Whistleblower Policy (Enterprise-wide)

June 2022

Document Metadata and Version Control	
Effective Date	June 1, 2022
Approval Date	May 25, 2022
Document Type	Policy
Version Number	7.02
Review Frequency	Annual
Status	Renewal
Replace	Whistleblower Policy (Enterprise-wide) October 2020
Applicable Entities	Bank of Nova Scotia
Approval Authority	Board of Directors 5/25/2022
Policy Sponsor	Paul Baroni, EVP and Chief Auditor
Policy Owner	Laurel Pollard, VP Audit Professional Practice
Content Manager	Dwayne Hobbs, Director Whistleblower & Conduct
Advice and Counsel	Frances Fitzgerald, VP & Associate General Counsel
Key Changes	The Policy has been amended to meet the requirements of the Financial Consumer Agency of Canada (FCAC) Whistleblower Guideline published March 2022, effective June 30, 2022.
Metadata for GRM RO&R tracking	
	[This section to be completed by Content Manager]
Issuing Legal Entity	Bank of Nova Scotia
Country, Region	Global
Issuing Functional Group	Audit
Principal Risk or subset	Compliance Risk
Document Required by Regulation	Yes Bank Act (Canada) Sarbanes-Oxley (US) Dodd-Frank (US) FCAC Whistleblower Guideline
Next Approval Date	October 2022

1 Introduction

1.1 Purpose

The Bank of Nova Scotia (the "Bank") has established channels through which employees can Raise a Concern to ensure that matters are reported and addressed. The Whistleblower Policy, (the Policy), as part of the larger Raise a Concern framework, enables employees to raise Concerns through a confidential and anonymous channel and provides the framework for how the independent and objective Whistleblower Program within the Audit Department will receive, assess, investigate and resolve Concerns, particularly when those Concerns constitute wrongdoing.

The Whistleblower Program is designed as a control to safeguard the integrity of the Bank, and its subsidiaries, financial reporting, its business dealings and to support adherence to the Scotiabank Code of Conduct (the Code) and its regulatory obligations. The Policy governs the operations of the Bank's Whistleblower Program that enables individuals to raise anonymous and confidential Concerns and wrongdoing that may otherwise not be known to management and ensure appropriate and impartial investigation is undertaken.

1.2 Scope

The Policy applies to all individuals in the Bank to whom the Scotiabank Code of Conduct applies, inclusive of employees, officers, directors, and contingent workers. External or third parties may also be Reporters and will be afforded protection from retaliation consistent with the Bank's obligations under the law.

1.2.1 *Entity and Geographic Scope*

This Policy is applicable to the Bank on an enterprise-wide basis including its domestic and international branches and agencies and directly or indirectly wholly owned and controlled subsidiaries of the Bank.

Each directly or indirectly wholly owned or controlled subsidiary of the Bank has its own board of directors, which may include senior officers of the Bank, and who has the responsibility to satisfy itself that appropriate frameworks, policies, and procedures are in place for the subsidiary. The subsidiary's senior management has responsibility to ensure policies comply with local regulatory requirements and it is expected that a subsidiary's board of directors or senior management will either adopt and ratify (with or without an addendum as appropriate), or approve a subsidiary-specific policy that aligns, in all material respects, with that of this Policy, as appropriate.
From time-to-time the Bank and subsidiaries may have recent acquisitions or situations where control of a subsidiary has been recently established. In these situations, there may initially exist a lack of conformity to the policies outlined in this document. The Bank will in these cases assess any deficiencies and develop an action plan to ensure they are rectified on a timely basis.

Refer to Appendix "C" for information on Subsidiary Policy Governance for this document.

1.2.2 *Activities covered by this Policy*

The Policy provides information on reporting wrongdoing or Concerns as part of the whistleblower process. Reporting can be done confidentially through several channels, including an independent third-party hotline/website that allows for anonymous reporting. It is in the interest of all stakeholders of the Bank that such Concerns be reported so that they can be appropriately addressed.

2 Policy Principles/Requirements

The Whistleblower Program supports adherence to the Code of Conduct as individuals can report potential or actual Concerns/Wrongdoing. Examples of Wrongdoing include Breaches of the Code of Conduct such as:

- ***Failing to follow the Law, such as the Bank Act (Canada)*** (Principle 1)
- ***Breaches of internal Policies and Procedures*** (Principles 2 through 5)
- ***Failure to honour our commitments to the communities in which we operate*** by failing to meet the Bank's voluntary Codes of Conduct or Public Commitments (Principle 6)
- ***Reporting Retaliation***. All individuals who are governed by the Scotiabank Code of Conduct are obligated to report any act to harm or intention to harm anyone for reporting wrongdoing. Examples are statements, conduct or actions involving terminating, disciplining, demoting, suspending, harassing, intimidating, coercing or discriminating against an individual reporting wrongdoing in good faith in accordance with this Policy.

