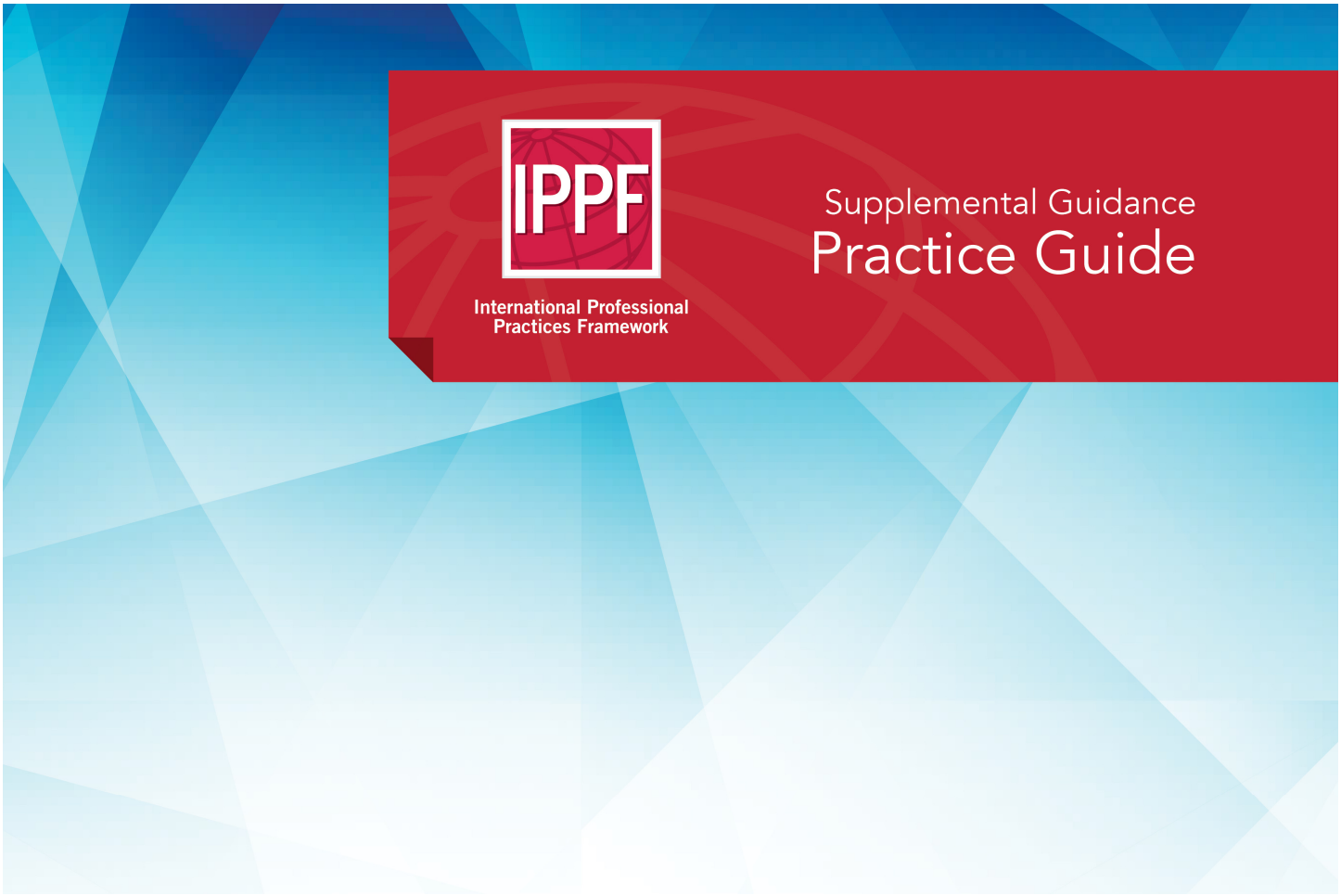


Supplemental Guidance

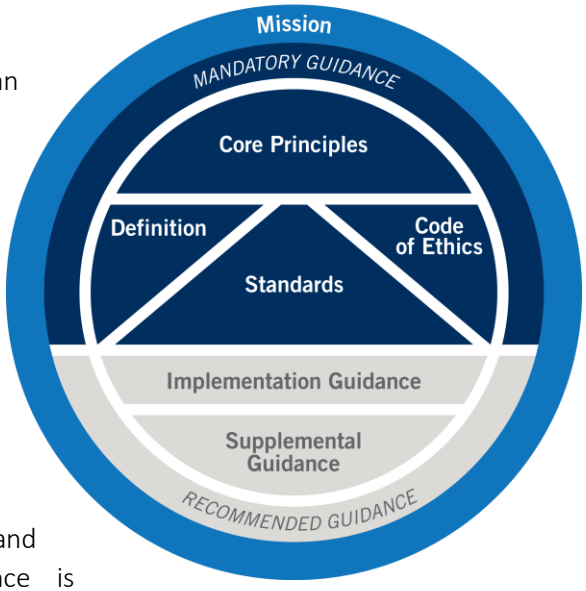
Practice Guide

Auditing Culture

The Institute of Internal Auditors | Global

About the IPPF

The International Professional Practices Framework® (IPPF®) is the conceptual framework that organizes authoritative guidance promulgated by The IIA for internal audit professionals worldwide.



Mandatory Guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The mandatory elements of the IPPF are:

- Core Principles for the Professional Practice of Internal Auditing.
- Definition of Internal Auditing.
- Code of Ethics.
- *International Standards for the Professional Practice of Internal Auditing*.

Recommended Guidance includes Implementation and Supplemental Guidance. Implementation Guidance is designed to help internal auditors understand how to apply and conform with the requirements of Mandatory Guidance.

About Supplemental Guidance

Supplemental Guidance provides additional information, advice, and best practices for providing internal audit services. It supports the *Standards* by addressing topical areas and sector-specific issues in more detail than Implementation Guidance and is endorsed by The IIA through formal review and approval processes.

Practice Guides

Practice Guides, a type of Supplemental Guidance, provide detailed approaches, step-by-step processes, and examples intended to support all internal auditors. Select Practice Guides focus on:

- Financial Services.
- Public Sector.
- Information Technology (GTAG®).

For an overview of authoritative guidance materials provided by The IIA, please visit www.globaliia.org/standards-guidance.

Table of Contents

Executive Summary

The culture of an organization drives how it conducts business and executes its strategies. All organizations have a culture, whether intentionally created or not. Likely there are also subcultures within an organization, especially if multiple locations or campuses exist. Each department or location may have its own unique culture aside from the overarching organizational culture. Global cultural differences also affect the desired objective of an intentional organizational culture. Further, elements of an organization's culture may be in a continuous state of flux.

