ESCALATION POLICY

Summary	The Escalation Policy sets forth requirements on who needs to escalate, what to escalate, when to escalate, the parties to whom to escalate, and how to follow up on escalations. It includes roles and responsibilities for the identification, investigation and resolution of Concerns and Incidents, as described herein. It also sets forth requirements for tracking and reporting of significant Incidents, as described herein, and Severity Level 1 or 2 Issues under the Assessment, Issue, and Corrective Action Plan Policy ("AICAP Policy").		
Scope/Target Audience	This Policy applies to Citigroup Inc. ("Citigroup") and its consolidated subsidiaries, including Citibank, N.A. ("CBNA") (collectively, referred to as "Citi" or "Company"). The target audience for this Policy is all Citi employees. Temporary employees, consultants, contractors, secondees, third party service providers, and other types of third parties (collectively, "non-employees") may be contractually obligated to follow Citi policies. In such cases, non-employees are responsible for adhering to this Policy.		
Changes Since Last Version	Edits include language related to: • handling of Sensitive and Confidential Matters • governance Escalation Grid • monthly continuous improvement analysis • Legal Entity responsibilities • occurrences escalated or reported outside of the central significant Incident escalation process • Nigeria Whistle-blowing Addendum		
Owner	Chief Compliance Officer, Governance and Policy		
Owner Group	Independent Compliance Risk Management		
Principal Contact	John Whittaker		
Replaces	Version 4.0		
Aligned Documents	N/A		
Risk Category	L0: Compliance Risk	L1: Governance & Prudential Risk	L2: Governance Risk

Document ID No.:	8555
Issue Date:	12/21/2015
Revision Date:	12/11/2020
Effective Date:	12/11/2020
Version No.:	5.0
Original Language:	English

TABLE OF CONTENTS

Contents

1 INTRODUCTION / OBJECTIVE

1.1 OBJECTIVE

1.1.1 Citi has established this Escalation Policy ("Policy") for the prompt and consistent identification, escalation, reporting and resolution of Concerns or Incidents, as described herein.

1.1.2 This Policy sets forth requirements on who needs to escalate, what to escalate, when to escalate, the parties to whom to escalate, and how to follow up on escalations. It includes roles and responsibilities for the identification, investigation and resolution of Concerns or Incidents.

1.1.3 It also sets forth requirements for tracking and reporting of significant Incidents, as defined herein, and Severity Level 1 or 2 Issues under the AICAP Policy to Management Governance Committees and, as determined by those committees, the relevant Legal Entity Board, or Board Committee, and, where appropriate, to Citigroup Inc. or Citibank, N.A. Board of Directors or committees thereof ("Board" or "Board of Directors").

1.2 EFFECTIVE DATE / TRANSITION PERIOD

1.2.1 The Policy revision is effective immediately except as follows:

- Escalation Channels, businesses and functions will implement new or revised operating processes by December 31, 2020.
- Each Escalation Channel, business and function will revise, as appropriate, Policies, Standards, Procedures, and Other Documents that reference escalation or incident management to conform to the revised Escalation Policy by December 31, 2020.
- Each Escalation Channel, Business[1] and Function will revise, as appropriate, Procedures to support these revisions by April 30, 2021.

1.3 RELATED POLICY DOCUMENTS

1.3.1 This Policy is a revision of the previous version of the Escalation Policy and supersedes all previous versions. Key related global documents include, but are not limited to, the following:

- Code of Conduct
- Global Disciplinary Review Policy
- Assessment, Issue, and Corrective Action Plan Policy
- Operational Risk Management Policy
- Business, Risk and Control Committee Guidelines
- Global Regulatory Reporting Policy

[1] GCB and ICG including each unit within their businesses

- Risk Governance Framework
- Policy Governance Policy
- Fraud Risk Management Policy
- ICRM Procedures for Products and Functions
- Global AML Issue Escalation Standard
- Global Sanctions Significant Issue Escalation Standard
- Markets Conduct Issue Tracking Procedure

1.4 DISPENSATIONS AND WAIVERS

1.4.1 Requests for waivers and dispensations must be submitted in writing and approved by the Policy Owner in accordance with the Policy Governance Policy and implementing Standards and Procedures. Requests must include supporting documentation, identify the local law/regulation and describe compensating controls and/or corrective action plans to comply with the requirements of the Policy.

1.4.2 Waivers must be reapproved every 12 months. Requests for an extension must be in writing to the Policy Owner or delegate, confirm that there are no changes to the circumstances supporting the exception, include details of the current status of controls, and describe the progress of the corrective actions and/or effectiveness of compensating controls, where applicable.

1.5 BOARD APPROVAL/BOARD REPORTING

1.5.1 Board approval is not required for this Policy except as follows. The Australia Addendum must be approved by the Citigroup Pty Ltd Board of Directors.

1.6 GOVERNANCE

1.6.1 This Policy is owned by the Chief Compliance Officer, Governance and Policy. This Policy, and material amendments to this Policy, must be approved in writing by the Owner or his/her designee. The Australia Addendum (Appendix D) and any substantive revision of the Addendum must also be approved by the CBNA Sydney Branch Senior Officer outside Australia.

1.6.2 The Chief Compliance Officer, Governance and Policy will oversee execution of the Policy and provide direction and oversight regarding Policy Document architecture, development and management to Citi's Businesses and Functions to develop Policies, and their implementing Standard and/or Procedures.

1.6.3 The Policy owner will assess the Policy effectiveness and report policy assessment metrics in accordance the Policy Governance Policy.

1.6.4 Business and Function implementing Standards and/or Procedures must be reviewed and approved in accordance with the Policy Governance Policy.

2 POLICY PROVISIONS – ALL EMPLOYEES

2.1 INTRODUCTION

This Policy sets forth requirements on who needs to escalate, what to escalate, when to escalate, the parties to whom to escalate, and how to follow up on escalations. Key principles are outlined in this section.

2.2 WHAT AN EMPLOYEE MUST ESCALATE

2.2.1 Employees[2] must promptly escalate compliance risk concerns related to: (i) violations or potential violations of applicable law, rule, or regulation ("Violations"), or breaches of applicable Policy, Standard or Procedure[3] ("Breaches"), including Violations or Breaches resulting from Misconduct as defined in this paragraph, (ii) behavior that is a departure from industry or other applicable standard of conduct (whether external or internal), (iii) breaches of Citi's Code of Conduct or other ethical standard[4], or (iv) deliberate avoidance or manipulation of controls ((ii) – (iv) collectively "Misconduct"), regardless of the significance or severity. Items (i) – (iv) are collectively defined as "Concerns" for the purposes of this Policy.

2.2.2 Employees need not determine the significance or severity of Concerns, rather, employees must escalate all Concerns, regardless of the level of severity.

2.2.3 Escalation must never be a substitute for employees making decisions that they are authorized to make or for effective discussion and decision-making. In addition, employees can seek guidance from their managers, others in their management chain, or from supporting functions. These interactions are not considered "escalations" for purposes of this Policy.

2.2.4 The table in Appendix A lists examples of some of the types of Concerns to escalate. This list is not exhaustive; other types of Concerns require escalation in line with established escalation procedures.

2.3 TIMELINESS OF ESCALATION

2.3.1 The early recognition and prompt escalation of Concerns is key to mitigating risk. Employees who become aware of Concerns must promptly escalate them. It may be

[2] The target audience for this Policy is all Citi employees. Temporary employees, consultants, contractors, secondees, third party service providers, and other types of third parties (collectively, "non-employees") may be contractually obligated to follow Citi policies. In such cases, non-employees are also responsible for adhering to this Policy.
[3] As defined by the Policy Governance Policy
[4] Including but not limited to codes of conduct related to professional licenses

necessary to escalate prior to all the facts and risks being fully known, but an employee must have an articulate basis for escalating the Concern.

2.3.2 If an employee knowingly fails to promptly escalate a Concern, they may be subject to disciplinary action, up to and including termination of employment.

2.4 HOW AND TO WHOM AN EMPLOYEE NEEDS TO ESCALATE

2.4.1 The first point of contact to escalate is each employee's direct manager.

2.4.2 In the event that a potential conflict of interest exists that may bias the manager's perspective or willingness to act, or if the direct manager is the subject of or implicated in the Concern, an employee is permitted to instead escalate directly to their manager's manager. In addition, employees are permitted to escalate directly to an Escalation Channel (refer to section 2.5). An employee who is uncertain as to which is the appropriate Escalation Channel is permitted to escalate to any Escalation Channel of their choosing.

2.4.3 Certain jurisdictions maintain local disclosure procedures that appoint a specific person for this purpose. Employees in those jurisdictions can escalate directly to that person.

