International Professional Practices Framework

Implementation Guide

Code of Ethics: Confidentiality

IIA Code of Ethics Principle 3: Confidentiality

Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so.

Rules of Conduct

Internal auditors:

3.1. Shall be prudent in the use and protection of information acquired in the course of their duties.

3.2. Shall not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organization.

Getting Started

The *International Standards for the Professional Practice of Internal Auditing* require conformance with the Code of Ethics, comprising four principles. Each principle is accompanied by rules of conduct that internal auditors must implement to properly demonstrate the principle. This implementation guide is intended to demonstrate how to achieve conformance with the principle of confidentiality.

Internal auditors should start with a good understanding of their professional obligations, as expressed in the IPPF and any additional professional standards and guidance relevant to the organization and industry within which they work. Membership in professional organizations may help internal auditors stay current with relevant professional obligations.

Information includes data in physical form, such as printed documents, and in electronic form, such as audio, video, and encoded data. Confidentiality involves protecting information from being disclosed to unauthorized individuals and entities, both within and outside the organization. Internal auditors should understand the laws and regulations related to confidentiality and information security for the jurisdictions in which their organization operates, as well as knowing any policies specific to their organization and internal audit activity. Such policies may identify, for example, the type of information that may be disclosed, the parties that must authorize the disclosure, and the procedures to be followed.

Although confidentiality is not explicitly referenced in the *Standards*, requirements related to limiting the dissemination of engagement results are discussed in implementation standards 2201.A1, 2330.A1, 2330.C1, 2410.A3, and 2440.A2. Internal auditors should review those standards, their implementation guides, and relevant supplemental guidance from The IIA.

Considerations for Implementation

Chief Audit Executive

Policies and Procedures

Organizations usually issue information security policies to protect the data they acquire, use, and produce and to ensure compliance with the laws and regulations that pertain to the industry and jurisdiction within which they operate (e.g., the European Union's General Data Protection Regulation or the EU-U.S. Privacy Shield Framework). These policies are implemented through explicit procedures and other controls and typically cover data privacy, record retention, and physical and digital security of information within and outside the organization.

To better understand the impact of legal and regulatory requirements and protections (e.g., legal privilege or attorney-client privilege), the chief audit executive (CAE) should consult with legal counsel. The organization's policies and procedures may require that specific authorities review and approve business information before external release.

The CAE may implement additional policies, processes, and/or procedures that the internal audit activity and external consultants must follow; typically, these are closely aligned with the IPPF's Mandatory Guidance. Internal auditors should follow the policies and procedures set by the organization and the CAE, as well as complying with any relevant laws and regulations.

To protect proprietary information, policies and procedures may require internal auditors to take the following precautions, even when handling information internally:

- Collect only the data required to perform the assigned engagement and use this information only for the engagement's intended purposes.

- Protect information from intentional or unintentional disclosure through the use of controls such as data encryption, email distribution restrictions, and restriction of physical access to the information.
- Eliminate copies of or access to such data when it is no longer needed.

One example of information typically protected from internal disclosure is personally identifiable human resource information; for instance, individual salaries and records of reprimands or personal problems discussed with supervisors and HR personnel. Access to this information might be restricted or monitored through physical controls, such as locked filing cabinets, and through information system controls, including password protection and encryption of data. The CAE should periodically assess and confirm internal auditors' need for access to areas and databanks containing confidential information and should confirm that access controls are working effectively.

The implementation standards that accompany Standard 2330 – Documenting Information require the CAE to control access to the engagement records, in part by developing requirements for retaining the records, regardless of the medium in which each record is stored. These rules must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

Additionally, Standard 2440.A2 requires the CAE to assess the potential risk of releasing assurance engagement results and to restrict the use of assurance engagement results, except as required by laws, statutes, or regulations. Engagement reports typically contain distribution lists that are approved by the agreement of the CAE, senior management, and the board. The standard's accommodation for legal, statutory, and regulatory requirements ensures that the CAE and internal auditors are able to comply with requests by regulators and with transparency laws in public sector organizations.

Training

During meetings or trainings of the internal audit activity, the CAE may discuss the principles, rules, policies, and expectations related to confidentiality. Internal auditors may use the opportunity to brainstorm and discuss the potential impact of sharing various types of confidential organizational information. The CAE may require internal auditors to sign a form acknowledging that they attended such sessions and understand relevant policies, procedures, and expectations. It is especially vital for the CAE, as the leader of the internal audit activity, to set the tone for the value of ethics among the team by upholding the Code of Ethics principles and rules of conduct.

Individual Internal Auditors

Ultimately individual internal auditors are responsible for their personal conformance with the Code of Ethics. This is perhaps most evident in relation to performing internal audit engagements, during which internal auditors may receive confidential, proprietary, and/or personally identifiable information. Internal auditors may handle such information throughout the engagement (e.g., while gathering information about an activity under review and during testing).