Poor organizational culture has been identified as the root cause of many serious issues across numerous industries around the world. In response, key business stakeholders, including boards and regulators with responsibility for oversight of the control environment, have heightened their focus on the role of organizational culture and the actions that arise out of that culture to constitute conduct risk management.

One of internal audit's key responsibilities is to assess the adequacy and effectiveness of the internal control environment directly impacted by culture and the conduct that arises from employees acting out and exhibiting their interpretation of the values of that culture. This can be difficult to do as employees of the organization themselves, and it is why objectivity is fundamental to this type of audit. Internal audit, as the third line of defense in an organization's governance framework, is uniquely positioned to assist an organization in evaluating its culture.[1]

This guidance is intended to assist internal auditors in understanding and evaluating the overarching culture of an organization, as well as assessing the existence of subcultures. The conduct that results from organizational culture(s) will be mentioned in this publication but more fully explored and addressed at a later time.

Code of Ethics

Objectivity

Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgments.

International Professional Practices Framework (IPPF), 2017 Edition

1. The Institute of Internal Auditors. The IIA's Position Paper: *The Three Lines of Defense in Effective Risk Management and Control* (Altamonte Springs: The Institute of Internal Auditors, 2013).

Introduction

Culture is difficult to define; however, for the purposes of this supplemental guidance, organizational culture and the conduct that occurs within that culture is defined as follows:

> Culture represents the invisible belief systems, values, norms, and preferences of the individuals that form an organization. Conduct represents the tangible manifestation of culture through the actions, behaviors, and decisions of these individuals.[2]

Note: Terms in bold are defined in the glossary in Appendix B.