2.5 ESCALATION CHANNELS TO WHICH AN EMPLOYEE CAN ESCALATE

2.5.1 Managers, persons appointed in accordance with Section 2.4.3 and others to whom an employee escalates must promptly further escalate to one of the following Escalation Channels, in accordance with its scope of authority and responsibility (see Appendix A):

- Human Resources ("HR") Concerns: Escalate directly to HR, Employee Relations, or Labor Relations.
- Compliance Concerns: Escalate to Independent Compliance Risk Management ("ICRM") Officer.
- Security, internal fraud-related and physical violence-related Incidents: Escalate to Citi Security and Investigative Services ("CSIS").
- Ethics Office: Employees can always escalate Concerns to the Citi Ethics Office.
- In addition to the above, concerns related to legal or litigation exposure should be brought to internal legal counsel ("Legal").

Contact information for these Escalation Channels can be found in Appendix B.

2.5.2 Concerns related to threats or acts of violence, including domestic violence that impact the workplace or employees, must be promptly escalated to CSIS or HR. In addition, if an employee is contacted directly by law enforcement with an inquiry related to a threat, an act of violence or an ongoing internal fraud Concern, the employee must forward the inquiry to either CSIS or Legal. If an employee is contacted directly by law enforcement or a regulator with an inquiry concerning

anything else, including but not limited to legal or regulatory Concerns, the employee must forward the inquiry to Legal.

2.5.3 Citi encourages employees to escalate Concerns openly. However, Concerns can be escalated to the Citi Ethics Office anonymously to the extent permitted by applicable laws and regulations. See Appendix B for Ethics Office contact information. Employees who wish to escalate Concerns anonymously must not provide their names or other identifying information when submitting a Concern. If an employee chooses to remain anonymous and does not provide a means to contact him/her, Citi may be unable to obtain the additional information needed to investigate or address the Concern. Escalations ought to, therefore, provide as much detailed information as possible. Including specific information, such as the business or function, location, individuals, transactions, events, and dates involved to enable a more effective investigation. When employees choose an anonymous escalation option, Citi encourages those employees to check back through the anonymous Escalation Channel so that they can provide more information if requested.

2.6 POST-ESCALATION EMPLOYEE PROTOCOL

2.6.1 It is the responsibility of the employee to follow up on an escalated Concern, if an employee is aware or has reason to believe that a Concern they have escalated to their manager or Escalation Channel is not being acted upon. In such instances, they must further escalate to one of the Escalation Channels referenced in section 2.5, or to another member of their management chain.

2.7 PROHIBITION ON RETALIATION

2.7.1 As set forth in the Code of Conduct, employees who escalate Concerns in good faith will not be subject to adverse consequences for escalating their Concerns. Citi prohibits retaliatory action against individuals who escalate Concerns or questions in good faith or participate in a subsequent investigation of such Concerns. Retaliation is a serious issue and includes any adverse action taken because an employee has engaged in such activity. As part of any investigation, Citi respects the rights afforded under applicable laws and regulations to all parties related to the Concern.

2.7.2 Every manager is responsible for creating a work environment free of retaliation, and is held accountable for the behavior of employees under their supervision. Employees who engage in retaliation against a colleague because he or she has escalated a Concern or question in good faith or for participating in an investigation may be subject to disciplinary action, up to and including termination of employment or other relationship with Citi, in accordance with the Citi Global Disciplinary Review Policy, and local Policies or Procedures that apply.

2.8 EMPLOYEE DISCLOSURES TO A GOVERNMENT, REGULATORY OR SELF-REGULATORY AGENCY

2.8.1 Nothing contained in this Policy prohibits or restricts an employee from voluntarily disclosing confidential information to a government, regulatory, or self-regulatory agency as required by local jurisdiction regulations, including, but not limited to, under Section 21F of the U.S. Securities Exchange Act of 1934 and the rules thereunder, or from disclosing confidential information, including trade secrets, to a government official or an attorney in connection with the reporting or investigation of a suspected violation of law or to an attorney or in a court filing under seal in connection with a retaliation or other lawsuit or proceeding, as permitted under Section 7 of the Defend Trade Secrets Act of 2016. Employees do not need prior permission from Citi to raise such Concerns, and employees are not required to notify Citi after doing so.

2.9 EMPLOYEE PARTICIPATION IN INVESTIGATIONS

2.9.1 Employees might be asked to participate in appropriately authorized investigations of Concerns. All employees must cooperate fully with internal or external investigations. Employees with knowledge of an escalated Concern or investigation must appropriately safeguard information relevant to the Concern within their possession or control.

2.9.2 Employees must never withhold, destroy, tamper with or fail to communicate relevant information or records in connection with an investigation. Employees must also maintain and safeguard the confidentiality of an investigation to the extent possible, including in Section 2.9.1, or by applicable law, except as otherwise provided herein. Employees must not make false statements to or otherwise mislead internal or external auditors, investigators, legal counsel, Citi representatives, regulators, or other governmental entities. Doing so may be grounds for disciplinary action, up to and including termination of employment and may also be subject to criminal prosecution.

3 POLICY PROVISIONS – ESCALATION CHANNELS, BUSINESSES AND FUNCTIONS

3.1 ESCALATION CHANNEL PROCESSES

3.1.1 Each Escalation Channel maintains a process to (1) refer Concerns that are outside of its area of direct responsibility to the appropriate Escalation Channels and/or area for further investigation, (2) handle escalated Concerns in accordance with their function's investigation (if applicable), Concern management and escalation processes and procedures, and (3) report Concerns, as appropriate, in line with Citi's governance framework.

3.1.2 **HR**: Each HR representative to whom an HR Concern (see Appendix A for examples of HR Concerns) is escalated must determine whether the Concern is within its area of responsibility and whether it is significant. HR Concerns are investigated by:

- Human Resources Professional Services, Employee Relations, Labor Relations or other HR representative or
- Another appropriate Escalation Channel (e.g., Legal, CSIS, ICRM) working in conjunction with HR.

Once investigated, HR Concerns are referred to Disciplinary Committees to the extent required by Citi's Global Disciplinary Review Policy.

Significant HR Concerns must also be promptly reported to the ICRM Central Incident Escalation Team, taking into account relevant sensitive and confidential information considerations as well as legal privilege when applicable in accordance with HR Escalation Procedures. Sensitive or confidential significant HR Concerns will be reported directly to the Head of HR and the Chief Compliance Officer.

3.1.3 **Legal**: Legal's primary role within Citi is to act as a provider of legal services to the businesses and other functions, including the Escalation Channels. Each Lawyer to whom a legal or litigation matter is escalated must handle it appropriately, in line with the practices of the Legal Department and such lawyer's legal judgment. Lawyers must also refer Incidents and Concerns escalated to them to the appropriate Escalation Channel for resolution in accordance with the requirements of this Policy. On a regular basis, the Chief Compliance Officer meets with the General Counsel to discuss sensitive legal matters and various areas of mutual interest or significance. At least quarterly, the General Counsel reports to the Board of Directors on the most significant litigations in accordance with Legal Department Escalation Procedures

3.1.4 **ICRM**: Each ICRM representative to whom a Concern is escalated must determine whether the Concern is within its area of responsibility and escalate to their respective managers as appropriate. ICRM is responsible for assessing the Concern and determining whether it constitutes a compliance risk incident.

A compliance risk incident ("Incident") is an occurrence that has led to or may lead to an adverse compliance consequence, which may put Citi, its employees, customers or other stakeholders at risk. Incidents fall into the following Governance, Risk & Compliance ("GRC") Risk Categories: Money Laundering Risk, Sanctions Risk, Bribery Risk, Market Practices Risk, Customer/Client Protection Risk or Governance & Prudential Risk. In addition, Incidents include violations of applicable laws, rules or regulations or Policy breaches in any GRC Risk Category and Misconduct.

Other non-compliance risk incidents, such as operational risk incidents, technology risk incidents and compliance risk incidents communicated by compliance assurance, internal audit, external audit, or a regulator managed in the regular course of business, are not covered by this Policy. Occurrences escalated or reported outside of the central significant Incident escalation process may still be escalated via the compliance escalation process based on ICRM Executive Management Team's ("EMT") judgement.

Criteria for Assessing Significance

ICRM is responsible for assessing the Incident and determining the appropriate GRC Risk Category and whether it is significant, with support from Risk Category and ICRM subject matter experts, Businesses and Global Functions. Criteria for assessing significance[5] needs to take into account the following factors:

- Incidents, including actual violations of applicable legal, regulatory or Policy requirements:
  - That could result in a Level 1 or Level 2 Issue or have a High or Medium-High breadth of impact, in accordance with the issue severity rating as defined by the AICAP Policy, or
  - That may result in losses and events greater than $25MM, or
  - Which represent material breaches potentially impacting the safety and soundness of Citi or deemed to potentially cause substantial harm, including a substantial impact on business objectives, reputation or strategy.

