Guideline

Title	Integrity and Security - Guideline
Category	Sound Business and Financial Practices
Date	January 31, 2024
Sector	Banks Cooperative Credit Associations Foreign Bank Branches Foreign Insurance Branches Life Insurance and Fraternal Companies Property and Casualty Companies Trust and Loan Companies

Table of Contents

A. Overview

A1. Purpose

A2. Scope

A3. Application

A4. Key terms

A5. Outcomes

A6. Related guidelines

1. Relationship between integrity and security

2. Policies and procedures

3. Integrity

- 3.1 Character
- 3.2 Culture
- 3.3 Governance

- 3.4 Compliance

4. Security

- 4.1 Physical premises
- 4.2 People
- 4.3 Technology assets
- 4.4 Data and information
- 4.5 Third-party risks
- 4.6 Undue influence, foreign interference, and malicious activity

Appendix: Summary of expectations in Integrity and Security guideline

A. Overview

Public confidence in the Canadian financial system depends on the integrity and security of financial institutions. To this end, the *Office of the Superintendent of Financial Institutions Act* includes a requirement for OSFI to supervise financial institutions to determine that they have adequate policies and procedures to protect themselves against threats to their integrity or security, including foreign interference. Accordingly, financial institutions must take steps to ensure they are managing risks associated with integrity and security by putting such policies and procedures in place.

A1. Purpose

Set expectations for integrity and security and highlight related expectations in existing guidelines.

A2. Scope

This guideline sets out expectations for integrity and security policies and procedures. It is applicable to all federally regulated financial institutions, including foreign bank branches and foreign insurance company branches, to the extent it is consistent with applicable requirements and legal obligations related to their business in Canada.Foreign

bank branches refers to foreign banks authorized to conduct business in Canada on a branch basis under Part XII.1 of the *Bank Act*. Foreign insurance company branches refers to foreign entities that are authorized to insure in Canada risks on a branch basis under Part XIII of the *Insurance Companies Act*. Expectations for branches are set out in Guideline E-4 on Foreign Entities Operating in Canada on a Branch Basis.

A3. Application

This guideline applies on a risk basis, proportional to such factors as the institution's:

- Ownership structure, including parent-subsidiary or home office-branch relationships and relationships with related parties and large shareholders
- Business arrangements, including joint ventures and strategic alliances
- Strategy and risk profile
- Scope, nature, and location of operations

Financial institutions should consider their susceptibility to undue influence, foreign interference, and malicious activity when applying the expectations in this guideline.

Where financial institutions face obstacles to meeting expectations in this guideline (for example, local laws and regulatory expectations; limitations associated with leased premises), they should understand the risks to which they are exposed and take appropriate mitigating actions.

A4. Key terms

- **"Contractor"** is a person contracted to perform work or services for the financial institution as a non-employee (for example, self-employed persons and persons contracted through another entity such as an employment agency, among others).
- **"Foreign interference"** includes activities that are within or relating to Canada, detrimental to the interests and security of Canada, and are clandestine or deceptive or involve a threat to any person, including attempts to covertly influence, intimidate, manipulate, interfere, corrupt, or discredit individuals,

organizations, and governments to further the interests of a foreign state-or-non-state actor.

- **"Integrity"** includes actions, behaviours, and decisions consistent with the letter and intent of regulatory expectations, laws, and codes of conduct.
- **"Leader"** is an individual with people management responsibility.
- **"Malicious activity"** includes actions taken with the intent of causing harm including theft, coercion, fraud, manipulation of information or disruptions that are otherwise illegal, malicious, clandestine, or deceptive in nature. Malicious activity can originate from foreign or domestic actors and may have national security implications.
- **"Responsible persons"** include directors and senior management of financial institutions as defined in the Corporate Governance Guideline and branch management of foreign entities operating in Canada on a branch basis. Others may be considered responsible persons, based on their roles, responsibility, or influence with respect to the financial institution.
- **"Security"** includes protection against malicious or unintentional internal and external threats to:
    - real property, infrastructure, and personnel ("**physical threats**")
    - technology assets ("**electronic threats**")
- **"Undue influence"** includes situations where a person or entity engages, with malicious intent, in actions, behaviours, deception or the use of power to impact actions, decisions, or behaviours in their own or another's interests. Undue influence can originate from foreign or domestic actors and may have national security implications.