This definition captures the complexity of defining and then assessing an intangible organizationwide quality or aspect that comprises human belief systems, social norms, and other psychological factors.

Internal audit teams operating in certain industries and/or jurisdictions are required to assess and regularly report on the appropriateness of their organization's culture and the effectiveness of conduct risk management activities. However, even without regulatory guidance, internal auditors can add value through the objective assessment and reporting of organizational culture and conduct risk management.

This type of work is consistent with internal audit's mission as defined by The IIA, and required by Standard 2110 – Governance. In this way, the internal audit activity can provide management with opportunities to develop a strong internal control framework that aligns with stakeholder expectations and supports **boards**, audit committees, and executive management in their oversight roles.

Mission of Internal Audit

To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight.

International Professional Practices Framework (IPPF), 2017 Edition

This practice guide will help internal auditors understand risks associated with an organization's culture, how effective management of those risks supports a successful control environment, and how to approach an assessment of culture. After reading this guidance, internal auditors should be able to:

- Understand the business significance of culture and conduct risk in an organization's control environment.
- Identify the key components of culture and conduct risk.

2. Elizabeth St-Onge, Ege Gürdeniz, and Elena Belov, *Measuring Conduct and Culture: A How-To Guide for Executives* (New York: Oliver Wyman, 2018), 2. https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/april/Conduct_and_Culture_Measurement_Oliver_Wyman.pdf.

- Understand key stakeholder concerns and expectations related to culture and conduct risk.
- Recognize internal audit's role in assessing and reporting on organizational culture.
- Understand, based on example tools/guidance, possible approaches to assess and report on an organization's culture and management of conduct risk.

Business Significance: Risks and Opportunities

People often behave differently in the corporate environment than they do at home. Culture and conduct have business significance because they are elements of the control environment, which is the foundation for all other layers of control, such as general computer controls and business process controls. If the culture of an organization is toxic, it erodes the effectiveness of all other control layers.

A common factor cited when discussing an organization's culture is "tone at the top." Many studies have shown that most people who change jobs do so because of their immediate boss.[3,4] Common reasons to change jobs include boredom, struggling with work/life balance, and feeling unheard and unappreciated. Interestingly, all of these factors are at least somewhat in the control of the supervisor. Intentionally or not, supervisors set the cultural tone for their team and contribute by operating within the culture of the broader organization. Many leaders are unaware of the importance of their role in setting and modeling an appropriate culture. Thus employees may be confused, unmotivated, or see opportunities to take advantage.

Studying the corporate failures of the last few decades indicates identifiable key risk factors arising from cultural problems. Those risk factors, in no particular order, include but are not limited to:

- Unreasonable expectations including deadlines, profitability, or levels of efficiency.
- Incentives not aligned with values.
- Employees (including internal auditors) lack knowledge of key risk management activities and potential risk impacts.
- An inflexible hierarchy impeding the flow of information up, down, and across the organization.
- A pervasive environment of mistrust toward auditors and regulators including a lack of understanding of the role of controls in achieving business objectives.
- An attitude of hubris (e.g., "That will not happen here." or "That has never happened to us before.")

3. Marcel Schwantes, "Why Do Employees Quit on Their Bosses? Because of 5 Common Reasons Still Not Addressed, Says New Research," *Inc.*, December 21, 2018, https://www.inc.com/marcel-schwantes/why-do-people-quit-their-jobs-exactly-new-research-points-finger-at-5-common-reasons.html.

4. David Novak, "Here's the No. 1 reason why employees quit their jobs," June 21, 2019, https://www.nbcnews.com/better/lifestyle/here-s-no-1-reason-why-employees-quit-their-jobs-ncna1020031.

- Lack of accountability, especially at senior levels of the organization.
- Failure to enforce codes of conduct and related policies and procedures.
- Management (and, in some cases, the board) refusing to acknowledge information contrary to their opinions.
- Disregard of laws and regulations if they are not conducive to the organization achieving its objectives.

For example, if employees are penalized for mistakes (that may or may not be the result of their actions) in an environment of fear and blame, management regularly overrides key controls, and challenge is discouraged, bad actors can operate freely until their behavior becomes the norm. Other employees who behave honestly may leave the organization or become corrupt themselves, resulting in further deterioration of the culture.