2.1 Subject Principal Risks and /or Requirements

A trusted, effective and responsive Whistleblower Program is critical to support the management of risks:

- Legal & Compliance Risk, including Conduct Risk
- Reputational Risk
- Operational Risk
- The requirement to protect Whistleblowers is central to the effective execution of the Policy. As stated in the Code, the Bank will protect from retaliation any individual who raises issues or reports Concerns in good faith in accordance with the methods described in the Code. Retaliation against any individual who raises a Concern, in good faith, is not tolerated.

2.2 Regulatory Obligations

The primary regulatory obligations covered by this policy are:

- Bank Act (Canada) Part XVI.1 Sections 979.1 through 979.4 which defines wrongdoing, retaliation and the requirement for the Bank to establish a mechanism for employees to report

wrongdoing for the purposes of investigation and resolution.

- Sarbanes-Oxley Section 301 describes the responsibility of the Audit Committee to establish a method for employees to report internal fraud, auditing and accounting Concerns and whistleblower retaliation for investigation and resolution.
- Other relevant obligations include Financial Consumer Agency Act (Canada), the FCAC Whistleblower Guideline, Dodd-Frank Act (US), Volcker Rule, Financial Conduct Authority Handbook (UK) and the Prudential Regulatory Authority Rulebook (UK) which place regulatory scrutiny on consumer protection provisions, aspects of market abuse, define accountability and how particular categories of Concerns or protected disclosure should be managed within the Bank.

3 Policy Program Description

The Bank takes all Concerns seriously and will investigate all Reasonable Complaints. The third-party independent Hotline/web-portal allows the Reporter to provide additional information required by the investigations on an anonymous basis. **Reporters are asked to provide as much information as possible (including who, what, where and when).** The quality and completeness of the report has a direct impact on the timeliness and scope of investigations.

Reporters using the third-party reporting system are encouraged to record the Case Number and PIN so they may remain engaged to respond to questions from investigators and to ultimately receive notification that the matter has been closed.

There are several channels through which individuals may report wrongdoing or otherwise raise Concerns. Employees should choose the channel that is most appropriate given the nature of their Concern. The reporting options are described in the Raise a Concern tab available of the Scotiabank Live intranet site. Employees, including employees of third parties who sell or further the sale of Bank products are encouraged to seek advice on the Raise a Concern and Whistleblower processes from the Staff Ombuds (staff.ombudsman@scotiabank.com) at any point in the process. All other reporters may contact the Office of the President.

3.1 Principles

The program is designed to be:

3.1.1 *Effective*

The Whistleblower Program is designed to ensure that all concerns raised through the channel are assessed, investigated when appropriate and tracked to conclusion.

3.1.2 *Accessible*

The Whistleblower channel at Scotiabank.EthicsPoint.com is available 24/7 on a global basis. Reports may be filed either using the web platform or by speaking to a Communication Specialist from the 3rd party service provider. Online reports can be submitted in English, French or Spanish. Hotline callers are able to submit reports in over 20 languages including English, French and Spanish.

3.1.3 *Safe & Secure*

In addition to the option to report concerns anonymously, other controls exist to safeguard whistleblowers and the process, including logical access and strict confidentiality protocols. Reports are redacted of Personally Identifiable Information when escalation is required. Retaliation against individuals raising concerns is prohibited by the Code of Conduct.

3.2 Examples Of Wrongdoing

Wrongdoing includes breaches of the law, the Code of Conduct, policies and procedures or failure to meet any voluntary codes of conduct or public commitment of the Bank. Specific examples of wrongdoing included in the Employee Misconduct and Consequence Management Policy are Conflicts of Interest, Honesty & Integrity Violations, Confidentiality and Security of Assets, Treatment and Retaliation.

3.3 Whistleblower Program Reporting Channels

Scotiabank has established a mechanism for confidential and anonymous submission of reports through an independent third party. This channel is best suited to those wishing to remain anonymous as it creates a secure, controlled, impartial and safe means of communication between the Whistleblower Program Office and the Reporter. This independent third party provides a hotline and a website (scotiabank.ethicspoint.com) that are accessible 24 hours a day, 7 days a week in all countries in which the Bank operates.