In addition to the minimum standards described above, the following areas maintain risk specific criteria and protocols in their associated Standards and/or Procedures:

- Anti-Money Laundering: Global AML Issue Escalation Standard
- Sanctions: Global Sanctions Significant Issue Escalation Standard
- Anti-Bribery: Anti-Bribery Executive Management Team Charter
- Markets Conduct: Markets Conduct Issue Tracking Program

ICRM Products and Functions Compliance maintains the ICRM Escalation Procedure, which includes procedures for the escalation of compliance risk.

When an Incident is determined to be a significant compliance risk Incident, it must be promptly escalated to the ICRM Central Incident Escalation Team for escalation to the Chief Compliance Officer, ICRM management, and the Risk Category Subject Matter Expert.

Quarterly, the Chief Compliance Officer reports to the Global BRCC and the Board Audit Committee on significant Incidents and severity level 1 and 2 Issues in the aggregate, in accordance with selected themes and narrative information regarding individual concerns.

3.1.5 **CSIS:** Concerns that are escalated or referred to CSIS are subject to a prompt initial analysis to determine whether CSIS is the appropriate recipient and, if so, whether it requires investigation, in accordance with CSIS's established criteria. Once a Concern is referred for investigation, it must be communicated to other Escalation Channels and key stakeholders, as appropriate. Those Concerns that are not within the purview of CSIS are routed to the appropriate Escalation Channel in accordance with CSIS Escalation Procedures. CSIS provides a report of the most significant cases (Cases of Significance Report), based on CSIS's investigative procedures and established criteria, to members of the Executive Management Team, comprising direct reports of the Chief Executive Officer. In addition, CSIS must promptly report significant cases to the ICRM Central Incident Escalation Team, taking into account relevant sensitive and confidential information considerations as well as legal privilege when applicable in accordance with CSIS Escalation Procedures. Sensitive or confidential significant CSIS Concerns will be reported directly to the Chief Compliance Officer.

3.1.6 **Ethics Office**: The Ethics Office receives Concerns via the Citi Ethics Hotline. The Ethics Office reviews Concerns received and either refers them to the appropriate area (such as HR, Global Public Affairs, or customer service) for further handling and resolution, or assigns them to an investigative function for investigation.

3.1.7 Regardless of the Escalation Channel receiving the Concern, each must ultimately be routed to the appropriate area for investigation, resolution and reporting. Therefore, each Escalation Channel is responsible for promptly referring Concerns that falls outside its area of direct responsibility or that they are unable to handle appropriately, to the appropriate Escalation Channel. It is also not unusual for a Concern to implicate more than one Escalation Channel, e.g., Human Resources and ICRM; in that event, the Concern must be brought to the attention of each appropriate Escalation Channel so it can be addressed and escalated in accordance with their respective responsibilities.

---

[5] Where the term "significant" or "significance" is used throughout this document, reference the section on Criteria for Assessing Significance

3.2 ICRM CENTRAL SIGNIFICANT INCIDENT REPORTING

3.2.1 The ICRM Central Incident Escalation Team is responsible for receiving significant, or potentially significant, compliance risk Incidents from the Escalation Channels for consolidation, tracking and prompt reporting to ICRM senior management.

3.2.2 The ICRM Central Incident Escalation Team must aggregate and promptly report significant, or potentially significant, compliance risk Incidents received from the Escalation Channels to the Chief Compliance Officer and ICRM senior management.

3.2.3 On a monthly basis, the ICRM Central Incident Escalation Team will report significant, or potentially significant, compliance risk Incidents to the first, second and third lines of defense.

3.2.4 The ICRM Central Incident Escalation Team will also submit significant, or potentially significant, compliance risk Incidents for incorporation into the governance reporting processes.

3.3 INCIDENT AND ISSUE MANAGEMENT

3.3.1 If an Incident is determined to be an Issue (as described in Section 3.3.2), the appropriate Issue Owner, as defined in the AICAP Policy, is responsible for making an initial determination of the severity level of the Issue. They must do so by applying the severity level ratings and criteria set forth in the AICAP Policy, in consultation with Human Resources, Legal, ICRM, and/or other areas, in their discretion, as useful. Issues that warrant individual attention and remediation must be entered in iCAPS (as defined in the AICAP Policy).

3.3.2 An Incident becomes an Issue when the assessment of the Incident concludes a business or function is unable to mitigate risk to an acceptable level due to the inadequate design, ineffective execution or absence of an appropriate control in accordance with how Issue is defined within the AICAP Policy.

3.3.3 In the event that an Issue has been entered into iCAPS prior to the identification of a related Incident, the existence of the Issue does not negate an employee's responsibility to escalate the Incident in accordance with the requirements of this Policy.

3.3.4 Descriptions of significant Incidents and severity level 1 and 2 Issues must take into account relevant sensitive and confidential information considerations as well as legal privilege when applicable. Questions about whether the description or escalation of an Incident must be modified due to these concerns must be referred to Legal, Human Resources, and/or the Ethics Office, as applicable. See also Appendix C for further guidance on handling of sensitive and confidential escalation matters.

3.3.5 Significant Incidents and severity levels 1 and 2 Issues must be reported to the appropriate Management Committees in accordance with this Policy. Those

individuals or management meetings to which significant Incidents or severity level 1 and 2 Issues are escalated prior to the reporting to a BRCC are able to revise the severity level as additional facts and further consideration may warrant.

3.3.6 Businesses and Functions need to identify the legal entity or legal entities impacted by the Incident to facilitate reporting as needed to each Legal Entity's regulator (which may be different from those of Citi's principal global regulators).

3.4 REPORTING TO MANAGEMENT COMMITTEES

3.4.1 Ultimately, significant Incidents and severity level 1 and 2 Issues must be reported to the appropriate Management Committees subject to the severity level applied to the Incident (Legal Entity, Regional, Country and Business/Functional) and, as necessary, to the Board of Directors, for the purpose of good governance. The role of these Committees is described in Section 4, below.

3.5 CONTINUOUS IMPROVEMENT MONITORING

3.5.1 On a monthly basis, the ICRM Central Incident Escalation Team performs analysis on a sample of Level 1 and 2 Issues to assess whether significant Incidents were appropriately escalated prior to becoming Issues, or that there is appropriate rationale as to why not, as not all Issues will have an associated Incident. The results of the analysis are documented and communicated to members of the three lines of defense to promote continuous improvement of the escalation processes.

3.6 REPORTING TO REGULATORS

3.6.1 Citi must identify and report significant Incidents to be brought to the attention of the appropriate regulator(s) in a consistent and timely manner. Reporting must comply with the reporting requirements for Incidents that are applicable to the specific Legal Entity regulator, which can be different from those of Citi's principal global regulators.

3.6.2 Reporting efforts must be coordinated, to the extent practicable, with others who are engaged with a particular Incident. Coordinated reporting promotes efficiency and avoids duplication of efforts for our regulators and for Citi. See also the Global Regulatory Reporting Policy.

3.7 CONFIDENTIALITY

Descriptions and escalations of significant Incidents and severity level 1 and 2 Issues must take into account relevant sensitive and confidential information considerations as well as legal privilege when applicable. If an Escalation Channel, business, or function is aware that an Incident is the subject of a litigation or legal investigation, they must consult with Legal regarding appropriate escalation and investigation of the Incident. Questions about whether the description or escalation of an Incident must be modified due to these concerns must be referred to Legal, Human Resources, and/or the Ethics Office, as applicable. See also Appendix C for further guidance on handling of sensitive and confidential escalation matters.

4 ROLES & RESPONSIBILITIES

4.1 ALL EMPLOYEES (FIRST, SECOND THIRD LINE AND CONTROL/SUPPORT UNITS) MUST

- Promptly escalate Concerns, regardless of the significance or severity of the Concern, to their managers or otherwise to an Escalation Channel.
- Cooperate fully with internal or external investigations as called upon to do so.
- Safeguard information within their possession and control that is relevant to a Concern.
- Maintain and safeguard the confidentiality of an investigation to the extent possible, except as otherwise provided by applicable law.
- Further escalate the Concern if the employee is aware that it is not being acted upon.
- Promptly escalate any instance of retaliation for having raised a prior Concern.

4.2 MANAGERS (FIRST, SECOND AND THIRD LINE) MUST

- Handle and resolve Concerns arising within areas of their direct responsibility, assuming no conflict of interest.
- Consult with their manager on additional escalation required based on their respective business or function escalation procedures.
- Promptly escalate Concerns to the appropriate Escalation Channel.
- Promptly escalate Violations or Breaches related to Compliance Risk Incidents to ICRM.
- Handle Concerns in the best interest of the Citi franchise, and where applicable, Citibank N.A. or other legal entities, including those outside of their area of responsibility.
- Inform the Policy Owner or Policy Contact if they reasonably believe that a Policy has been breached.
- Encourage employees to feel comfortable escalating Concerns and see to it that employees under their direction are aware of all resources available for seeking advice or reporting an Incident, including the Citi Ethics Office.
- Refrain from engaging in or tolerating retaliatory acts against anyone working on Citi's behalf.
- Clearly communicate to their teams Citi's prohibition of workplace retaliation.