Management should be clear on what it will and will not tolerate in terms of its **risk appetite**. This includes culture-related risks. An organization may choose to define actions, situations, or risk impacts related to culture that constitute a breach of its risk appetite parameters and develop a system to facilitate reporting on the remediation status of internal audit or risk management's findings regarding these breaches. (See Appendix D for an example.)

Conversely, a positive, affirmative, open culture supports the organization's attainment of its goals and objectives because it generally creates a more enjoyable place to work, enhances productivity, and leads to overall improved performance in addition to reducing risk exposure.

Healthy organizations have several common cultural characteristics including:

- *Positive tone from the top* – Executive management and the board work together to define the organization's values and proactively emphasize and model those values, ensuring strategies are consistent with the values, and holding management accountable to executing their duties within the organization's risk appetite.
- *Clear communication* – Management reinforces the values and culture through clear communication of expectations across the organization. Methods include formal communications, day-to-day interactions, and meetings with employees, customers, and third parties.
- *Open dialogue* – Management actively gathers and listens to feedback. All levels are open to constructive criticism and problem solving through methods including information obtained from second- and third-line functions via inputs such as well-received and acknowledged employee suggestion/question program, ethics hotlines, open door policies, employees' events and meetings, and more.
- *Employee engagement* – All employees (to the extent possible) are engaged in objective setting and strategy discussions. In larger organizations this may be accomplished through two primary methods: input into setting their own personal goals and objectives; and understanding of how those individual goals and objectives align with the overall

organization's strategy and objectives. When employees are engaged in objective setting, it improves the probability that they are supportive of the objectives and strategies. People who are working toward a mutually agreed upon objective require less external motivation.

- *Incentives aligned with core values –* All employees' compensation, variable compensation, promotions, and other talent management are governed by a clear understanding of the organization's core values and its risk appetite.

The following sections will describe methodologies and options internal auditors may use to assess an organization's culture.

Role of Internal Audit

Some regulators, mostly in the financial services industry, have issued guidance on their expectations for internal auditors regarding their assessments of culture and/or cultural issues. Most organizations in industries such as manufacturing and energy, for example, are under no obligation to comply with such regulatory requirements. Indeed, they may be unaware of their existence.

An organization's management and board are responsible for culture and conduct risk management. However, the internal audit activity may advise them in many ways, such as:

- Identifying root causes not only for areas that have received observations and recommendations from internal audit regarding culture but also for areas judged as operating with best practices. Identifying and analyzing root causes from both perspectives results in powerful tools to gauge frequency and assess how cultural elements are drivers of results in improvement of affected areas.
- Assessing the **governance** structure (roles and responsibilities) related to culture and conduct.
- Assessing the organization's programs for communicating values, strategies, and objectives.
- Assessing the effectiveness of culture-related trainings including code of conduct, ethics, sexual harassment, etc. (e.g., How seriously do employees take the training? Are the delivery methods effective?)
- Performing internal audit engagements that consider employee incentive and hiring programs, disciplinary actions, and escalation protocols, treatment of "whistleblowers" or employees that speak up and escalate issues and other key performance indicators (KPIs) or key risk indicators (KRIs) that may be relevant to the organization's culture.
- Analyzing information related to culture gathered for other purposes in the organization (e.g., analyzing and trending employee survey data).

All of these activities are consistent with Standards 2100 – Nature of Work, 2110 – Governance, 2120 – Risk Management, and 2130 – Control.

In addition, certain attributes are needed for individuals assigned to culture-related risk audit engagements. Internal auditors leading culture-focused engagements should be:

- Familiar with the organization's unwritten rules including hierarchical norms and how employees from different levels communicate with each other.
- Skilled at reading body language and "reading the room" to ensure nonverbal cues are considered appropriately.
- Experienced and/or respected enough in the organization to be able to ask hard questions that may touch on uncomfortable subjects.
- Focused on the objective facts of an engagement rather than their personal feelings about the people or processes involved.

These elements are critical and necessary for all internal auditors in all assignments, but particularly so in the sensitive areas associated with an organization's culture and the offshoots of culture that may exist with departments and individual locations.

