the Board of Directors and senior management should consider:

[17] At most small and medium-sized IIROC firms, the Board of Directors often consists of senior management personnel as well.

[18] IIROC Rule 1502, which will become effective December 31, 2021, stipulates that IIROC firms must assign responsibility for each significant area of risk to an appropriate Executive. If technology risk is considered a significant area of risk for an IIROC firm, compliance with this Rule will need to be considered.

- reviewing the risk register to ensure that the high risk events have been identified and are being appropriately managed
- reviewing policies and procedures to ensure that technology risk management is integrated and incorporated in all relevant aspects of business operations
- establishing responsibility and accountability structures to oversee the management of technology risk
- approving risk tolerance and risk appetite thresholds for technology and security incidents, and monitoring major breaches of such thresholds
- developing performance metrics to determine the success or effectiveness of a risk management control
- requiring and reviewing audits or table-top exercise results that test and validate controls both internally and at suppliers / external vendors

As technology risk becomes pervasive, the Board members and senior management responsible for governance should be engaged in understanding the technological environment that the firm operates in. For smaller firms, where this can be challenging, they can consider, for example:

- hiring specialists and expert consultants in technology and risk management to advise the Board of Directors and senior management
- training and educating Board members and senior management on the relevant technologies, innovations and risks
- onboarding new Board members and hiring senior management personnel who have the relevant technology risk management backgrounds

The Board of Directors and senior management should be engaged and involved in determining the firm's strategic technology plan and managing the risks to ensure the long-term success of the firm.

9. Conclusion

With the increasing reliance and dependence on technology and automation, IIROC firms are encouraged to look more closely into managing the risks associated with this reliance. Effective management of technology risk is possible if some basic principles are followed.

Firms that do not have a formalized framework today to manage technology risk should consider taking the first steps by reaching out to risk management and technology risk consultants to design and implement a uniquely customized framework, which takes into consideration the business model and stakeholders of the firm, to manage the firm's risk from technology usage.

10. Appendices

A. Guides and references

Global standards

- ISO 27000
- NIST
- COBIT

Publications

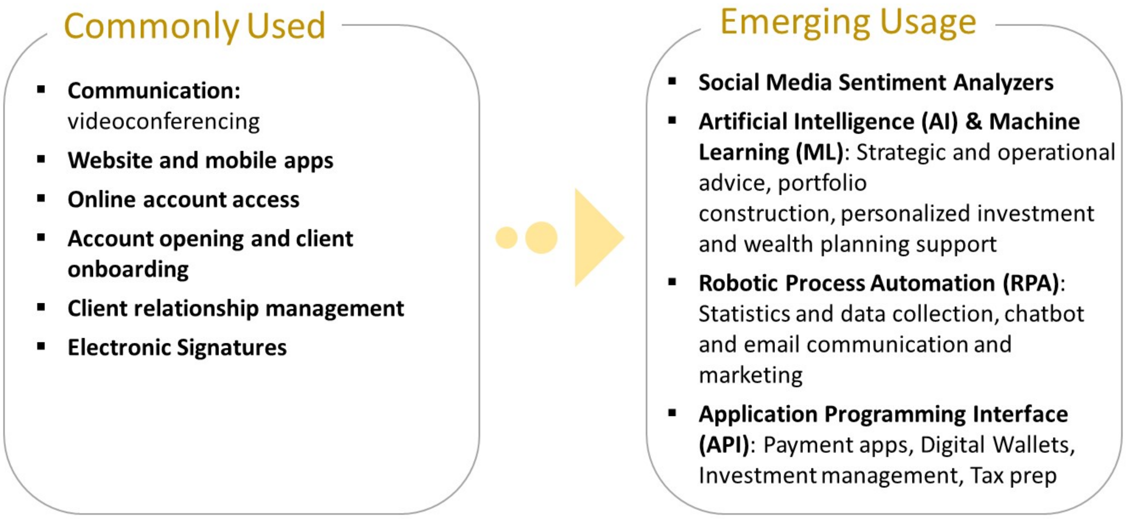
- Cybersecurity Best Practices Guide, Investment Industry Regulatory Organization of Canada (IIROC), 2015
- Cyber Incident Management Planning Guide, Investment Industry Regulatory Organization of Canada (IIROC), 2015
- Developing financial sector resilience in a digital world, Office of the Superintendent of Financial Institutions, September 2020
- Forging New Pathways: The next evolution of innovation in Financial Services, World Economic Forum, September, 2020
- Guidelines for processing personal data across borders - Office of the Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada, January, 2009
- IIROC Cyber Governance Guide, Investment Industry Regulatory Organization of Canada (IIROC), January, 2020
- ISO/IEC 19086-1 Cloud Computing Service Level Agreement Framework, International Organization of Standardization
- Privacy and outsourcing for businesses - Office of the Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada, January, 2014
- What you need to know about mandatory reporting of breaches of security safeguards - Office of the Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada, October, 2018