Individuals calling the hotline from Canada or the United States can call 1-800-443-0312.

If a report is submitted anonymously, the identity of the individual raising the Concern through the hotline or website (together the hotline) is not known to the Bank. The Reporter will be provided with a confidential PIN number that will allow for further anonymous communication through the Hotline. The Reporter will receive an initial response from the Whistleblower Program office within 5 working days of the initial report. The length of the investigation is contingent on the scope, complexity and nature of the Concern raised.

Reports of wrongdoing or Concerns that are raised through the Hotline are submitted to the Chair of the Audit & Conduct Review Committee (ACRC) and/or the Bank's Chief Auditor to ensure independent review and investigation.

In addition, Whistleblower Concerns may be raised as follows:

3.3.1 *Scotiabank Global Compliance.*

Regulatory compliance Concerns can be raised to globalcompliance@scotiabank.com. and questions or Concerns related to the Code should be directed to Conduct.Risk@scotiabank.com.

3.3.2 *Directly to Audit.*

Concerns may be raised in writing directly to a VP within Audit or a country Chief Auditor via email or other correspondence. This may be done on an anonymous basis.

3.4 External Reporting

Bank employees may report concerns to certain regulators directly, where channels are available. For example, in Canada, employees may submit concerns to the Commissioner of the FCAC or the Superintendent of OSFI. Employees may also contact law enforcement agencies in their jurisdiction where warranted.

3.5 Emergencies

The Whistleblower program is not equipped to address urgent matters related to physical security and immediate dangers to the health and safety of customers, employees or property. Emergencies should be reported to Corporate Security through the Security Operations Centre at 416-866-5050 or CS.SOC@bns.scotiabank.com.

3.6 Customer Complaints

As the hotline and web reporting portal are publicly available it is possible that customers may make use of the Whistleblower channel to raise Concerns. When a report is assessed as a customer complaint and not a report of wrongdoing, these matters will be escalated to the appropriate Business Line or Corporate Function stakeholders for investigation and remediation.

3.7 Disclosures

Notwithstanding the Bank's obligation to protect the anonymity of individuals who raise Concerns, there are circumstances where the identity of these individuals, when known, will be shared with Regulators at their request or if otherwise required by law or regulation. Disclosures of this nature will be approved by General Counsel. Disclosures to a Regulator will be made using Registered Confidential means including secure data transfer in order to safeguard the identity of a Reporter. The Reporter will be notified of this disclosure by the Whistleblower Program Office, using the same means by which the Reporter filed their initial report.

3.8 Risk Program Activity / Outcome

3.8.1 Escalation

Individuals who have Concerns, inclusive of wrongdoing, are required to report, normally to their direct manager or someone in their reporting chain. If escalations are not addressed or the circumstances warrant, individuals should escalate through a Raise a Concern channel as appropriate. The Whistleblower channels allow for anonymous reporting. This ensures that all potential risks are identified and escalated to the appropriate levels for remediation. If you are a People Manager who has received a Concern that cannot be resolved, you are encouraged to raise the Concern through the appropriate Raise a Concern channel, including as the Whistleblower Program. Individuals receiving anonymous letters with allegations of wrongdoing should similarly escalate.

3.8.2 Investigation & Adjudication

All Whistleblower reports that are received through the Hotline are first directed to the Bank's Chief Auditor and his/her respective delegates (together **"Primary Recipients**"). Upon receipt of a report, the Primary Recipients will jointly ~~evaluate~~ assess the severity of the Concern to determine whether a concern constitutes wrongdoing and whether an internal or external investigation is required.

The Primary Recipients will then assign the investigation accordingly and maintain oversight of the investigation to ensure appropriate and timely resolution. All investigations are conducted according to the Bank's investigative standards or Audit Methodology.

3.8.3 Remediation

The Whistleblower Program Office will work with the stakeholder Business to develop action plans to monitor and remediation control weaknesses, address wrongdoing and recommend appropriate disciplinary action to address open risk in accordance with the Bank's Employee Misconduct Consequence Management Policy. In some circumstances the Audit Department may open and track Audit Issues in accordance with Audit Methodology.

3.9 Regulatory Compliance

Where an allegation concerns a potential breach of a consumer protection provision, an investigation will take place to determine if the claim can be substantiated. If the allegation is substantiated, Global Compliance or the Compliance Office of the impacted Business Line or Corporate Function will receive a report summary and will determine whether the matter requires regulatory disclosure. If disclosure of the matter to a regulator is deemed necessary, such disclosure will reference that the Bank was made aware of the matter through a Whistleblowing report.