As stated by Standard 1100 – Independence and Objectivity, "The internal audit activity must be **independent**, and internal auditors must be objective in performing their work." Standard 1120 – Individual Objectivity states internal auditors must have an impartial, unbiased attitude and avoid any **conflict of interest**. For example, internal auditors who may have been involved with the development and/or implementation of any relevant programs (e.g., employee engagement groups, creating ethics training or codes of conduct) should not be assigned to these engagements. However, small audit activities may have limited options in this regard. If this occurs, Standard 1130 – Impairment to Independence or Objectivity requires that **impairment** in fact or appearance be appropriately disclosed.

These issues must be carefully considered before assigning employees to embark on audits of culture.

Planning and Performing the Engagement

Gather Information

The **chief audit executive** (CAE), or internal auditors assigned by the CAE, should be involved as observers in various meetings throughout the organization regarding values and strategic planning. Internal auditors attending these meetings should be conscious of the information that pertains to or may affect culture. This information will also help internal auditors identify where culture-related risk information is retained in the organization.

An insurance company CAE offers the following advice:

> "An internal auditor increases their chances of understanding whether the culture is good or bad by being involved as observers in committees where management discusses information key to the organization's strategies. Internal auditors should be on the Enterprise Risk Management (ERM) committee. Ideally, it is beneficial for CAEs to attend executive committee meetings as observers. Internal auditors must develop the ability to use their eyes, ears, and minds to watch people interact and think. If internal auditors are not engaged or embedded in the organization's governance entities to see those behaviors on a regular basis, then KPIs and KRIs related to culture may deteriorate unbeknownst to management."

This CAE also suggested attending meetings in which executive management presents financial and performance results. He states internal auditors should watch what people do and say when they talk about risk occurrences.

While gathering information to understand the cultural factors that are subject to the audit, internal auditors should also review prior assessments (e.g., risk assessments, reports by assurance, and consulting service providers), process flows and controls, and interviews of relevant stakeholders. To identify key risks and controls for a culture assessment, internal auditors should have a thorough understanding of the way their organization sets, communicates, and expresses its values. Documents internal auditors may want to review while gathering information include:

- Any value statements (may be labeled mission or vision statements or contained within these documents) published by the organization. Many times these are public and appear on the organization's website.
- Top-level, business-line level, and process-level strategies, objectives, and business plans.
- Risk appetite statements.
- Organization charts (high level and business units) and related reporting lines.
- Roles, responsibilities, and accountabilities of other control functions (e.g., compliance, risk management) and senior management.
- Governance framework.
- Tone at the top and leadership communications with employees.
- Products/services approvals and selling processes.
- Risk escalation protocols.
- Documentation of exceptions and management overrides.
- Codes of conduct/ethics including policies and procedures on speaking up, non-retaliation, and treating customers fairly.
- Ethics hotline information and training materials.
- Results of culture-related training and testing programs (e.g., sexual harassment, ethics, code of conduct).
- Employee survey results.
- Exit interview data.

Resources

Audit Engagement

For detailed instructions on how to plan and scope an audit engagement, see IIA Practice Guide "Engagement Planning: Establishing Objectives and Scope."

Risk Assessment

For more information on how to perform a risk assessment, see IIA Practice Guide "Engagement Planning: Assessing Fraud Risks."

This guide includes a risk assessment "how to" guide that can apply to any topic.

Third Parties

When planning an audit related to culture risks, internal auditors should consider the risks posed by the organization's third-party relationships.

For more information, see IIA Practice Guide, "Auditing Third-party Risk Management."

- Board and relevant committee minutes (e.g., governance, risk, nomination and remuneration, and ethics committees).
- Management's risk and control self-assessments (RCSAs) including management's action plans and their status.
- Relevant culture-related and risk management policies including incentives and compensation policy, requirements, reports, and expectations.
- Recruitment, onboarding, performance management, retention, and exiting processes.
- Status of issues raised by internal audit or other control functions, external auditors, and regulators taking into consideration repeated and long outstanding issues and root causes that may be related to culture.
- External auditor's report on the audited financial statements and letter of representation.

Some of these elements are public knowledge and can be obtained easily. Others will be more difficult and internal audit may have to work with available data to infer a conclusion.