B. Technology usage among IIROC firms

Customer Service and Experience

Over the last few years, IIROC firms have significantly increased investments in technologies to enhance customer service and experience. Some of the more widely used technologies are related to virtual communications (e.g., videoconferencing tools) and the secure collection of information from the client. Electronic signatures is another area of automation that is increasingly becoming the norm rather than an exception, the acceleration of whose adoption was brought about by circumstances resulting from the pandemic.

Several IIROC firms are also in various stages of deployment of technologies related to the client account opening and the onboarding process. Similarly, websites and mobile apps offering clients online access to their account information and other client relationship management systems are also areas where technology is being widely used. Note that these observations do not include those firms that offer clients online trading services (i.e., Order Execution Only firms and robo-advisory) where the technologies supporting the client trading interface and corresponding applications are integral to their business model.



Commonly Used

- **Communication:** videoconferencing
- **Website and mobile apps**
- **Online account access**
- **Account opening and client onboarding**
- **Client relationship management**
- **Electronic Signatures**

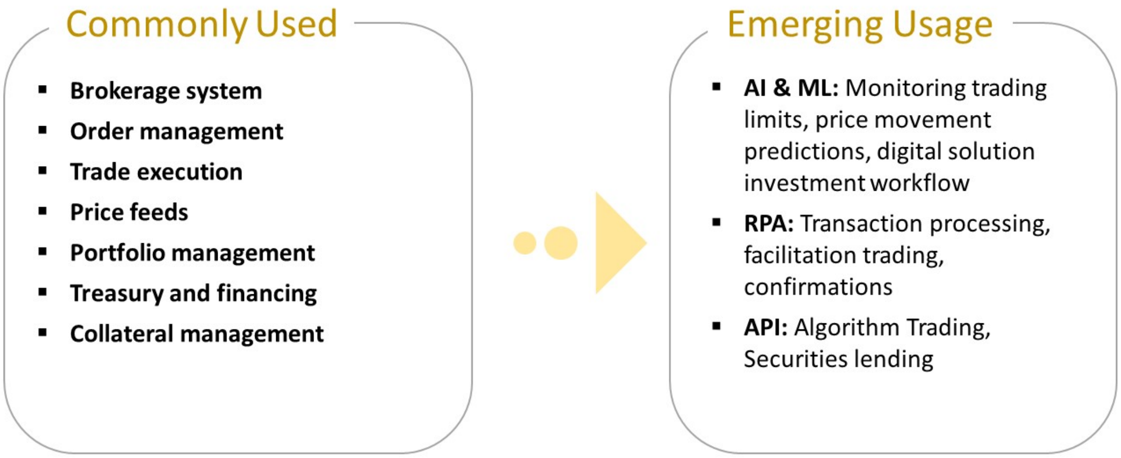
Emerging Usage

- **Social Media Sentiment Analyzers**
- **Artificial Intelligence (AI) & Machine Learning (ML)**: Strategic and operational advice, portfolio construction, personalized investment and wealth planning support
- **Robotic Process Automation (RPA)**: Statistics and data collection, chatbot and email communication and marketing
- **Application Programming Interface (API)**: Payment apps, Digital Wallets, Investment management, Tax prep

Trading Operations

The trading function of IIROC firms, which includes the clearing and settlement process, relies significantly on a whole host of technology and automation as part of their core operations.

A brokerage system, encompassing the recordkeeping of accounts, transactions and asset information, is the core technology system used across IIROC firms. Similarly, IIROC firms use technology in a number of other areas including, but not limited to, order management, trade execution, price feeds, portfolio management, financing operations and collateral management.