4.3 CITI SECURITY AND INVESTIGATIVE SERVICES MUST

- Refer Concerns escalated to them that are outside of their area of direct responsibility or that they are unable to handle appropriately to the appropriate Escalation Channel.
- Independently investigate alleged, suspected or actual internal fraudulent activities, Cyber Security Incidents (also known as Information Security Incidents or SIRTs), incidents related to physical violence and other incidents that are the subject of an escalation or referral.
- Conduct CSIS investigations in accordance with the CSIS Investigation Procedures.
- Assess the level of significance of incidents escalated to them, using the significance criteria set forth in the CSIS Investigation Procedures.

- Provide a report of the most significant cases (Cases of Significance Report) to members of the Executive Management Team, comprising direct reports of the Chief Executive Officer.
- Promptly report significant cases to the ICRM Central Incident Escalation Team.
- Report sensitive or confidential significant CSIS Concerns directly to the Chief Compliance Officer.
- Maintain Escalation Channel specific procedures to support the Escalation Policy.
- Train relevant employees necessary to support execution of CSIS escalation procedures.

4.4 HR MUST

- Refer Concerns escalated to them that are outside of their area of direct responsibility or that they are unable to handle appropriately to the appropriate Escalation Channel.
- Investigate HR Concerns and determine significance.
- Oversee resolution of Concerns within their areas of responsibility that are escalated to them.
- Promptly report significant HR Concerns to the ICRM Central Incident Escalation Team.
- Report sensitive or confidential significant HR Concerns directly to the Head of HR and the Chief Compliance Officer.
- Maintain Escalation Channel specific procedures to support the Escalation Policy.
- Train or communicate requirements to relevant employees necessary to support execution of HR escalation procedures.

4.5 LEGAL MUST

- Refer Concerns escalated to them to the appropriate Escalation Channel.
- Advise and support first and second line functions, and control units to oversee resolution of Concerns or Incidents escalated to them.
- Maintain Escalation Channel specific guidelines to support the Escalation Policy.
- Make relevant employees aware of the requirements of the Escalation Policy in support of consistent execution of Legal escalation practices.

4.6 ETHICS OFFICE MUST

- Refer Concerns escalated to them to the appropriate investigative functions.
- Maintain Escalation Channel specific procedures to support the Escalation Policy.
- Train or communicate requirements to relevant employees necessary to support execution of Ethics Office escalation procedures.

4.7 ICRM MUST

- Refer Concerns escalated to them that are outside of their area of direct responsibility or that they are unable to handle appropriately to the appropriate Escalation Channel or investigative function.
- ICRM senior management assess and determine the severity of Incidents.
- Promptly escalate significant, or potentially significant Incidents to the appropriate level of

ICRM management.

- Centrally receive significant, or potentially significant, Incidents from Escalation Channels for centralized tracking and reporting.
- Promptly report significant, or potentially significant, Incidents to the Chief Compliance Officer and ICRM senior management.
- Communicate significant, or potentially significant, Incidents across the three lines of defense on a periodic basis.
- Perform continuous improvement monitoring analysis.
- Maintain Escalation Channel specific procedures to support the Escalation Policy.
- Train or communicate requirements to relevant employees necessary for the execution of ICRM's escalation procedures.

4.8 BUSINESSES AND FUNCTIONS MUST

- Cooperate with and assist the Escalation Channels in their respective investigative, Concern or Incident management, assessment of significance, and reporting responsibilities, as necessary.
- Identity the legal entity or legal entities impacted by the Incident.
- Escalate significant Incidents to the appropriate level of business, function, or legal entity senior management.
- Maintain protocols and procedures for the appropriate escalation of Concerns within the business or function to support the Escalation Policy.
- Determine the need, and if necessary, train relevant employees for the execution of businesses or function procedures.

4.9 INTERNAL AUDIT

Internal Audit provides independent risk-based assurance over the escalation process, including this Policy, based upon a risk-based audit plan and audit methodology as approved by the Citigroup Inc. Board of Directors. Issues raised during the audit process are governed by the Internal Audit Charter and do not require escalation in line with this Policy. If Internal Audit receives an escalated compliance Incident outside the scope of their regular responsibilities, they must escalate the compliance Incident in accordance with this Policy.

5 REPORTING TO MANAGEMENT GOVERNANCE COMMITTEES

5.1 REPORTING TO MANAGEMENT GOVERNANCE COMMITTEES

5.1.1 Once an Incident has been escalated for investigation and resolution as described above, it is important that it also be reported to appropriate management governance committees such as Legal Entity, Regional, Country and Business/Functional committees (e.g., BRCC), if it is determined to be a significant Incident or a severity level 1 or 2 Issue under the AICAP Policy. This further reporting of significant Incidents and severity level 1 or 2 Issues must be done regardless of whether it has been resolved. The incident significance determination can change as more facts become known as such the reporting should be based on the point in time severity with downgrades to Incidents or Issues already reported called out. Legal Entities or jurisdictions must determine whether incidents or Issues of lower severity levels must also be reported to Senior Management or appropriate management governance committees such as such as Legal Entity, Regional, Country and Business/Functional committees. See Business Risk and Control Committee Standard or minimum management governance reporting standards to be applied by local and regional managers with geography, business or functional governance responsibility. Also refer to the Escalation Grid in the Citi Governance Policy, which provides guidance for core management reporting of escalatable matters and minimum management governance reporting standards for each of the GRC Level 0 Risk categories.

5.1.2 In reporting on significant Incidents and severity level 1 and 2 Issues, the confidentiality, and anonymity in certain circumstances, of the individual who escalated the Incident or severity level 1 or 2 Issue must be maintained; in certain circumstances, this can require that the method by which it was originally escalated not be disclosed. Descriptions and escalations of significant Incidents and severity level 1 and 2 Issues must take into account relevant sensitive and confidential information considerations as well as legal privilege when applicable. If an Escalation Channel is aware that an Incident is the subject of a litigation or legal investigation, the Escalation Channel must consult with Legal regarding appropriate escalation and investigation of the Incident. Questions about whether the description or escalation of an Incident must be modified due to these Concerns must be referred to Legal, Human Resources, and/or the Ethics Office, as applicable.

5.1.3 Senior Management, including individuals within Escalation Channels, with board reporting responsibilities must also determine whether a significant Incident or severity level 1 or 2 Issue needs to be brought to the attention of the Board of Directors or subcommittee of the Board. See Business, Risk and Control Committee Standard for further information.

5.2 MANAGEMENT GOVERNANCE COMMITTEES

5.2.1 To review and oversee significant Incidents and severity level 1 and 2 Issues, each

BRCC or other appropriate management governance committee must include those recorded as Issues in iCAPs for which the respective committee has oversight responsibility.

5.2.2 Each management governance committee must also review and further escalate significant Incidents and severity level 1 and 2 Issues in line with the governance hierarchy in accordance with the responsibilities set forth in its Charter. Reporting of significant Incidents and severity level 1 and 2 Issues to BRCCs must be in accordance with the Business Risk and Control Committee Standard.

5.2.3 Each BRCC must set forth in its respective Charter criteria for reporting significant Incidents and severity level 1 and 2 Issues to be reviewed by the BRCC and process to be further reported, in line with the committee hierarchy, by the BRCC, in accordance with the Business Risk and Control Committee Standard and consistent with the criteria requirements of this Policy.

5.2.4 The Group BRCC, chaired by the Citigroup Chief Executive Officer, must determine, in accordance with its responsibilities, established by its Charter, whether a significant Incident or a severity level 1 or 2 Issue must also be reported to the Board of Directors.

5.3 REPORTING TO THE BOARD OF DIRECTORS OR ITS COMMITTEES

5.3.1 The Chief Compliance Officer is responsible for reporting on certain compliance risk-related issues, including escalated significant Incidents and severity level 1 and 2 Issues, to the Audit Committees of the Boards of Directors for Citigroup Inc. and Citibank, N.A. no less than quarterly.

5.3.2 Nothing in this section is intended to limit Officers, Senior Management and those with reporting responsibilities from escalating and reporting Issues to the Board of Directors independent of these processes, in accordance with their scope of authority and responsibility.

6 EXECUTION ASSESSMENT

6.1 MANAGER'S CONTROL ASSESSMENT

6.1.1 The requirements of this Policy must be included in the relevant MCA, to the extent required by, and in accordance with the Governance, Risk & Compliance & Manager's Control Assessment Standards, which are appended to the Operational Risk Management Policy.

6.2 MONITORING AND TESTING

6.2.1 This Policy is subject to periodic assurance (monitoring) and testing pursuant to the ICRM Compliance Monitoring Procedure and the ICRM Compliance Testing Procedure, as applicable.

6.3 TRAINING

6.3.1 Training needs with regard to this Policy must be assessed and implemented in accordance with the requirements, roles and responsibilities set forth in the Global Independent Compliance Risk Management (ICRM) Training Standard.