Considering Culture and Conduct Risks in the Audit Plan

As discussed in the Business Significance: Risks and Opportunities section of this guide, risk factors are listed that may make an organization more vulnerable to culture-related incidents. Each risk factor — individually or aggregated — has the potential to manifest in a risk occurrence that may damage the organization's ability to meet its objectives. Since they are strategic in nature, these risk factors originate in senior levels of the organization and should be integrated into the risk assessment portion of annual audit planning.

Risk Assessment

To perform an audit of culture-related subjects, internal auditors may refer to the risk assessment in their overall annual internal audit plan to identify risks to the organization's culture generally and then narrow the focus of a preliminary risk assessment to identify the specific risks they intend to cover in the audit engagement. Culture-related risks can be identified anywhere in the organization, so it is important that internal audit conduct a thorough risk assessment as a guide in planning an engagement that will be of benefit to management and the board.

As internal auditors conduct their engagement-level risk assessments, they should review past workpapers and consider any past engagements that may contain information relevant for an organizational culture audit. Risks and controls may be gathered from the information available to internal auditors during the information gathering phase.

The results of this risk assessment will assist the CAE in determining the appropriate engagement approach, objectives, and scope. It will also assist the CAE in determining whether the resources available to the internal audit activity have the appropriate skill sets to be effective.

Example of Talent Acquisition Audit Including Cultural Risk Factors, part 1

Mapping risks to cultural risk factors is similar to mapping risks to their corresponding controls. Choosing talent acquisition as an example audit unit, Figure 1 shows how internal auditors may map the risks of the talent acquisition process to the cultural risk factors.

Based on internal audit's judgment, the talent acquisition risks that correspond to a particularly concerning cultural risk factor may be included in an audit, even though their impact and likelihood scores may not indicate they are key risks.

After internal auditors have identified and prioritized the risks, the next step is determining controls, if any, are in place to mitigate those risks and design tests for those controls. All documents generated by the risk assessment (e.g., heat map, risk and control matrix) should be included in the engagement workpapers.

Figure 1 offers an example of mapping the talent acquisition risks in the strategic risk category to the cultural risk factors.

Cultural Risk Factors

- Unreasonable expectations including deadlines, profitability, or levels of efficiency.
- Incentives not aligned with values.
- Employees (including internal auditors) lack knowledge of key risk management activities and potential risk impacts.
- An inflexible hierarchy impeding the flow of information up, down, and across the organization.
- A pervasive environment of mistrust toward auditors and regulators including a lack of understanding of the role of controls in achieving business objectives.
- An attitude of hubris (e.g., "That will not happen here." or "That has never happened to us before.")
- Lack of accountability, especially at senior levels of the organization.
- Failure to enforce codes of conduct and related policies and procedures.
- Management (and, in some cases, the board) refusing to acknowledge information contrary to their opinions.
- Disregard of laws and regulations if they are not conducive to the organization achieving its objectives.

Figure 1: Talent Acquisition Risks and Cultural Risk Factors

Risk Category: Strategic	
Talent Acquisition Risks	**Cultural Risk Factors**
▪ Restrictions on work visas and immigration. ▪ Failure to identify skill sets required for key or specialized positions. ▪ Reactive hiring strategy. ▪ Misalignment between the organization's and the Human Resources department's strategies, goals, and objectives. ▪ Competition between business lines for personnel.	▪ Management (and, in some cases, the board) refuses to acknowledge information contrary to their opinions. ▪ Inflexible hierarchy impedes the flow of information up, down and across the organization. ▪ An attitude of hubris (e.g., "That will not happen here." or "That has never happened to us before.")

Planning the Engagement

Auditors may use accessible information from past audits and key processes and controls related to culture to develop an audit of broad measures of an organization's culture. This engagement workplan could be constructed in a variety of ways. Three examples are:

1. Integrating culture risk factors into all engagements (integrated approach).
2. Selecting a set of key processes and controls related to culture, developing an engagement workplan, and performing targeted testing on the selected areas. This testing may be supplemented with interviews of a sample of employees in which auditors ask questions targeted to assess culture (targeted approach).
3. Top-down culture assessments that start with tone at the top and move down through all layers of the organization to individual employees (top-down approach).