Commonly Used

- **Brokerage system**
- **Order management**
- **Trade execution**
- **Price feeds**
- **Portfolio management**
- **Treasury and financing**
- **Collateral management**

Emerging Usage

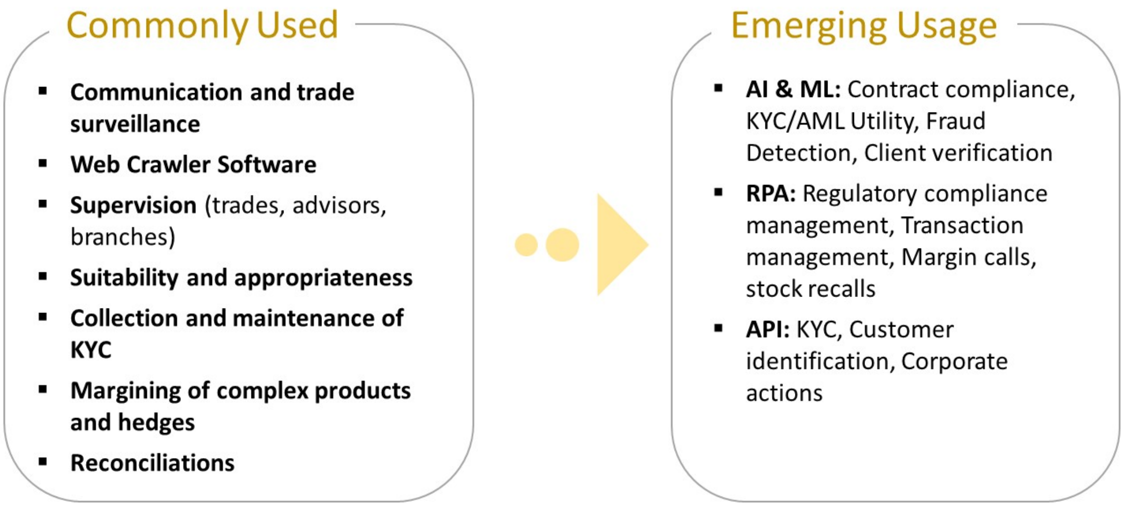
- **AI & ML:** Monitoring trading limits, price movement predictions, digital solution investment workflow
- **RPA:** Transaction processing, facilitation trading, confirmations
- **API:** Algorithm Trading, Securities lending

Compliance

The Compliance function at IIROC firms is increasingly relying on various technologies to assist them in discharging their regulatory responsibilities. Such types of technology are generally referred to as "RegTech" or Regulatory Technology.

From a conduct perspective, IIROC firms generally use technology to help the Compliance function in supervision (of trades, individuals, business locations, etc.), ensuring suitability and appropriateness of client trades, collection and maintenance of KYC requirements, and in producing information to clients such as account statements.

From a prudential perspective, IIROC firms rely on technology to ensure compliance with capital and liquidity requirements and the safeguarding of assets.



Commonly Used

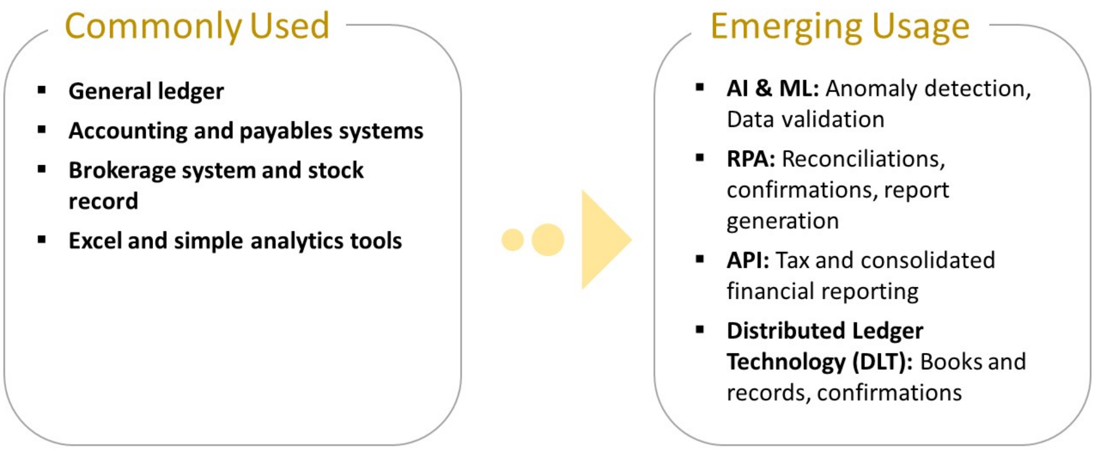
- **Communication and trade surveillance**
- **Web Crawler Software**
- **Supervision** (trades, advisors, branches)
- **Suitability and appropriateness**
- **Collection and maintenance of KYC**
- **Margining of complex products and hedges**
- **Reconciliations**