3.10 Reporting

3.10.1 *To the ACRC*

- Concerns assessed as being higher risk will be raised to the Chair of the ACRC either by the Chief Auditor or directly by Navex.
- The Chief Auditor will report quarterly, or more frequently as required, to the ACRC on the results of investigations of Concerns.
- Regulatory compliance matters of a significant nature can be reported to EVP, Chief Compliance Officer for further escalation as required.

3.10.2 *To Executive Management*

- The Chief Auditor may report the results of investigations where allegations of wrongdoing have been substantiated to executive management with responsibility for the area concerned, as appropriate. This will be done in order to advise them of the disposition and/or to ensure appropriate resolution of the Concern.

3.10.3 *To the Individual raising the Concern.*

- The status/resolution of the investigation will be communicated to the individual, where possible. If the Concern was raised through the Hotline, the Primary Recipients or a delegate will post the status/resolution on the Hotline, which can be accessed anonymously by the Reporter.
- When an investigation is complete, the individual will receive a response from the Whistleblower Program Office indicating that the matter has been investigated, adjudicated and that the case file has been closed. Whistleblowers have no entitlement to receive investigation reports or to otherwise be informed of the actions taken by Management to address a Concern, especially as it relates to disciplinary action against other employees.

3.10.4 *To the Compensation Review Committee*

- If the Subject of a Concern is found to have violated the Scotiabank Code of Conduct, the details of the wrongdoing will be reported to the Compensation Review Committee or the appropriate local committee as appropriate.

3.10.5 *Global Compliance (Enterprise Risk Culture & Conduct Risk).*

- On a quarterly basis, the Whistleblower Program Office will report aggregated data to Global Compliance for inclusion in the quarterly Conduct Risk report. A subset of this data will be provided to Business Lines upon request.

3.10.6 *To Subsidiary Chief Auditors*

- Chief Auditors of Subsidiaries will receive reporting for the purposes of reporting to Subsidiary Boards of Directors as required by law or regulation.

4 Roles and Responsibilities

Role	Responsibilities
First Line of Defense ("1st LoD")	
1A & 1B	
Business Lines	• Responsible for communicating and reinforcing the Policy. • Ensure that Concerns which constitute wrongdoing raised through their internal channels are directed to the Whistleblower channel for investigation and resolution as appropriate. • Support the investigation of Concerns reported through the Whistleblower Program when requested to do so and take appropriate steps to ensure the anonymity of individuals concerned, the confidentiality of allegations and that no retaliatory action is taken because of a disclosure. • When and as appropriate, responsible for executing action plans to remediate or correct any control weaknesses identified, as well as, address employee misconduct through established channels.
Second Line of Defense ("2nd LoD")	
Global Compliance	• Responsible for communicating and reinforcing the Policy. • Provide advice and counsel to the Whistleblower Program office. • Ensure that Concerns which constitute wrongdoing raised through their internal channels are directed to the Whistleblower channel for investigation and resolution as appropriate. • Support the investigation of Concerns reported through the Whistleblower Program when requested to do so and take appropriate steps to ensure the anonymity of individuals concerned, the confidentiality of allegations and that no retaliatory action is taken because of a disclosure. • When and as appropriate, responsible for executing action plans to remediate or correct any control weaknesses identified, as well as, address employee misconduct through established channels. • Ensure the collection and dissemination of conduct related data and metrics under the mandate of the Organizational Behavior & Ethics Committee. • Oversee the reporting of Regulatory Compliance Issues arising from Whistleblower reports
Third Line of Defense ("3rd LoD")	
Audit	• Accountable to ensure that Whistleblower allegations are appropriately investigated and reported to the Audit and Conduct Review Committee of the Bank and Executive Management as appropriate.

4.1 Reporting Examples

The following chart simplifies options for reporting Concerns. Notwithstanding these recommendations, **individuals always retain the option to report Concerns to the Whistleblower channel when retaliation is possible.** The Staff Ombuds Office can provide advice about how a Concern could be raised.