APPENDIX A: EXAMPLES OF POTENTIAL CONCERNS

This table lists examples of the types of Concerns that must be escalated, and the suggested Escalation Channel to which such Concerns can be escalated in the event that escalation to the manager is not appropriate in accordance with Section 2.4.2. This list is not exhaustive; other types of Concerns will require escalation.

The function to which the Concern is escalated represents the function or functions that typically handle such Concerns, but, in the event of uncertainty, employees can choose to escalate their Concerns to any of the Escalation Channels listed in the Policy.

In addition, as explained in Section 2.5, employees can always escalate Concerns to the Ethics Office.

Nature of Potential Concern	Primary Escalation Channel[6]
Human Resources Concerns: • Employment Discrimination that is unlawful or in violation of Citi Policies. (Includes employment discrimination based on race, sex, gender, pregnancy, gender identity or expression, color, creed, religion, national origin, nationality, citizenship, age, physical or mental disability or medical condition as defined under applicable law, genetic information, marital status (including domestic partnerships and civil unions as defined and recognized by applicable law), sexual orientation, culture, ancestry, familial or caregiver status, military status, veteran's status, socioeconomic status, unemployment status, status as a victim of domestic violence, or any other basis prohibited by law.) • Harassment that is unlawful or in violation of Citi Policies. (Includes any form of sexual harassment and any harassment that is based on the characteristics enumerated in Employment Discrimination.) • Workplace health and safety Concerns. (Includes Concerns relating to contagion, failure to follow Citi's health and safety directives, threats of workplace violence, and impairment due to consumption of alcohol, illegal drugs, or controlled substances.) • Violations of wage and hour or other employment-related laws • Employee Misconduct (Includes violations of law and breaches of Citi Policy.) • Retaliation for raising any Legal or Ethical concern, or for participating in the investigation of any such Concerns, as well	Human Resources

[6] The Escalation Channels in this Appendix represent the primary Escalation Channel for escalation for each type of Concern. As noted in this Policy, employees may escalate to any Escalation Channel they choose.

Nature of Potential Concern	Primary Escalation Channel[6]
as any conduct that has the purpose or effect of suppressing the escalation of any Concern	
Lawsuits, subpoenas, litigation-related document and information requests	Legal
Business Conduct, Market Conduct (unauthorized trading, misrepresentation, market manipulation)	ICRM
Conflicts of interest (improper contacts with third parties, conducting outside business activities without approval). Example includes: • Employee does not adhere to procurement protocols and appoints a third party vendor on the basis of personal interests	
Sales Practice. Description of Sales Practice Risk includes: • Opening / Closing without Consent: Risk of harm to customers may arise from opening and/or closing of accounts or products without customer knowledge or authorization, or upon request • Funds Manipulation: Risk of harm to customers may arise from execution of transactions to / from customer accounts without customer knowledge or authorization • Product Disclosure: Risk of harm to customers may arise from providing inaccurate, false or misleading product / service information to customer • Product Steering: Risk of harm to customers may arise from pressuring customer to choose certain products or services that are unwanted / unrequested, or are different than the customer's stated preferences	
Anti-Money Laundering, Sanctions, Bribery, Foreign Corrupt Practices Act violations. Examples include: • Employee willfully ignores Citi's Products and Services being intentionally misused for the purposes of money laundering, terrorist financing, evading taxes or other illegal activities • Employee knowingly facilitates money laundering, terrorist financing, tax evasion or any other financial crime • Employee provides or facilitates services (e.g., relationships, accounts, securities holdings, transactions) to sanctions targets (e.g., country, region, government, individual, entity, vessel, or aircraft subject to U.S. and/or Non-U.S. sanctions) • Employee improperly processes, approves or otherwise facilitates the opening/maintenance of account/relationship or a transaction (including securities holdings) for the benefit of, or involving, a target of sanctions (e.g., country, region, government, individual, entity).	

Nature of Potential Concern	Primary Escalation Channel[6]
• Employee attempts to circumvent, or advises a third party (e.g., client, vendor) on circumvention of, sanctions regulatory or Citi Policy requirements through the omission, alteration or removal of a reference to a sanctions target from any record or document subject to sanctions screening. This includes, for example, records and documents related to a transaction (e.g., payment instruction, trade financing agreement, securities holding), account/relationship, employee or third party relationship (e.g., non-employees, vendor, supplier). • Employee offers anything of value (e.g., gifts, entertainment, employment opportunities) to anyone for the purpose of influencing the recipient to take or refrain from taking any official action or to induce the recipient to conduct business with Citi	
Information Security. Examples include: • Employee discloses personal, proprietary or confidential information about any client, supplier, vendor, distributor, shareholder, business partner or Citi to any unauthorized person, including another Citi employee • Employee does not return all means of access to Citi information and all copies of such information when their employment or association with Citi ends	CSIS
Internal Fraud/Theft, Misrepresentation (falsifying records, forgery, defacement/destruction, false statements to Citi representatives or regulators). Examples include: • Employee falsifies or engages in irregular practice(s) with respect to non-business related expenses, such as false claims for expense reimbursement • Employee processes a fraudulent journal entry to conceal the nature of an unexpected operational loss • Employee steals or inappropriately possesses Citi property	
Threats or acts of violence, including domestic violence that impacts the workplace	

APPENDIX B: ESCALATION POLICY CONTACTS

The following table contains contact information for the Escalation Channels mentioned in this Policy. Employees can contact any of the Escalation Channels below with Concerns.

Escalation Channel	Contact Information for Escalation Channel
Human Resources (HR)	• Website: https://citiforyou.citigroup.net/ • Contacts: https://citiforyou.citigroup.net/en-us/Pages/Need-Help.aspx?isSharedPage=true
ICRM	• Website: https://www.citi.net/EN/compliance • Contacts: ICRM Escalations Collaborate site

CSIS	• Website: https://www.citi.net/EN/csis
	• If you have Concerns about fraud, theft, threats or acts of violence, including domestic violence that impacts the workplace, immediately contact the CSIS Regional Command Center:
	  ○ NAM/U.S. toll free: 1-800-349-9714
	  ○ International direct or collect: +1-813-604-4100
	  ○ APAC – Regional Command Center: +65 6789 9333
	  ○ EMEA – Regional Command Center: +44 20-7500-3333
	  ○ LATAM – Regional Command Center: +506 4051 9911
	  ○ MEXICO – Regional Command Center: +52 55 1226 9994
	• Incident reporting:
	https://www.citi.net/EN/Pages/csis/ContentPages/resources.aspx

Legal	• Website: https://www.citi.net/EN/LEGAL • Contacts:https://www.citi.net/EN/Pages/legal/ContentPages/legal-directories.aspx

Ethics Office	• Website: https://www.citi.net/EN/Pages/ethicsoffice/ContentPages/report.aspx?src=/EN/ethicsoffice
	• Citi Ethics Hotline (24 hours per day, seven days per week, and multi-lingual)
	  ○ U.S. toll free: 1-866-ETHIC 99 (1-866-384-4299)
	  ○ International direct or collect: 1-212-559-5842
	  ○ Dial your country access code and 866-384-4299

The following table contains additional useful contact information for the Escalation Policy.

Additional Contacts	Contact Information
Country Chief Compliance Officers	• Website:https://www.citi.net/EN/Pages/compliance/ContentPages/chief-country-compliance-officer-nam.aspx
Risk Category Subject Matter Experts	• Website:https://www.citi.net/EN/Pages/riskmanagement/ContentPages/CBDC-Useful-Contacts.aspx

APPENDIX C: HANDLING OF SENSITIVE AND CONFIDENTIAL ESCALATION MATTERS

When escalating identified Concerns within a country, region, line of business or function, or when onward forwarding reported concerns to another Escalation Channel, the focus should be on the transparent and accurate reporting of the known facts.

When handling sensitive or confidential employment, legal or regulatory matters, it is important to communicate information in a manner that maintains compliance with country data privacy regulatory requirements and Citi's Information Security and Confidentiality policies, and to limit the recipients of that information to those that have a "need to know." Not doing so can result in the inadvertent release of Restricted, Confidential or Personally Identifying Information (PII), which may violate data privacy controls, cross-border data transfer requirements, impact reputation or be damaging to client, customer, employee and / or regulatory relationships, and/or expose Citi to potentially avoidable legal risk.

When assessing the reporting and handling of these issues, please consider the following:

- Focus on facts; while prompt escalation requires communication and onward forwarding before all facts are known or validated, it is important to use language that distinguishes known facts from concerns or speculation;

- Where the Concern includes Restricted, Confidential or PII data, be sure to apply Citi Information Security standards, which may require the encryption of said data. Click here for guidelines on how to encrypt data for electronic distribution within Citi's network;

- Where the Concern involves a sensitive or confidential employment, client/customer, regulatory or legal matter, limit the audience only to those with an absolute need to know and mark the communication "Confidential" or, if you are an attorney or escalating directly to an attorney, "Privileged & Confidential." You should also consider redacting any PII, customer or client data (e.g., employee name, customer name, institutional client name) from the communication before escalating the Concern. If necessary, it may be appropriate to provide the redacted PII, customer or client data to certain escalation recipients separately;

- If you aware that the Concern is or is likely to be the subject of litigation or a legal investigation, consult with Legal regarding appropriate escalation and investigation.