A5. Outcomes

1. Actions, behaviours, and decisions are consistent with the letter and intent of regulatory expectations, laws, and codes of conduct.

2. Operations, physical premises, people, technology assets, and data and information are resilient and protected against threats.

A6. Related guidelines

While many guidelines play a role—directly and indirectly—in enhancing the integrity and security of financial institutions, the following directly support integrity and security expectations:

- Corporate Governance Guideline
- Guideline B-10: Third-Party Risk Management
- Guideline B-13: Technology and Cyber Risk Management
- Guideline E-4: Foreign Entities Operating in Canada on a Branch Basis
- Guideline E-13: Regulatory Compliance Management
- Guideline E-17: Background Checks on Directors and Senior Management
- Guideline E-21: Operational Risk Management and Resilience
- Regulatory Notice on Culture Risk Management

1. Relationship between integrity and security

While integrity and security are distinct concepts and the outcomes of separate risk management practices, financial institutions can enhance their security by acting with integrity. For example, a lack of integrity can increase an institution's vulnerability to physical or electronic security threats. That is, failures to appropriately protect security are often rooted in failure to comply with regulatory expectations, laws, or codes of conduct.

2. Policies and procedures

Adequate policies and procedures to protect against threats to integrity or security, including foreign interference, must be established, implemented, maintained, and adhered to.

Existing policies and procedures should be assessed against expectations in this guideline and related guidelines. Effective monitoring, control, and reporting systems and procedures should be developed and maintained. Any

gaps or deficiencies should be identified, reported to senior management, and addressed. The effectiveness of policies and procedures should be demonstrable and assessed on a regular basis, including when the financial institution identifies new threats or becomes aware of new information.

3. Integrity

Outcome: Actions, behaviours, and decisions are consistent with the letter and intent of regulatory expectations, laws, and codes of conduct.

Integrity is demonstrated in actions, behaviours, and decisions that are consistent with the letter and intent of regulatory expectations, laws, and codes of conduct. It is people within organizations that take or fail to take actions and make decisions. Increasing the likelihood their behaviour demonstrates integrity can be achieved in several different ways, including by:

1. Ensuring people are of good **character**
2. Promoting a **culture** that values compliance, honesty, and responsibility
3. Subjecting actions, behaviours, and decisions to sound **governance**
4. Verifying **compliance** of actions, behaviours, and decisions with regulatory expectations, laws, and codes of conduct

Integrity is an important value in and of itself. A lack of it can damage reputation, result in fraud, cause legal issues, and increase vulnerabilities to undue influence, foreign interference, and malicious activity. Creative compliance, regulatory arbitrage, and any other measures designed to circumvent codes of conduct, regulatory expectations, or laws are not consistent with upholding the intent of the law, regulatory expectations, codes of conduct and other relevant standards and can jeopardize the integrity of the financial institution. Finally, financial risks often find their root cause in failures of integrity. Thus, enhancing integrity reduces risks to solvency and supports the overall safety and stability of a financial institution and, consequently, the financial system.

3.1 Character

Principle 1: Responsible persons and leaders are of good character and demonstrate integrity through their actions, behaviours, and decisions.

The way people behave depends to an extent on their character. Responsible persons and leaders who behave honestly and responsibly demonstrate elements of good character.

The more senior someone is in an organization, the more power and influence they typically wield. It is, therefore, particularly important that responsible persons demonstrate integrity through their actions, behaviours, and decisions.

Refer to Guideline E-17 Background Checks on Directors and Senior Management.

3.2 Culture

Principle 2: Culture that demonstrates integrity is deliberately shaped, evaluated, and maintained.

Culture influences behavioural norms, which send signals throughout an organization about what is, and is not, valued, important, and acceptable. This impacts actions, behaviours, and decisions relating to management, compliance, risk taking, issue response, and learning and growth.

Culture should be deliberately shaped, evaluated, and maintained. It should also be consistent with the financial institution's behavioural expectations of what is considered acceptable and unacceptable. This said, there is no ideal culture; sound culture depends to some extent on context. All cultures, however, should reflect a commitment to norms that encourage ethical behaviour.