According to Standard 2330 – Documenting Information, internal auditors must document sufficient, reliable, relevant, and useful information to support the engagement results and conclusions. Internal auditors should consider the confidentiality of this information when documenting internal audit work and observations in engagement workpapers and reports. The work program or engagement workpaper templates may include reminders about confidentiality; electronic formats may contain automated controls that required internal auditors to acknowledge such reminders before they are able to access and complete their workpaper documentation.

A few standards relevant to planning and performing engagements specifically mention the prudent use and protection of information, as described in Rule 3.1. Internal auditors planning an assurance engagement involving third parties are required to establish a written understanding of the restrictions related to the distribution of engagement results and the access to engagement records (Standard 2201.A1). When releasing the results of an assurance engagement to parties outside the organization, internal auditors must stipulate limitations regarding how the results may be distributed and used (Standard 2410.A3).

To comply with the rules of conduct related to the confidentiality principle, internal auditors must follow established procedures for disclosure, including contacting the correct authority in the organization for permission before disclosing any information. Internal auditors may do this by obtaining written permission and retaining the authorization in their workpapers.

Finally, Rule of Conduct 3.2 emphasizes that internal auditors must not use any information for personal gain. For example, internal auditors should not use insider financial, strategic, or operational knowledge of an organization to bring about personal financial gain by purchasing or selling shares in the organization. Another example is releasing insider knowledge to journalists or via other media without proper authorization. Using insider information to develop a competitive product or selling proprietary information to a competitor also violates this confidentiality rule. Furthermore, internal auditors should not abuse their privilege to access information, such as using access to customer records to look up a neighbor's recent purchases or to view the health records of a celebrity.

Considerations for Demonstrating Conformance

Chief Audit Executive

The CAE may demonstrate support of internal audit confidentiality through evidence of policies, processes, procedures, and training materials implemented to cover confidentiality as it applies to the internal audit activity and the organization. Minutes from meetings and/or trainings where confidentiality was discussed with members of the internal audit activity also evidence the CAE's work to support conformance.

Regarding the release of engagement results, reports, or related information, the CAE demonstrates conformance with the confidentiality principle and rules of conduct by documenting and retaining records of disclosures approved by legal counsel, if applicable, and by senior management and the board. The CAE evidences control of access to records by documenting and communicating internal audit policies and procedures and by implementing mechanisms that restrict access and mitigate the risk of circumventing or otherwise violating these controls.

Individual Internal Auditors

Records of attendance at trainings on confidentiality should be retained, with internal auditors' signatures acknowledging their understanding of confidentiality and relevant policies, procedures, laws, and regulations. Internal auditor performance reviews also may include feedback about whether internal auditors have followed policies and procedures related to confidentiality and the disclosure of information.

Internal auditors demonstrate conformance with engagement record confidentiality by documenting distribution restrictions in engagement workpapers and reports and by retaining authorizations of all disclosures and approved distribution lists. A signed acknowledgment attesting that engagement-related information has been kept confidential may be retained within the work program.

If there are no reports or investigations of individual auditors violating policies, procedures, and rules related to confidentiality, then it is likely that the internal audit activity as a whole is in conformance with the principle.

Applicability and Enforcement of the Code of Ethics

This Code of Ethics applies to both entities and individuals that perform internal audit services.

For IIA members and recipients of or candidates for IIA professional certifications, breaches of the Code of Ethics will be evaluated and administered according to The IIA's Bylaws, the Process for Disposition of Code of Ethics Violation, and the Process for Disposition of Certification Violation. The fact that a particular conduct is not mentioned in the Rules of Conduct does not prevent it from being unacceptable or discreditable, and therefore, the member, certification holder, or candidate can be liable for disciplinary action.

About The IIA

The Institute of Internal Auditors (The IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 190,000 members from 170 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

About Implementation Guidance

Implementation Guidance, as part of The IIA's International Professional Practices Framework® (IPPF®), provides Recommended Guidance (nonmandatory) for the internal audit profession. It is designed to assist both internal auditors and internal audit activities to enhance their ability to achieve conformance with the *International Standards for the Professional Practice of Internal Auditing.*

Implementation Guides describe considerations that may be applied and actions that may be taken to implement The IIA's Mandatory Guidance. Implementation Guides do not detail programs, processes, procedures, or tools.

For other authoritative guidance materials provided by The IIA, please visit our website at https://globaliia.org/standards-guidance.

About The IIA's Code of Ethics

The IIA's Code of Ethics comprises two essential components:

- Four principles relevant to the profession and practice of internal auditing.
- Rules of conduct for each principle that describe behavioral norms expected of internal auditors.

The purpose of The IIA's Code of Ethics is to promote an ethical culture in the profession of internal auditing.

The complete Code of Ethics may be found at https://globaliia.org/standards-guidance/mandatory-guidance/Pages/Code-of-Ethics.aspx.

Disclaimer

The IIA publishes this document for informational and educational purposes. This guidance material is not intended to provide definitive answers to specific individual circumstances. The IIA recommends seeking independent expert advice related to specific situations. The IIA accepts no responsibility for anyone placing sole reliance on this guidance.

Copyright

February 2019