APPENDIX D: AUSTRALIA ADDENDUM

1. OBJECTIVE

An individual is eligible for whistleblower protection under Australian law if they make a disclosure that qualifies for protection. The aim of whistleblower protection is to safeguard individuals who disclose misconduct so that they can do so safely, securely, and with the comfort that they will be protected and supported.

This Addendum seeks to provide information on the specific statutory whistleblower protection available under the Australian law, including:

- How an individual can make an Eligible Disclosure (i.e., a disclosure that qualifies for whistleblower protection);
- Responsibilities of an individual who makes a disclosure;
- Responsibilities of an individual who receives a disclosure;
- Whistleblower protection available;
- How Citi investigate Eligible Disclosures;
- Fair treatment and support of individuals who makes, or are mentioned in an Eligible Disclosure

Disclosures that do not qualify for protection under Australian law are not covered by this Addendum. Refer to the Citi Code of Conduct for information about the general protection Citi provides to individuals irrespective of whether statutory whistleblower protection is applicable.

1.1 SCOPE

This Addendum supports the Escalation Policy and applies to:

- Citi legal entities within Australia ('**Citi**'),
- the Citi Ethics Office,
- an Eligible Disclosure made in relation to a foreign Citi Related Body Corporate, and
- an Eligible Disclosure made to an Eligible Recipient of a foreign Citi Related Body Corporate.

Note that potential applicable laws in the host country of an employee, or former employee will need to be considered where the individual is an expatriate or temporarily assigned to work in another country. For any cross-border matters, the Australia General Counsel, and General Counsels in all other relevant countries must be consulted confidentially.

1.2 TARGET AUDIENCE

The target audience for this Addendum is all Citi Officers and employees, the Citi Ethics Office, and Eligible Recipients of a foreign Citi Related Body Corporate. It is also acknowledged that Eligible Whistleblowers includes a broad range of people who have had a relationship with Citi (see Section 1.7.4 below).

This Addendum is made available to Citi Officers and employees via the Citi Policy Directory.

1.3 OWNER

This Addendum is owned by the Chief Compliance Officer of Australia (**CCCO**).

1.4 EFFECTIVE DATE / TRANSITION PERIOD

This Addendum is effective from 1 January 2020.

1.5 RETIRED POLICIES / RELATED POLICIES

This Addendum must be read in conjunction with:

- Escalation Policy, and
- Code of Conduct.

1.6 BOARD APPROVAL

Citigroup Pty Limited (**CPL**) Board and Citibank, N.A: Sydney Branch (**CBNA**) Senior Officer outside Australia (**SOoA**) approval of this Addendum is required. This Addendum will be reviewed annually.

1.7 KEY DEFINITIONS

1.7.1 AUSTRALIAN LAW

Australian law means the *Corporations Act 2001 and Taxation Administration Act 1953.*

1.7.2 DIRECTOR

Director means a person appointed or acting as a Board Director, or alternate to a Board Director of:

- Citi, or
- a foreign Related Body Corporate of Citi

.

1.7.3 ELIGIBLE DISCLOSURE

An Eligible Disclosure is a disclosure that is made by an Eligible Whistleblower, to an Eligible Recipient (whether openly, confidentially, or anonymously), about an Eligible Matter.

1.7.4 ELIGIBLE WHISTLEBLOWER

Eligible Whistleblower means Citi's existing and former employees or Officers, suppliers of services or goods to Citi and their employees (whether paid or unpaid), and Citi associates[7].

Relatives, spouse, or dependents of an Eligible Whistleblower are also included.

An Eligible Whistleblower also includes a trustee, custodian or investment manager of a Citi Superannuation Entity.

1.7.5 ELIGIBLE MATTER

Eligible Matter means a disclosure, where the discloser has **reasonable grounds** to suspect the information:

a) Concerns misconduct, or an improper state of affairs in relation to Citi or its foreign Related Body Corporate (e.g., dishonest or unethical behavior, conduct that cause harm or prohibited by Citi's Code of Conduct), **or**

b) indicates that Citi or its foreign Related Body Corporate, or an Officer or employee of Citi or its foreign Related Body Corporate, has engaged in conduct that:

- constitutes an offence against, or a contravention of the *Corporations Act*, *Australian Securities and Investments Commission Act 2001*, *Banking Act 1959*, *Financial Sector (Collection of Data) Act 2001*, *Insurance Act 1973*, *Life Insurance Act 1995*, *National Consumer Credit Protection Act 2009*, *Superannuation Industry (Supervision) Act 1993, or an instrument made under the above legislations*, or
- constitutes an constitutes an offence against any other law of the Commonwealth that is punishable by imprisonment for a period of 12 months or more, or
- represents a danger to the public or the financial system, **or**

indicates misconduct, or an improper state of affairs or circumstances, in relation to the tax affairs of the entity or an associate (within the meaning of section 318 of the *Income Tax Assessment Act 1936*) of the entity, and considers that the information may assist the eligible recipient to perform functions or duties in relation to the tax affairs of the entity or an associate (within the meaning of section 318 of the *Income Tax Assessment Act 1936*) of the entity.

Note that the discloser can still qualify for protection even if their disclosure turns out to be incorrect, however protection is unavailable where the discloser did not believe the information to be true.

Some work related grievances are not covered

Eligible Matters does not include personal work related grievances unless it relates to whistleblower victimization. Personal work related grievances that do not qualify for protection must be escalated to Human Resources[8].

Below are some examples of personal work-related grievances that are not protected disclosures unless it relates to whistleblower victimization:

- an interpersonal conflict between the discloser and another employee;
- a decision relating to the engagement, transfer or promotion;
- a decision relating to the terms and conditions of engagement; and
- a decision to suspend or terminate the engagement, or otherwise to discipline the discloser.

1.7.6 ELIGIBLE RECIPIENTS

Eligible Recipients means any of the following:

a) Senior Manager, Director, Company Secretary, Officer, Auditor, Actuary of Citi or a Foreign Citi Related Body Corporate,

b) the Citi Ethics Office,

c) a Director of the Trustee of a Citi superannuation entity, or a person authorized by the Trustee to be an Eligible Recipient, or

[7] Citi associates is as defined under the *Corporations Act 2001* and s318 of the *Income Tax Assessment Act 1936*.

d) if the disclosure relates to a taxation matter, a registered Tax Agent/Business Activity Statements (BAS) agent who provides tax agent services or BAS services to Citi, and any employee or Officer who has functions or duties relating to Citi's tax affairs.

Note that protection is also available if the disclosure:

- is made to Australian Securities and Investments Commission (ASIC), Australian Prudential Regulation Authority (APRA) or another prescribed Commonwealth authority prescribed by regulation,
- is made to a lawyer for the purpose of obtaining legal advice or representation about the operations of the whistleblower protections under Australian law,
- is of public interest or relates to a health and safety emergency, and is made to a journalist or a member of the Parliament of the Commonwealth, the Parliament of a State or the legislature of a Territory provided certain statutory requirements have been satisfied. Refer to Section 1317AAD of the Corporations Act 2001 for further information on protection eligibility criteria for these disclosures, or
- the disclosure relates to a tax matter and is made to the Tax Commissioner and the discloser considers that the information may assist the Tax Commissioner to perform his or her functions or duties under a taxation law in relation to the entity or an associate (within the meaning of Section 318 of the Income Tax Assessment Act 1936) of the entity.

1.7.7 OFFICER

Officer is as defined in Section 9 of the *Corporations Act 2001.*

1.7.8 RELATED BODY CORPORATE

Related Body Corporate is as defined in Section 9 of the *Corporations Act 2001.*

1.7.9 SENIOR MANAGER

Senior Manager is as defined in Section 9 of the *Corporations Act 2001* to mean a person (other than a director or secretary of the corporation) who:

- makes, or participates in making, decisions that affect the whole, or a substantial part, of the business of Citi; or
- has the capacity to affect significantly Citi's financial standing.

This includes the following individuals within Citi:

- Members of the Executive Committee,
- Accountable Persons per the CPL and CBNA Banking Executive Accountability Regime Policies,
- Responsible Person per the CPL and CBNA Fit and Proper Policies, and
- An individual of a Foreign Citi Related Body Corporate that are equivalents of the above.

[8] These disclosures may be protected under other legislation, such as the Fair Work Act 2009.

1.7.10 SUPERANNUATION ENTITY

Superannuation Entity is as defined under the *Superannuation Industry (Supervision) Act 1993.*

2. HOW TO MAKE A DISCLOSURE THAT QUALIFIES FOR PROTECTION

The Australian law provides protection to individuals who make disclosures about certain matters. It is important for an individual to be aware of how they can qualify for this protection.