Emerging Usage

- **AI & ML:** Contract compliance, KYC/AML Utility, Fraud Detection, Client verification
- **RPA:** Regulatory compliance management, Transaction management, Margin calls, stock recalls
- **API:** KYC, Customer identification, Corporate actions

Finance & Reporting

IIROC firms have been using technology to assist in the finance and reporting functions for several years. Various systems such as general ledger accounting systems and brokerage systems are used. Excel spreadsheets and other simple analytics tools are commonly used to combine information from the various finance and reporting systems to generate complete reporting packages.



Commonly Used

- **General ledger**
- **Accounting and payables systems**
- **Brokerage system and stock record**
- **Excel and simple analytics tools**

Emerging Usage

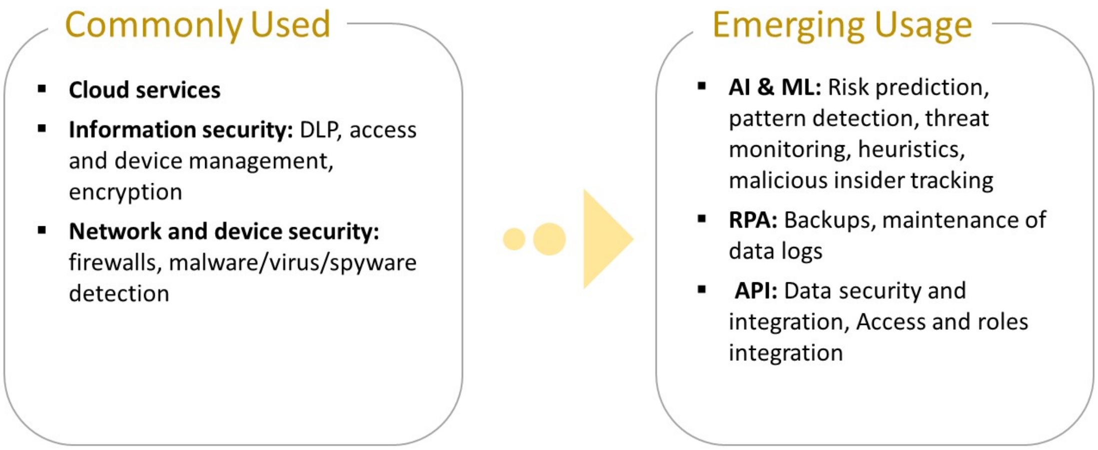
- **AI & ML:** Anomaly detection, Data validation
- **RPA:** Reconciliations, confirmations, report generation
- **API:** Tax and consolidated financial reporting
- **Distributed Ledger Technology (DLT):** Books and records, confirmations

Information Technology, Security and Management

In the recent years, IIROC firms have been implementing technology to address the risks brought on by the explosion of cyberattacks, the growth of big data and the increase in privacy regulation.

One of the fastest growing areas where technology is being implemented is in the adoption of cloud services.

Technology is also being used to help firms manage information security risks, for example for data loss prevention, access management, asset management, monitoring anomalous activity, and to protect systems and data including encryption, firewalls, anti-malware, etc.