Refer to Regulatory Notice on Culture Risk Management.

3.3 Governance

Principle 3: Governance structures subject actions, behaviours, and decisions to appropriate scrutiny and challenge.

Sound governance subjects actions, behaviours, and decisions to appropriate scrutiny and challenge. Effective governance builds trust with stakeholders, including shareholders, the public, employees, and regulators; it provides a structured approach to managing important risks to the financial institution.

Accordingly, important decisions around business plans, strategies, risk appetite, culture, internal controls, and oversight of senior management should be subject to effective governance.

Oversight of senior management includes setting out responsibilities and providing for accountability mechanisms.

Behavioural expectations should be codified in normative documents such as codes of conduct and conflict of interest policies and procedures. It is important to communicate expectations clearly to employees, contractors, and stakeholders, including how non-compliance issues will be addressed, resolved, and disclosed.

Codes of conduct establish and communicate behavioural expectations, apply to all employees, and include regular training.

They should highlight the importance of:

- Following the law, relevant regulatory expectations, policies, procedures, and processes
- Avoiding conflicts of interest, such as bribery and other unacceptable influences
- Maintaining objectivity and avoiding bias in decision-making processes
- Ensuring security and confidentiality of assets, communications, and information

They should cover the detection, disclosure, avoidance, and management of real, potential, and perceived conflicts of interest.

They should be assessed for effectiveness and reviewed and updated on a regular basis.

Conformity with them, including conflicts of interest, should be monitored based on risk, considering individual roles, functions, and potential exposure to undue influence, foreign interference, and malicious activity.

Refer to the Corporate Governance Guideline.

For branches of foreign banks and insurance companies, refer to Guideline E-4 Foreign Entities Operating in Canada on a Branch Basis.

3.4 Compliance

Principle 4: Effective mechanisms to identify and verify compliance with regulatory expectations, laws, and codes of conduct exist.

Compliance risk management is essential to maintaining integrity. It should ensure that compliance can be accurately and expediently verified. It should also ensure that people have effective channels to raise concerns over non-compliance with regulatory expectations, laws, and codes of conduct. Compliance includes not just adhering to the letter of such requirements, but also upholding their intent given the associated impacts on reputation and public trust.

Appropriate compliance risk management includes establishing an effective, enterprise-wide Regulatory Compliance Management (RCM) framework. This should accurately and expediently validate actions, behaviours, and decisions against applicable regulatory expectations, laws, and codes of conduct, both in letter and intent.

An RCM framework should also provide effective internal channels to raise concerns and provide constructive feedback: for example, through regular reporting and anonymous whistleblowing programs internal to the financial institution. What constitutes effective internal channels depends on the organization and its context. In all cases, channels should be regularly reviewed, updated, and brought to the attention of employees. External channels to raise concerns, such as whistleblowing programs run by government agencies or law enforcement, should also be

brought to the attention of employees.

Refer to Guideline E-13 on Regulatory Compliance Management.

4. Security

Outcome: Operations, physical premises, people, technology assets, and data and information are resilient and protected against threats.

Security includes protection against malicious or unintentional external or internal threats to real property, infrastructure, and personnel (physical threats), and technology assets (electronic threats). Such threats may arise from human error or be the unintended consequences of otherwise benign activity. They may also result from undue influence, foreign interference, or other malicious activity.

Integrity helps to reduce vulnerability to threats. In other words, security is strengthened by people with good character, a culture that is focused on sound governance and an appropriate and well-established RCM framework.

Sound operational risk management and operational resilience also reduce underlying vulnerability to threats, particularly to threats that might disrupt operations. This said, some threats, especially those arising from undue influence, foreign interference, or other malicious activities, may not cause disruption. Non-disruptive threats may require additional methods of detection and prevention to complement current operational risk management and operational resilience practices.

Accountability for security cannot be contracted out. Services performed by third parties should be subject to appropriate risk management measures.

Policies and procedures governing all types of threats, internal and external, should be established and maintained and consider threats associated with undue influence, foreign interference, or malicious activity. They should be assessed for effectiveness, reviewed, and updated on a regular or ongoing basis.