To qualify for this protection, the individual must make an Eligible Disclosure.

An Eligible Disclosure is a disclosure that is:

- made by an Eligible Whistleblower, and
- made directly to an Eligible Recipient, and
- about an Eligible Matter.

Refer to Section 1.7 for definitions of the above terms.

Refer to Section 5 for details on protection available for Eligible Disclosures.

Citi Ethics Office

The Citi Ethics Office is an Eligible Recipient designated by Citi to receive whistleblower disclosures. Per Appendix B of the Escalation Policy, an individual is able to make a disclosure anonymously and/or confidentially to the Ethics Office 24 hours per day, seven days per week via the Citi Ethics hotline, email, website or by mail. Contact information is available in Appendix B of the Escalation Policy and the Citi Code of Conduct.

Note that although the Citi Ethics Office is the preferred escalation point for whistleblower matters, an individual can also disclose a matter to other Eligible Recipients as defined under Section 1.7.6.

3. RESPONSIBILITIES OF INDIVIDUALS WHO MAKE A DISCLOSURE

The individual must understand how they can make an Eligible Disclosure and the protections available under this Addendum.

Individuals are encouraged to seek independent legal advice if they are unsure how whistleblower protection applies under Australian law, or how it applies to their circumstance.

When making a disclosure, the individual must tell the recipient that:

- they are making a disclosure under this Addendum, and
- whether they wish to make a disclosure:
    - anonymously (if an individual prefers not to disclose their identity to others, an individual may choose to adopt a pseudonym for the purpose of their disclosure so that they can be contactable to assist with the investigation.), or
    - confidentially, or
    - gives consent for their identity to be disclosed.

4. RESPONSIBILITIES OF INDIVIDUALS WHO RECEIVE A DISCLOSURE

The recipient must be aware that there are severe penalties under the Australian law for:

- disclosing the identity of an individual qualifying for protection, or disclosing information that is likely to identify the individual. Refer to Section 5.2 for exceptions to protection of anonymity and confidentiality, and

- causing or threatening detriment to an individual on the basis of a belief or suspicion that the individual or another person has made, proposes to make, or could make an Eligible Disclosure. Refer to Section 5.3 for Citi's policy on retaliation, harassment, and victimization.

4.1 ANONYMOUS DISCLOSURES

If an individual wishes to remain anonymous they must specify this to the recipient. The recipient must respect the individual's wishes to remain anonymous.

Upon receiving an Eligible Disclosure, the recipient must either:

- refer the individual to the Citi Ethics Office, or
- if the individual does not wish to contact the Citi Ethics Office, the recipient must escalate the concern directly to the Citi Ethics Office. The recipient must not provide the individual's name or other identifying information when escalating the concern, or to others.

4.2 ALL OTHER DISCLOSURES

The recipient must refer any Eligible Disclosure, or any matters that they suspect may be an Eligible Disclosure, to the Citi Ethics Office for investigation. The recipient must not disclose to others about the content of the disclosure or the identity of the individual.[9]

4.3 PROTECTION FOR THE RECIPIENT

When a recipient escalates a matter, they too become a discloser themselves.

The recipient must consider Section 2 and understand how they can also qualify for protection under Australian law.

5. WHISTLEBLOWER PROTECTION AVAILABLE

The following whistleblower protections are available to an individual who makes an Eligible Disclosure from the time the disclosure is made.

5.1 GENERAL PROTECTIONS

- The individual is not subject to any civil, criminal or administrative liability (including disciplinary action) for making the disclosure. This protection does not grant immunity for any misconduct the individual has engaged in that is revealed in their disclosure;
- The individual has immunity from lawsuit from making the disclosure;
- No contractual or other remedy may be enforced, and no contractual or other right may be exercised, against the individual on the basis of the disclosure;
- Under circumstances prescribed under s1317AA of the *Corporations Act 2001*,

if the disclosure is made to ASIC, APRA, or a prescribed Commonwealth authority, the information is not admissible in evidence against the individual in criminal proceedings or in proceedings for the imposition of a penalty, other than proceedings in respect of the falsity of the information.

5.2 ANONYMOUS AND CONFIDENTIAL DISCLOSURE

An individual who qualifies for protection has the right to anonymity and confidentiality unless they consent to their identity being disclosed. Statutory penalties apply to unauthorized disclosure of an individual's identity, if the individual qualifies for whistleblower protection. The individual may lodge a complaint by contacting the Citi Ethics Office, or alternatively, with a regulator, such as ASIC, APRA or the ATO, for investigation of a breach of confidentiality.

A discloser can choose to remain anonymous while making a disclosure, over the course of the investigation and after the investigation is finalized. Citi however, may not be able to undertake an investigation if it is not able to contact the discloser.

This protection does not extend to disclosure of the discloser's identity to ASIC, APRA, a member of the Australian Federal Police, or a lawyer for the purpose of obtaining legal advice or legal representation in relation to the operation of the Australian law.

5.2.1 DISCLOSURE OF INFORMATION FOR INVESTIGATION

The information contained in a disclosure can be disclosed without the individual's consent if the information:

a) does not include the individual's identity,

b) the entity has taken all reasonable steps to reduce the risk that the discloser will be identified from the information; and

c) it is reasonably necessary for investigating the issues raised in the disclosure.

5.3 PROTECTION FROM RETALIATION, HARASSMENT / VICTIMISATION

There are severe penalties under the Australian law for causing or threatening detriment[10] to an individual for making or proposing to make an Eligible Disclosure. These penalties apply both to Citi and the individual offender. The individual can contact a regulatory body or can seek compensation and other remedies through court if they suffer a loss, damage or injury because of a disclosure, and Citi fails to prevent a person from causing the detriment.

Citi prohibits any form of retaliatory action against anyone who makes an Eligible Disclosure. Retaliation is a serious issue and includes any adverse action taken because an employee has engaged in such activity. As part of any investigation, Citi respect the rights that are afforded under applicable laws and regulations to all parties related to the matter.

---

[9] Refer to Section 5.2 for exceptions to confidentiality.

Allegations of retaliatory action, harassment, or victimization must be escalated to the

Citi Ethics Office. A person who retaliates against another individual for raising Concerns, or being involved in an investigation will be subject to action under the disciplinary procedure up to and including termination of employment or other relations with Citi.

6. HOW ELIGIBLE DISCLOSURES ARE INVESTIGATED

Citi believes it is essential an individual feels secure when raising a concern and encourage individuals to communicate their Concerns openly. Individuals may be interviewed as part of that investigation. All contacts and investigations are treated as confidentially as possible, consistent with the need to investigate the matter, subject to applicable laws and regulations, and conducted in a timely manner. Investigators must only disclose information on a need-to-know basis and must otherwise safeguard and take appropriate steps to prevent the unauthorized disclosure of such confidential information.

Upon receiving a disclosure, the Citi Ethics Office will assign the matter to the appropriate function for investigation, documentation, and reporting in accordance with its investigation procedures. An assessment of whether a disclosure qualifies for statutory whistleblower protection, and a risk assessment of detriment against a discloser is performed with assessment outcome advised to the investigator where appropriate. Appropriate actions will be undertaken to reduce potential detriment to the discloser.

The investigator will contact the discloser throughout the investigation process to assist with the investigation.

The discloser will be sent an acknowledgement after the disclosure is received, and will be informed by the investigator once the investigation is concluded. The discloser will not be provided with the outcome where it is inappropriate to do so.

Findings from investigations will be documented and reported in accordance with respective procedures. Method for documenting and reporting of findings will depend on the nature of the disclosure.

Disclosers are encouraged to contact the Citi Ethics Office if their identity has been exposed without their consent.

7. FAIR TREATMENT AND SUPPORT OF INDIVIDUALS WHO MAKES, OR ARE MENTIONED IN AN ELIGIBLE DISCLOSURE

When Concerns are raised with respect to possible misconduct or unethical behavior,

Citi conducts investigations thoroughly, fairly, with discretion, and in a timely manner in line with values stated in the Citi Code of Conduct.

An individual that is the subject matter of a disclosure will be:

- advised the disclosure as and when required by procedural fairness,

---

[10] Examples of detriment include but not limited to: dismissal of an employee, harassment or intimidation or discrimination, alter an individual's position or duties to their disadvantage, damage to a person's reputation, property, or other damage. Note that actions such as managing a discloser's unsatisfactory work performance is not considered to be detrimental conduct, if the action is in line with Citi's performance management framework.

- advised of any referrals to a regulator or law enforcement as appropriate, subject to any regulatory requirements or obligations,
- advised of the outcome of the investigation as and when appropriate.