A Common Risk Language

One key factor internal auditors should keep in mind is that they must speak the same language as their organization and move in the same direction regarding culture.

Management can and should decide what works for them in terms of establishing and communicating culture.

Internal auditors should not feel they are compromising by designing culture-related audits within management's framework. That is making the internal auditor's job easier. It makes it more powerful because findings are communicated back in words the organization understands.

Any of these approaches would allow internal auditors to develop a list of relevant cultural risk factors and map their audit results to those factors. They may spot trends or common themes that could be presented to senior management and the board.

Internal auditors should be mindful of the terminology they use when identifying and assessing cultural issues within their organization. The words "culture," "ethics," or other related terms may be inappropriate or imprecise given the organization's social and cultural context. These words may also be difficult to translate accurately. If this is the case, internal auditors should use words and phrases that have clear and understandable meaning for their stakeholders.

The CAE should consult with human resources, legal, and/or the relevant board member (i.e., audit committee chair) to discuss the engagement plan before beginning the audit.

Standard 2210 – Engagement Objectives

If the CAE is using the integrated approach and embedding testing of cultural issues in a regular audit, specific culture-related objectives would not be needed unless requested by management or the board. However, if the CAE is using the targeted approach focusing on cultural factors, then the engagement objectives should be tied to the organization's stated core values.

Prior to the engagement, the CAE should discuss how internal auditors will approach interviewing management due to the sensitivity of cultural issues. Preferably, interviews would be conducted by experienced internal audit team members. Less experienced team members may benefit by attending planning sessions of this type to complement and develop their skill sets.

Objectives of Assurance Engagements

- Reflect risks to the business objectives of the area or process that were assessed as significant during the preliminary risk assessment (Standard 2210.A1).
- Consider the probability of significant errors, fraud, noncompliance, and other exposures (Standard 2210.A2).
- Identify appropriate evaluation criteria (Standard 2210.A3).

Standard 2220 – Engagement Scope

From a scope perspective, internal auditors should integrate discussions and testing surrounding the organization's core values. The approach selected will help guide execution. If no core values statements exist, the CAE should consider proxies such as ethics policies, the code of conduct, risk appetite statements, etc., as discussed in the Gather Information section of this guide.

Standard 2230 – Engagement Resource Allocation

Certain skills sets are needed for those assigned to culture-related risk audit engagements. In conformance with Standard 2230 – Engagement Resource Allocation, the CAE should assess the skills of internal audit team members periodically to ensure that the internal audit activity has the appropriate skills to provide meaningful information and insight to management on culture-related risks.

A key factor in determining resource allocations is integrating new auditors into audits where culture or cultural risk factors will be assessed. If the internal audit activity has high turnover, new auditors may require briefing on these issues. As such, it may be beneficial to have new auditors sit in on interviews conducted by more experienced audit team members, specifically when sensitive cultural issues will be discussed with management. This can be a training tool to aid new auditors in becoming familiar with an organization's jargon or familiar terms, and to observe the nuances of such discussions. This is also a suitable tactic for auditors who may encounter unique situations such as language barriers with an employee's native tongue.

The right question asked the wrong way may hamper a productive interview. CAEs should consider including new auditors in brainstorming sessions, risk assessments, and so on, to improve their knowledge and understanding specifically in regard to issues of culture. This can be particularly important for auditors conducting interviews in the field for organizations with a global footprint, which may have particular and broader cultural protocols.

Behavioral Interviewing

Interview techniques attempt to assess not only the subject's actions but also to determine their motivations, beliefs, and underlying values that create the subconscious filter through which they make decisions.

Some organizations work with organizational psychologists and/or general psychologists to either perform the interviews and analysis of the data or to assist in the process.

For further information on behavioral interviewing and other related techniques, see "Supervision of Behaviour and Culture: Foundations, practice & future developments" by DeNederlandscheBank (2015) https://www.dnb.nl/en/binaries/Book%20Supervision%20of%20Behaviour%20and%20Culture_tcm47-380398.pdf

If work regarding culture is performed by another assurance provider, the CAE should also confirm the work is objective and thorough. As noted in Standard 2050 – Coordination and Reliance, the CAE should carefully consider the competency, **objectivity**, and due professional care of other providers, as well as clearly understanding the scope, objectives, and results of their work. Responsibility for ensuring adequate support exists for the conclusions and opinions reached by the internal audit activity rests with the CAE.