Commonly Used

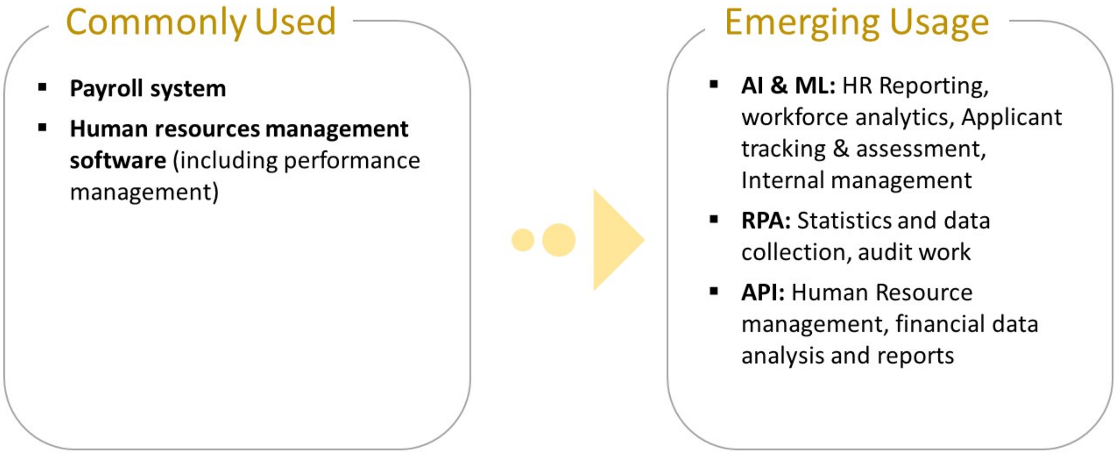
- **Cloud services**
- **Information security:** DLP, access and device management, encryption
- **Network and device security:** firewalls, malware/virus/spyware detection

Emerging Usage

- **AI & ML:** Risk prediction, pattern detection, threat monitoring, heuristics, malicious insider tracking
- **RPA:** Backups, maintenance of data logs
- **API:** Data security and integration, Access and roles integration

Human Resources, Administrative, Legal, and Other Areas

IIROC firms rely on various technologies and applications to manage their human resource and administrative functions. Most firms use technology of some kind to store human resource information including payroll, personal information, performance management, hiring, etc. The involvement of technology would depend on the size and scope of the firm. For example, payroll services are generally conducted in-house if the firms are larger or outsourced to a vendor at smaller firms.