The threat environment, including as it relates to third parties, should be assessed, and internally reported at least annually, with security precautions implemented to protect physical premises, people, technology assets, and data and information.

Refer to Guideline E-21 Operational Risk Management and Resilience.

4.1 Physical premises

Principle 5: Physical premises are safe and secure and monitored appropriately.

Standards and controls should be adopted to govern access control and monitoring of:

- Physical buildings and office spaces, including assets, storage, and equipment contained within those spaces
- Any areas where sensitive work or discussions may occur

Technical security inspections should be conducted to protect physical and digital assets, including periodic sweeps for covert surveillance, listening, or tracking devices. The scope and frequency of such inspections should be carried out in a manner that aligns with the threat environment.

Refer to Guideline B-13 Technology and Cyber Risk Management and Guideline E-21 Operational Risk Management and Resilience.

4.2 People

Principle 6: People should be subject to appropriate background checks, and strategies should be put in place to manage risk.

Security standards and controls to protect people from undue influence, foreign interference, and malicious activity should be established and maintained. Subjecting people to appropriate background checks can identify

vulnerabilities to these factors, helping to develop strategies to minimize risks. Standards and controls should consider factors such as authority, seniority, and access to sensitive information.

4.2.1 Background checks

Responsible persons, employees, and contractors should be subject to appropriate, risk-based background checks that are:

- Conducted prior to employment
- Renewed on a regular basis
- Reviewed off-cycle based on certain criteria

At a minimum, appropriate checks include verification of identity and background but frequently include:

- Education and professional credentials
- Personal and professional references

In addition, at a minimum, responsible persons and employees and contractors occupying higher-risk positions should be subject to:

- Criminal records checks
- Financial inquiries (credit checks)

OSFI may request that specific individuals of the financial institution obtain a higher level of security clearance, depending on roles and responsibilities.

Refer to Guideline E-17 Background Checks on Directors and Senior Management.

4.3 Technology assets

Principle 7: Technology assets should be secure, with weaknesses identified and addressed, effective defences in place, and issues identified accurately and promptly.

Threat actors can disrupt, destroy, damage, access, modify, and maliciously use technology assets. Such incidents may result in financial loss and reputational damage and harm to depositors and policyholders and may have national security implications. The intensity of defences established should be proportional to the likelihood of threats and the severity of impact to the financial institution and their employees, clients, and other stakeholders should the technology asset be compromised.

Refer to Guideline B-13 Technology and Cyber Risk Management.

4.4 Data and information

Principle 8: Data and information should be subject to appropriate standards and controls ensuring its confidentiality, integrity, and availability.

Data security, including confidentiality, integrity, and availability, should be maintained. Requirements and protections should be defined and established throughout the data lifecycle, with controls in place for data at rest, in transit, and in use.

Structured and unstructured data should be adequately identified, classified, and protected based on personnel access requirements. When classifying data, its vulnerability to malicious activity, undue influence, or foreign interference should be considered. Standards and controls for data protection should define personnel access requirements to sensitive data. Mechanisms to identify and escalate unauthorized access to data by people or systems should be put in place. The intensity of defences established should be proportional to the likelihood of threats and the severity of impact to the financial institution and their employees, clients, and other stakeholders should the data be compromised.

Refer to Guideline B-13 Technology and Cyber Risk Management and Guideline E-21 Operational Risk Management and Resilience.

4.5 Third-party risks

Principle 9: Third parties should be subject to equivalent and proportional measures to protect against threats.

Accountability for security of the financial institution rests with the financial institution, even as it relates to business outsourced to third parties. This includes threats posed by undue influence, foreign interference, or malicious activity.

Not all third-party arrangements pose the same level of risk to the financial institution's security. Due diligence on the third party from an integrity and security perspective should be proportional to the third party's access to the financial institution's physical premises, people, technology assets, and data and information.

Based on that initial proportionality assessment, the following should be assessed before engaging a third party and on an ongoing basis thereafter:

- The likelihood of threats to the third party
- The ability of the third party to address threats
- The existence and adequacy of the third party's policies and procedures protecting against threats
- The adequacy of the third party's background check processes

In relation to foreign interference, the following information about the third party and its subcontractors should also be considered:

- Location of operations
- Location of corporate headquarters
- Connections to foreign governments
- Ownership structure

It is also important to ensure that processes for the selection of third parties are objective, reducing the potential for bias, undue influence, or foreign interference.