Type of Concern	Recommended Channel
Concerns of People Managers about their employees	Escalate within normal channels. There is no requirement to file a whistleblower Concern.
Workplace Concerns such as harassment and discrimination or Occupational Health & Safety Concerns	Employee Relations
Advice about Human Resource policies, staffing, promotions	AskHR
Wrongdoing by someone who is not an employee, director, officer, contingent working or third party operating on behalf of the Bank	Corporate Security 416-866-5050 or email CS.SOC@bns.scotiabank.com.
Emergencies that threaten customers, employees and Bank assets	
Concerns related to Regulatory Compliance	globalcompliance@scotiabank.com
Questions about the Code of Conduct	Conduct.Risk@scotiabank.com.
Any Concern that has already been raised with management or through another channel for which no action has been taken	Whistleblower
Breaches of the Law	
Breaches of the Code of Conduct	
Breaches of Internal Policies and Procedures	
Retaliation or threat of retaliation for raising a Concern	
Money Laundering	
Market Abuse: Insider trading, front-running, breaches of securities laws	
Bribery & Corruption	
Auditing & Accounting Concerns	
Privacy Breaches or Misuse of Confidential Information	
Improper Sales Practices (violations of consumer protection laws, failing to gain customer consent, misrepresentation)	
Internal Fraud	

5 Policy Exceptions and Escalation

There are no exceptions to the Policy.

Appendix A Terms and Acronyms

Terms and Definitions

Key Terms	Definition
ACRC	Audit & conduct Review Committee (of the Bank of Nova Scotia)
Concern	A matter of interest or importance. Refer to the Raise a Concern Guide.
Content Manager	The person responsible for the development and updating of the Policy or document and works on behalf of the Policy Owner.
Contingent Worker	Agency workers where Scotiabank has a contract with an agency who is the employer of a worker or has retained a worker who is assigned by the agency to provide services to Scotiabank; Independent contractors, where Scotiabank has entered directly into a contract with an individual (or the company owned by an individual) to provide services to Scotiabank directly; and / or Service provider workers, where Scotiabank has entered into a contract with a company to provide services to Scotiabank or to complete a project for Scotiabank.
FCAC	Financial Consumer Agency of Canada
OSFI	Office of the Superintendent of Financial Institutions
Policy Owner	The custodian of a Policy document who is responsible for the development, update, maintenance and communication of such document.
Policy Sponsor	The executive who is ultimately responsible for the Policy document and who advocates the development, approval and enforcement of such document. In Executive Office, minimum of a Senior Vice President level. In subsidiaries, it may be a Vice President level.

Primary Recipients	The group of individuals who can receive and respond to reports from the third-party service provider, inclusive of the EVP & Chief Auditor, SVP Internal Audit, VP Audit Professional Practice, VP Enterprise Conduct & Ethics within Global Compliance and the Whistleblower Program Office.
Program Owner(s)	The individual who is responsible for the development of required supporting tools, processes and procedures that facilitate the operationalization of specific practices, activities and controls to manage risk. This may also include executing the risk program associated with managing the risk.
Reasonable Complaints	All Concerns are assessed by the Whistleblower Program Office for credibility and risk. Concerns should be made in good faith or in the interests of public good. If doubt exists, the Whistleblower Program Office will seek clarification from a Reporter. If a Concern is raised about a matter that has previously been documented, no investigation may be required.
Recipient	Individuals impacted by the Policy, or officers representing teams impacted by the Policy, or officers representing subsidiaries (hereafter referred to as "Recipient subsidiaries") that are expected to align their own practices to the Policy. Not all Recipients will necessarily be Stakeholders.
Report	Any Concern that has been escalated and documented by a Raise a Concern channel.
Reporter	Any individual who has raised a Report, inclusive of employees, directors, officers and contingent workers. External or third parties may also be reporters and will be afforded protection from retaliation consistent with the Bank's obligations under the law.
Retaliation	Any act that harms or intends to harm an individual in order to supress reporting of wrongdoing, refusing to do anything that would be reasonable considered to be wrongdoing or otherwise take steps to prevent wrongdoing from occurring. Examples of retaliation include dismissal, suspension, demotion, discipline, harassment or any act that disadvantages an individual inclusive of denying an employment benefit.
Stakeholders	Individuals or groups that are consulted in the policy development and update phases. Not all Stakeholders will necessarily be Recipients.
Whistleblower	A subset of Reporters who raise Concerns through the Whistleblower channel
Whistleblower Program	The combination of policies, people, process and technology that enable reporting, assessment, assignment, investigation, adjudication, remediation and reporting of Concerns that

	constitute wrongdoing It is managed by the Whistleblower Program Office who is accountable to the EVP & Chief Auditor.
Wrongdoing	The subset of Concerns that could reasonably be considered any act, or intention to act, that would constitute a breach of the Scotiabank Code of Conduct, an internal policy or procedure, the law, or any voluntary code of conduct or public commitment made by the Bank.