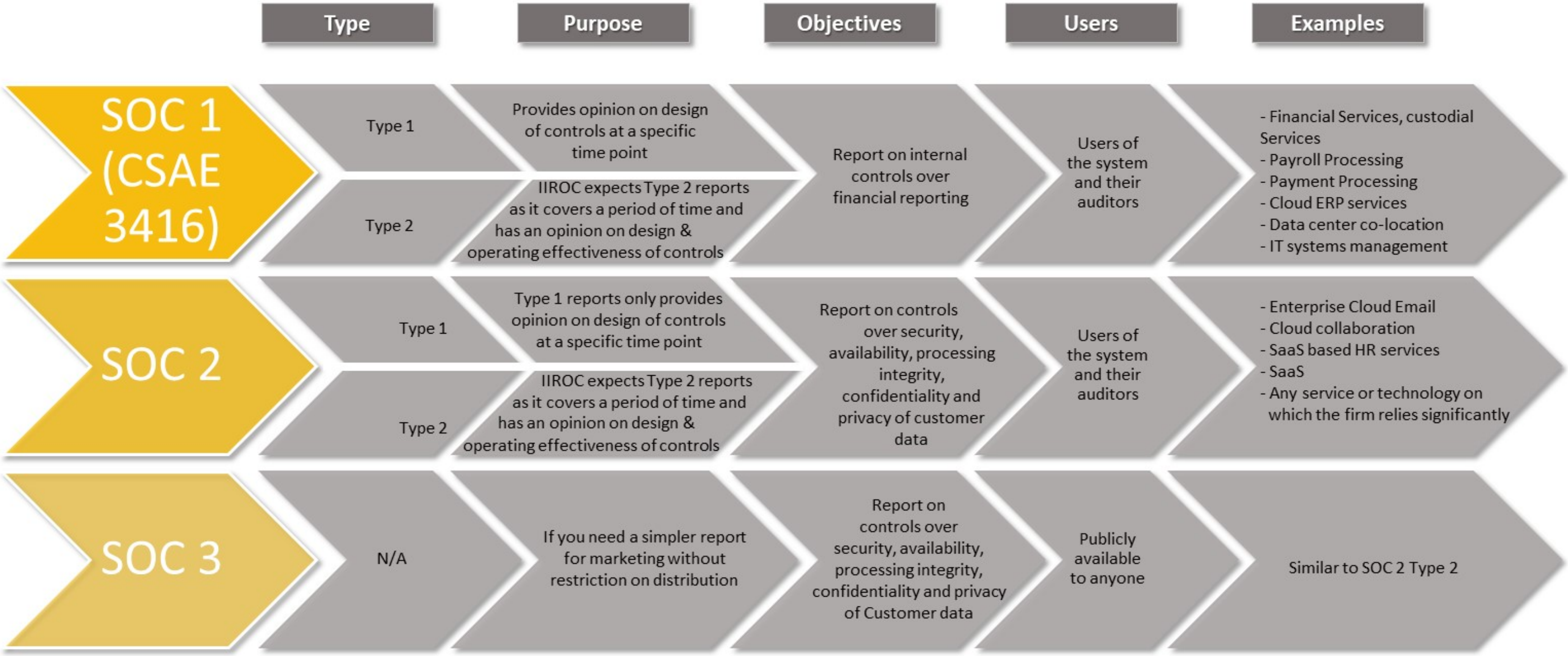
Commonly Used

- **Payroll system**
- **Human resources management software** (including performance management)

Emerging Usage

- **AI & ML:** HR Reporting, workforce analytics, Applicant tracking & assessment, Internal management
- **RPA:** Statistics and data collection, audit work
- **API:** Human Resource management, financial data analysis and reports

C. SOC Reports – A brief comparison



	Type	Purpose	Objectives	Users	Examples
SOC 1 (CSAE 3416)	Type 1	Provides opinion on design of controls at a specific time point	Report on internal controls over financial reporting	Users of the system and their auditors	- Financial Services, custodial Services - Payroll Processing - Payment Processing - Cloud ERP services - Data center co-location - IT systems management
	Type 2	IIROC expects Type 2 reports as it covers a period of time and has an opinion on design & operating effectiveness of controls			
SOC 2	Type 1	Type 1 reports only provides opinion on design of controls at a specific time point	Report on controls over security, availability, processing integrity, confidentiality and privacy of customer data	Users of the system and their auditors	- Enterprise Cloud Email - Cloud collaboration - SaaS based HR services - SaaS - Any service or technology on which the firm relies significantly
	Type 2	IIROC expects Type 2 reports as it covers a period of time and has an opinion on design & operating effectiveness of controls			
SOC 3	N/A	If you need a simpler report for marketing without restriction on distribution	Report on controls over security, availability, processing integrity, confidentiality and privacy of Customer data	Publicly available to anyone	Similar to SOC 2 Type 2

D. Glossary

Application Programming Interfaces (API)

An API is a set of functions that allows different applications to interact with each other and access data and other operating systems.

Artificial Intelligence (AI) and Machine Learning (ML)

AI is the application of computational tools to address tasks traditionally requiring human sophistication.

ML is a subset of AI that refers to technology that is self-learning / improving and can build predicted models from examples, data and experience rather than following pre-programmed rules.

Canadian Standard on Assurance Engagements (CSAE 3416)

The Canadian Standard on Assurance Engagements (CSAE 3416) addresses reporting on controls at a service organization relevant to user entities' internal control over financial reporting (CICA handbook).

Distributed Ledger Technology (DLT)

DLT refers to a consensus of replicated records shared digitally across multiple sites.

Infrastructure as a Service (IaaS)

IaaS provides virtual servers, networks, storage, and systems software designed to augment or replace data centers or individually networked computers.

On-Premise Hosting

On-premise means that a company keeps all its IT infrastructure onsite, which is managed either by themselves or a third party.

Platform as a Service (PaaS)

PaaS provides virtual servers where existing applications can be run or new ones developed without having to maintain local operating systems, server hardware, infrastructure, etc.

Risk Appetite

Total risk that a firm can bear, expressed in aggregate.

Risk Tolerance

Individual level of risk that a firm can bear, i.e., by department, activity or function.

Robotic Process Automation (RPA)

Robotic Process Automation (RPA) refers to the process of assigning manual, repetitive tasks to robotics instead of humans in order to streamline workflows in financial institutions.

Software as a Service (SaaS)

SaaS provides all the functions of a traditional application, but instead of taking up local computer resources, the functions flow through the Internet via the web browser.

Service Organization Control (SOC) Reports

SOC compliance reports cover the operations of a service organization. Refer to Appendix C for a comparison of various reports.

SSAE 18 (formerly SSAE 16)

SSAE 18 reports provide management with an independent assessment of the control procedures' adequacy and "reasonable assurance" over the processing control environment operating effectiveness that impacts user entities' internal control over financial reporting.

White Labeled/ External Solutions

White labelling is when a product or service created by one company (the producer) is then rebranded and sold by a different company (the marketer).