Various support is also available depending on the circumstances, for example:

- Employee Assistance Program provides confidential counselling and coaching to the employee and their immediate family free of charge.
- Targeted programs are available depending on individual circumstances.
- Leave options including one paid Health & Wellbeing day per annum.
- Return to Work Support via Specialist Rehabilitation Providers if further support is required on returning from leave.
- Online support via Citi For You/Minds at Citi including a range of psychological support, tools and information.

Further information on the support that are available must be directed to Human Resources.

8. GETTING ADVICE

Please direct general questions in relation to the Addendum to the CCCO in Australia.

Individuals are encouraged to seek independent legal advice if they are unsure how whistleblower protection applies under Australian law, or how it applies to their circumstances.

APPENDIX E: NIGERIA ADDENDUM

1. OBJECTIVE

The Nigeria Addendum was developed in accordance with the Central Bank of Nigeria's ("CBN") Guidelines for Whistle-blowing for Banks and Other Financial Institutions in Nigeria ("Guidelines"), which require that banks and other financial institutions in Nigeria implement a whistle- blowing policy to encourage stakeholders to bring unethical conduct and illegal violations relating to Citibank Nigeria to the attention of the appropriate authority. The provisions of the Addendum represent the minimum standards of whistleblowing which banks are expected to comply with. The Guidelines define "whistle-blowing" as "the reporting of alleged unethical conduct of employees, management, directors and other stakeholders of an institution by an employee or other person to appropriate authorities." A whistle-blower is "any person(s) including the employee, management, directors, depositors, service providers, creditors and other stakeholders of an institution who reports any form of unethical behavior or dishonesty to the appropriate authority". This addendum, along with the rest of the Policy's, including addenda, will be reviewed as part of the Policy's annual periodic review.

1.1 Scope

This Addendum applies to Citibank Nigeria Limited.

1.2 Target Audience

Citi Nigeria employees, management, directors, shareholders and contractors

2. STANDARD PROVISIONS

2.1 Regulatory Guidance

Citi Nigeria is to comply with all applicable laws and regulations and to:

- Encourage employees, management, directors or other stakeholders who have a good reason to believe that Citi Nigeria or any of its employees, management or directors have acted unethically or violated any law, regulation or policy related to Citi Nigeria activities, to report their concerns.
- Investigate the alleged violation and take appropriate corrective action(s). Employees are subject to Citi Nigeria Limited Disciplinary Policy.
- Conduct investigations while respecting the rights of the whistle-blower and the employee, management, director or other stakeholder accused of wrong doing.
- Conduct investigations in a confidential manner and in accordance with relevant laws, regulations and internal policies.
- Avoid damaging the reputation of suspected persons who are subsequently found innocent of alleged wrongful conduct by ensuring that the presumption of innocence applies until guilt is established.
- Prohibit any retaliatory action against an employee, management, director or other stakeholder for making a good faith report of a suspected unethical behavior, violation of any law, regulation, or Citi Nigeria policy by Citi Nigeria or any of its employees, management or directors or other agents authorized to act on its behalf.
- Prohibit any retaliatory action against a whistle-blower or employee, management, director or other stakeholder who has provided information in good faith in connection with an

internal investigation following a whistle-blowing report. Also refer to section 2.7 of the Escalation Policy.

- Confirm the whistle-blower is not protected from the consequences of his or her own wrongdoing by using the whistle-blowing mechanism as a cover.
- Take appropriate action against individuals who engage in retaliatory conduct prohibited by this Policy.

2.2 Conduct covered by this Policy may include:

- All forms of financial malpractice or impropriety or fraud;
- Failure to comply with a legal obligation or Statute;
- Actions detrimental to Health & Safety or the environment;
- Any form of criminal activity;
- Improper conduct or unethical behavior;
- Failure to comply with regulatory directives;
- Other forms of corporate governance breaches;
- Connected transactions;
- Insider abuses;
- Non-disclosure of interest;
- Attempts to conceal any of these, etc.

2.3 Reporting

A whistle-blower shall disclose any information in connection with the activities of Citi Nigeria which indicates any of the following:

1. that an infraction has been committed;
2. that a person has failed to comply with banking laws, internal policies and procedures, etc.; and
3. that someone has concealed matters falling within (1) or (2) above.

All contact and investigations are treated confidentially and the identity of the whistle-blower shall be kept confidential, consistent with the need to investigate and address the matter, subject to applicable laws and regulations. Complaints may be made anonymously, however whistle-blowers are encouraged to disclose their name when filing a report so that Citi Nigeria can obtain additional information to address the concern, if needed.

Citi prohibits retaliatory action against employees arising as a result of a disclosure made in good faith and if an employee feels that they have been the subject of retaliatory action as a result of a disclosure they should escalate to the Citi Nigeria Head of Internal Audit and/or the Citi Ethics Office in New York, USA.

All reports under this Policy should be made promptly to any of the following:
Citi Nigeria Hotline: +234 1 4638400; + 234 1 2798400 ext. 2216
Email: Nigeria.whistleblowing@Citi.com

The Citi Ethics Hotline remains available to Citi employees and any complaints/concerns

related to activities unconnected to Citi Nigeria should continue to be escalated in accordance with the Code of Conduct.

The Citi Ethics Hotline: +1-212-559-5842 (direct or collect)
E-mail: ethicsconcern@citi.com
Fax: +1-212-793-1347
Mail: Citi Ethics Office, One Court Square, Long Island City. N.Y. 11101 U.S.A.
Website submission: http://www.citigroup.com/citi/investor/ethics_hotline.html

These channels are available 24 hours a day, seven days a week. All reports are confidential to the extent possible.

Central Bank of Nigeria
E-mail: ethicsoffice@cbn.gov.ng/ anticorruptionunit@cbn.gov.ng
Telephone: +234 9 46239246 **and** +234 9 46236000.

2.4 Procedures

- The Head of Internal Audit of Citi Nigeria will review all reported cases under this Policy and make a recommendation on appropriate action to the Citi Country Officer/Managing Director (CCO). Where the report affects Executive Management, the matter will be referred to the Board. The Board of Directors of Citi Nigeria or CCO will take the necessary action within a reasonable time.
- If the reported issue relates to the Head of Internal Audit or the Audit function of Citi Nigeria, the Head of Internal Audit will recuse himself and the CCO will designate a person to review the matter and make a recommendation on appropriate action to the CCO or Board of Directors of Citi Nigeria, where the matter affects Executive Management.
- The Head of Internal Audit shall provide the Chairman of the Citi Nigeria Board Audit Committee with a summary of cases reported and the result of the investigation.

3. Execution Assessment

3.1 Manager's Control Assessment

3.1.1 The requirements of this Policy must also be included in the relevant Manager Control Assessments (MCA), to the extent required by, and in accordance with the Manager's Control Assessment Standards, which are appended to the **Operational Risk Management Policy**.

4. Roles & Responsibilities

Ref. No	Process	Primary Responsibility
1	Implement a Whistle-Blowing Policy and establish a whistle-blowing mechanism for reporting any illegal or unethical behavior	Board of Citi Nigeria
2	Review reported cases and recommend appropriate action	Internal Audit

3	Render quarterly reports to relevant regulators: a) on Citi's compliance with the provisions of the Central Bank of Nigeria's Whistle-blowing Guidelines b) on Citi's Corporate Governance compliance status c) on all Whistle-Blowing reports; and d) Corporate Governance related breaches	Independent Compliance Risk Management
4	Report annually to the Central Bank of Nigeria on Citi Nigeria's compliance with provisions of the Central Bank of Nigeria's Whistle-blowing Guidelines	Finance/External Auditor
5	Include a Whistle-Blowing compliance status in the audited financial statements	Finance/External Auditor
6	Review this policy every three years and notify relevant regulators of such reviews	Independent Compliance Risk Management

REVISION HISTORY

Date (mo-day-yr)	Version Type	Version Number	Description of Revision
7-2-2020	substantive	4.0	Includes governance and oversight updates of compliance Incidents and requirements for tracking and reporting of significant Incidents and Severity Level 1 or 2 Issues. Provides clarity on escalation standards, expectations and guidance for staff and management in order for the results of significant compliance risk Incidents referred to other areas outside of ICRM to be consistently reported back to the compliance risk management program. References additional risk specific escalation criteria and protocols (no changes to Australia Addendum)
12-11-2020	Substantive	5.0	• New language added to provide guidance for the handling of Sensitive and Confidential Matters • Reference to the Escalation Grid included, which provides guidance for core management reporting of escalatable matters at Citi • New language added to describe the monthly continuous improvement analysis the ICRM Central Incident Escalation Team performs on a sample of Level 1 and 2 Issues to assess whether significant Incidents were appropriately escalated • New language added to incorporate Legal Entity responsibilities into the escalation process • New language added to describe that occurrences escalated or reported outside of the central significant Incident escalation process may still be escalated via the compliance escalation process based on ICRM EMT's, including CCO's, judgement. • Update to include the Nigeria Whistle-blowing Addendum and subsequent retirement of the country-level Policy (ID 9683).