Appendix B Subsidiary Policy Governance

Each subsidiary's board of directors has the responsibility for overseeing that appropriate frameworks, policies and procedures exist for their respective subsidiary or group of subsidiaries. To assist the subsidiary board in carrying out this responsibility, subsidiary senior management has responsibility to assess the applicability of this Policy for adoption or alignment, in all material respects, by the subsidiary.

It is expected that a Recipient subsidiary's board of directors or senior management will adopt and ratify this Policy, as appropriate for the jurisdiction. However, if there are differences in local regulatory/statutory requirements, and/or local best practices, these differences should be documented in an addendum, unless a separate subsidiary-specific policy is required by the local regulator. Such subsidiary-specific policy, to the extent practical, should be aligned, in all material respects, with that of this Policy, as applicable.

Subsidiary Assessment

Upon receipt of this Policy, a Recipient subsidiary should assess how the Policy impacts and aligns with the subsidiary's local practices and processes based on the type and scale of its operations, risks and controls, local legal and regulatory requirements and local best practices.

a. Subsidiaries should determine the applicability of the Policy to their local operations and complete a gap analysis as appropriate. If the Policy is not applicable, advise the Policy Owner.
b. Subsidiaries should adopt the Policy, as applicable to their circumstances, and have it ratified by an appropriate approval authority.
c. The subsidiary should consult with the Policy Owner and/or subject matter expert for Advice and Counsel when an addendum (subject to Addendum discussion below) or a local document will be utilized.

Subsidiary Options

1. Addendum

Should a Recipient subsidiary decide to adopt this Policy then an addendum may be appropriate. An addendum leaves the Policy in full force and effect and only replaces the specific section(s) set forth in the addendum. An addendum is required when local legal, regulatory, and/or organizational requirements conflict, or are absent from this Policy. Subsidiaries should not amend the Policy. Instead, they should create a separate Addendum, if required.

Addendums must be approved by the applicable local governing body (e.g., subsidiary board or management committee/senior management) subject to Advice and Counsel by the Policy Owner, and/or subject matter expert.

Where required (refer exceptions below under Advice and Counsel), Recipient subsidiaries that develop an addendum should submit it, to the appropriate Operating Parent

representative or Policy Owner, for Advice and Counsel prior to local approval. When approving an addendum, the Enterprise Policy must also be presented for adoption.

2. Subsidiary-Specific Policy

Where this Policy does not cover specific organizational or regulatory requirements, and an addendum is not considered appropriate, a subsidiary-specific policy may be created which should be based on the type and scale of the subsidiary's operations, controls, and local legal and regulatory requirements. In particular:

a. Where a subsidiary-specific policy is developed in the place of this Policy, Advice and Counsel by the Policy Owner, and/or subject matter expert should be obtained prior to local approval.
b. Where a subsidiary-specific policy is addressing a local legal or regulatory requirement or local best practice, Advice and Counsel may not be required (refer Advice and Counsel below for exceptions). However, the Enterprise Policy Owner should be provided a copy of the subsidiary-specific policy and where it has potential global implications (e.g. privacy, cyber security), the relevant risk subject matter expert at Executive Offices must be consulted.
c. Subsidiaries may supplement this Policy with additional documentation that is required by their regulators, boards, or senior management, or as required to operationalize this Policy. However, the supplementary documentation, to the extent applicable, should not contradict the requirements in this Policy. Such supplements should be sent to the Policy Owner, or their delegate, for information.

Subsidiaries should consult with the Policy Owner for those situations that are not covered by the above standards.

Advice and Counsel

The requirement for Advice and Counsel applies to all Recipient subsidiaries of the Bank. In jurisdictions outside Canada, Executive Office should generally provide Advice and Counsel to the Operating Parent subsidiary. While the Operating Parent subsidiary is to provide advice and counsel to all its related subsidiaries, there may be instances where it is appropriate for the Policy Owner to provide Advice and Counsel directly to a regulated Recipient subsidiary.

Advice and Counsel is not required for**:**

- Amendments for administrative (e.g., reporting or policy review frequency), minor organizational (e.g., Committee and Executive titles) changes, and other non-substantive changes
- Amendments to align with, and/or address, local regulatory requirements

Subsidiary Acknowledgement

An acknowledgment from Recipient subsidiaries to the Policy Owner from an executive level individual or designate is required. It is up to the Policy Owner to determine the appropriate form and tracking of the acknowledgement. Ultimately, the Policy Owner is required to monitor and track receipt of all required acknowledgements.