Refer to Guideline B-10 Third-Party Risk Management.

4.6 Undue influence, foreign interference, and malicious activity

Principle 10: Threats stemming from suspected undue influence, foreign interference, and malicious activity should be promptly detected and reported.

Measures should be put in place for the prompt detection of threats and their careful investigation, ensuring, among other things, appropriate limits on access to information, confidentiality, and the independence and integrity of the investigation.

Financial institutions are encouraged to report to the appropriate authorities, including the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, when there are reasonable grounds to believe that an incident or event has occurred related to undue influence, foreign interference, or malicious activity. OSFI should be informed immediately of any such communications.

Detected incidents and events, including those deemed not to meet the threshold of reporting to OSFI or other authorities, should be documented and inventoried by the financial institution as part of the management reporting process to senior management.

Appendix: Summary of expectations in Integrity and Security guideline

Summary of expectations - Integrity

Principle	Associated OSFI guidelines	New expectation	Expanded expectations
1. Responsible persons and leaders are of good character and demonstrate integrity through their actions, behaviours, and decisions.	E-17 Background Checks on Directors and Senior Management	Not applicable	Character of responsible persons as demonstrated through their actions, behaviours, and decisions.
2. Culture that demonstrates integrity is deliberately shaped, evaluated, and maintained.	Regulatory Notice on Culture Risk Management	Not applicable	Culture reflects a commitment to norms that encourage ethical behaviour.
3. Governance structures subject actions, behaviours, and decisions to appropriate scrutiny and challenge.	Corporate Governance Guideline E-4 Foreign Entities Operating in Canada on a Branch Basis	Not applicable	Governance that provides oversight of actions, behaviours, and decisions. Behavioural expectations are codified in normative documents such as codes of conduct and conflict of interest policies and procedures.
4. Effective mechanisms to identify and verify compliance with regulatory expectations, laws, and codes of conduct exist.	E-13 Regulatory Compliance Management	Not applicable	Compliance that focuses on not just the letter of requirements but also the intent. Effective channels, such as whistleblowing programs, to raise concerns over non-compliance.

Summary of expectations - Security

Principle	Associated OSFI guidelines	New expectation	Expanded expectations
5. Physical premises are safe and secure and monitored appropriately.	B-13 Technology and Cyber Risk Management Guideline E-21 Operational Risk Management and Resilience	Standards and controls for physical buildings, office spaces, physical file storage, and technical security inspections.	Not applicable
6. People should be subject to appropriate background checks, and strategies should be put in place to manage risk.	E-17 Background Checks on Directors and Senior Management	Risk-based background checks on all employees and contractors, as appropriate to the role.	Not applicable
7. Technology assets should be secure, with weaknesses identified and addressed, effective defences in place, and issues identified accurately and promptly.	B-13 Technology and Cyber Risk Management	Not applicable	Enhanced description of what constitutes malicious actions towards IT infrastructure.
8. Data and information should be the subject of appropriate standards and controls ensuring its confidentiality, integrity, and availability.	B-13 Technology and Cyber Risk Management Guideline E-21 Operational Risk Management and Resilience	Data classification considers vulnerability to malicious activity, undue influence, or foreign interference.	Personnel access requirements to prevent undue influence and foreign interference.

Principle	Associated OSFI guidelines	New expectation	Expanded expectations
9. Third parties should be subject to equivalent and proportional measures to protect against threats.	B-10 Third-Party Risk Management	Third-party risk management is conducted through an integrity and security lens and is proportional to the third party's access to the financial institution's physical premises, people, technology assets, and data and information. Transparent and objective procurement processes.	Not applicable
10. Threats stemming from suspected undue influence, foreign interference, and malicious activity should be promptly detected and reported.	E-13 Regulatory Compliance Management	Notification to OSFI when a report is made to RCMP, CSIS, or other authorities regarding undue influence, foreign interference, or malicious activity.	Not applicable