Subsidiary Renewal Cycle

Subsidiary-specific Policies and addendums to this Policy should be updated annually unless local laws, regulatory requirements, or process changes require more frequent updates. Subsidiary-specific Policies should be presented to local Boards for renewal every 2 years. Subsidiaries are required to communicate the Addendum to all local staff, following its approval be the local board

A subsidiary should align the timing of the update of their subsidiary-specific policies, development of a new policy/local addendum, to the extent possible, within 4 months of the effective date of this Policy, unless a later transition date has been agreed with the Policy Owner.

Appendix B.1 Subsidiary Acknowledgement Form

Set out below is a suggested Subsidiary Acknowledgement Form for use by Recipient subsidiaries which can be returned to the Policy Owner, or their delegate, as applicable.

Subsidiary Information

Policy Name: [Insert name of Enterprise Policy]

Subsidiary: [Parent Subsidiary]

Additional Subsidiaries: [List subsidiaries of the parent subsidiary for acknowledgment]

Contact: [Identify parent subsidiary contact person for the respective policy]

Executive Responsible: [Identify executive responsible for acknowledgment sign off]

Acknowledgement

I acknowledge that the [Insert name of Enterprise Policy] has been received, read and actioned*, as appropriate in relation to the subsidiaries identified above in the following manner (Tick one box below):

- ☐ **Enterprise Policy Not Applicable to Subsidiaries**
- ☐ **Adoption**
- ☐ **Adoption with an Addendum****
- ☐ **Develop a Subsidiary-specific Policy****

Rationale:

*** Action(ed) refers to the Recipient subsidiary conducting an assessment of the applicability of the policy and submitting the necessary documentation (Policy, addendum or Subsidiary-specific Policy) for adoption and/or approval at the appropriate level within the Recipient subsidiary. Refer to Section 2.6 and 2.7 of the Policy Management Standard for further guidance.**
**** Include a brief description of rationale for the addendum or Subsidiary-specific policy. Note, may require Advice and Counsel, refer Appendix C in the Policy Management Standard.**

Executive Sign-Off

Name:	**Title:**
Signature:	**Date:**

Appendix D Governance of Document

Maintenance

The Policy is reviewed and updated annually, and presented to the Board for approval every two years, or more frequently if there is a material change, using the following process:

- The Audit Department, as the Policy owner, reviews regulatory standards, industry best practices and effectiveness of the reporting channels and investigation procedures to determine whether any changes to the Policy are required, and updates the Policy accordingly;
- The updated draft of the Policy is circulated to relevant stakeholders for review as necessary; The updated Policy is presented to the ACRC of the Board and the Board of Directors for review and approval; and
- The approved Policy is distributed to appropriate business units for awareness, including global subsidiaries. Communication of the policy to employees is also conducted through the annual acknowledgement and certification of adherence to the Code.

Approval Authority

Role	Governance Responsibility
Approval Authority: Board of Directors	• Reviews and approves the Policy before becoming effective or where applicable, approves its retirement • Review periodic reports, as applicable
Policy Sponsor: EVP & Chief Auditor	• The executive who is ultimately responsible for the Policy and who advocates the development, approval and enforcement of the Policy • Assists in socializing new/updated Policy with relevant executive /senior management, as necessary • Provides sign-off of the draft Policy before submitting the Policy to the Approval Authority

Roles and Responsibilities

Role	Responsibility
Senior Management Organizational Behaviour & Ethics Committee	• Where applicable, the executives or committees' review and provides input on the Policy prior to its submission to the Approval Authority • Provides overarching governance and oversight to promote consistency across the Bank

Role	Responsibility
Policy Owner: VP Audit Professional Practice	• Custodian, maintenance, development, and approval of the Policy; Oversees the execution of the communication plan • Conducts a needs assessment and makes recommendations on developing new, material amendments or retiring a Policy • Oversees the work and drafts prepared by the Content Manager for the consultation process • Confirms which subsidiaries should be sent the Policy (i.e. Recipient subsidiaries listing) • Provides Advice and Counsel to Recipient subsidiaries, where necessary • Reviews and recommends the Policy for approval • Advisor in determining what supporting tools, procedures and job aids are necessary • Reviews and approves housekeeping or administrative changes.
Content Manager Director Whistleblower & Conduct	• Updates or develops Policy based on changes in organizational structure, internal processes, industry best practices, and regulatory developments and revises the text accordingly • Consults relevant Stakeholders for input and feedback on drafts • Maintains a Stakeholder tracking chart • Reviews and assesses input from Stakeholders; advises Policy Owner where material input has not been accepted • Notes items to be brought forward for next update • Maintains custody and ensures all key drafts are retained • Prepares the draft Summary of key changes, as needed, for review by Policy Owner, Policy Sponsor and Approval Authority • Develops and executes the Communication Plan • Ensures the Policy document is translated, as required • Responds to queries from Stakeholders and Recipients • Ensures the approved document is stored in the appropriate repository • Forwards the published Policy to Archives Information Management Office (AIM) to archives@scotiabank.com. • Forwards the published Policy to GRM Risk Oversight & Reporting. Mailbox is GRM RO&R Policy & Framework at Documentation.Repository@scotiabank.com
Stakeholders: Enterprise Conduct & Ethics, Global Compliance Corporate Security Employee Relations	• Provide review and input into the development and periodic update of the Policy including identification of the potential impact of the Policy to a Business Line, corporate function, Recipient subsidiary, etc. as appropriate. Refer section 2.3.2 of the Policy Management Standard • Assist with the execution of the communication plan for their respective areas

Role	Responsibility
Staff Ombuds Office Employee Law Group	
Recipient Subsidiaries	• Adapts Policies as relevant to their activities, scope and jurisdiction. Refer to Appendix C (or whatever the appendix above gets labeled, no need to reference the Standard you have it above), Subsidiary Policy Governance • Seek Advice & Counsel from the Policy Owner, subject matter expert, as appropriate, for addendums and subsidiary-specific Policies • Operating Parent provides Advice & Counsel for its subsidiaries on relevant Policies or Addendums • Returns Subsidiary Acknowledgement Form or equivalent evidence to Policy Owner

Communication Plan

The Whistleblower Policy should be read in conjunction with the Code of Conduct so communication of this policy must occur concurrently and in parallel with the release of the Code of Conduct as directed by Global Communications and Global Human Resources. The Policy will be sent to the Archives and Information Management Office and GRM RO&R Policy and Framework Mailbox.

This Policy will be included in the Raise a Concern page of Scotiabank Live, posted to Scotiabank.com with the Scotiabank Code of Conduct and will be included at www.gcs-whistleblower.com. The Policy will be posted in English, French and Spanish.

Implementation (for new and updated policies)

This Policy is effective June 1, 2022. The existing mechanisms and technology used to implement the Policy will remain in effect with no material changes.

Training will be provided in the form of the Annual Code of Conduct Acknowledgement. Additionally, select employees and third parties (involved in sales activities within Canada) will require additional training related to new consumer protection provisions. Employees involved in the detection and investigation of wrongdoing will receive ongoing training through individual training plans guided by the needs of their roles consistent with existing procedures.

Reference Material

This Policy refers to, and should be read in conjunction with, the following documents:

Code of Conduct

- Scotiabank Code of Conduct
- Raise a Concern Guide
- Raise a Concern Process
- Conduct Risk Management Policy
- Risk Culture & Conduct Risk Management Framework (upon approval)
- Global Human Rights Statement
- Global Investigations Standard
- Conduct Risk Management Policy
- Anti-bribery & Anti-Corruption Policy
- Employee Misconduct Consequence Management Policy
- Global Sales Conduct Management Policy

External Documents

- Bank Act (Canada)
- Dodd-Frank Act (US)
- Sarbanes-Oxley (US)
- FCA Handbook (UK)
- PRA Rulebook (UK)
- Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos (Resolución SBS N° 272-2017 (Peru)
- Section 1317AI – Corporations Act Australia
- FINANCIAL INVESTMENT SERVICES AND CAPITAL MARKETS ACT (Korea)
- Whistleblower Protection Act (Japan)

- RBI Framework for dealing with loan frauds dated May 7, 2015 (India)
- MAS Guidelines on Individual Accountability and Conduct (Singapore)
- Hong Kong Monetary Authority Supervisory Policy Manual: Code of Conduct, CG-3 Reporting Channel (Hong Kong)

External Reporting

The Financial Consumer Agency of Canada contact information can be found at https://www.canada.ca/en/financial-consumer-agency/corporate/contact-us.html.

The Office of the Superintendent of Financial Institutions contact information can be found at Contact Us (osfi-bsif.gc.ca).