Standard 2330 – Documenting Information

During planning, internal auditors document information in engagement workpapers. This information becomes part of the engagement work program that must be established to achieve the engagement objectives, as required by Standard 2240 – Engagement Work Program.

The process of establishing the engagement objectives and scope may produce any or all of the following workpapers:

- Process maps.
- Summary of interviews.
- Preliminary risk assessment (e.g., risk and control matrix and heat map).
- Rationale for decisions regarding which risks to include in the engagement.
- Criteria that will be used to evaluate the area or process under review (required for assurance engagements, according to Standard 2210.A3).

Given the sensitivity of some of the views expressed during an audit of culture-related risks, safeguards may be necessary to ensure that working papers are only accessible to those in the audit department with a "need to know" (e.g., anonymizing the interviewees and limiting access to the "key" that identifies who is represented).

Performing the Engagement

As indicated, there are three main approaches to auditing an organization's culture. The integrated approach considers culture risk factors in all engagements. The targeted approach involves selecting a set of key processes and controls related to culture and developing an engagement workplan that tests them across the organization. The top-down approach is a comprehensive audit of all culture-related activities within an organization.

1. Integrated Approach

Example of Talent Acquisition Audit Including Cultural Risk Factors, part 2

Returning to the example talent acquisition audit engagement, Figure 2 illustrates the integration of cultural risk factors. As shown in these examples, consideration of cultural risk factors may result in additional testing, expanded samples, or cross-referencing other audits.

The risk "Reactive Hiring Strategy" was selected from the Talent Acquisition Risks listed in Figure 1, including hypothetical results of control testing, and observations and recommendations.

Figure 2: Example of a Talent Acquisition Process Audit

Risk Category: Strategic	Risk: Reactive Hiring Strategy

Audit Process

Key Controls

- Adequate and timely budget creation, review, and approval process mandated by time limits in the budgeting policy.
- Hiring requests matched to budget information.
- Timely posting of positions.

Control Test Steps

- Review budgets and hiring plans for business lines and discuss the process to develop a plan with management.
- Ask management how they approach the recruiting and hiring process, specifically to determine at what point they determine additional resources are required. Verify management's comments with HR representatives.
- Review a sample of requests for resources communicated from management to HR. Determine the reasonableness of the time lag between this communication and posting a position.

Control Testing Results

- Walk-through of budgeting process completed.
- Budget creation, review, and approval within the required time limits of the budgeting policy.
- Management reports they submit hiring requests within 10 days after budgets are approved, which is within the required time limits of the budgeting policy.
- Total hiring requests submitted for audit year: 100.
- Sample size: 20
- Obtained evidence that all requests are submitted timely and matched budgetary expectations.
- Obtained evidence of posting for 20 sampled positions. Postings were available an average of 90 days after requests received.

Observations and Recommendations

Observations

- Requests are submitted to the business line HR director. Directors are taking an average of 60 days to review requests, approve them, and send them to the unit's HR representative for posting.
- By the time positions are posted, the business has lost 25% of the resources they budgeted for the year negatively impacting production. HR directors report heavy workloads as the root cause of the delay between request and posting.

Recommendations

- Review resource levels, job descriptions, and organizational charts for HR departments. Obtain benchmarking information for similar organizations. Analyze people, processes, and technology to determine if additional resources are needed or process streamlining/reengineering is appropriate.
- See **Cultural Risk Factors** for further recommendations.

Once this audit program is complete, internal auditors may identify any risks, controls, and observations and recommendations that relate to the cultural risk factors. This analysis may lead to internal auditors completing additional procedures, root cause analysis, and, perhaps, additional observations and recommendations as shown in Figure 3.

Figure 3: Extended Recommendations for Cultural Risk Factors

Risk Category: Strategic	Risk: Reactive Hiring Strategy
Cultural Risk Factors	
Factors Present	
■ Unreasonable expectations including deadlines, profitability, levels of efficiency, etc. ■ Employees lack knowledge of key risk management activities and potential risk impacts. ■ Inflexible hierarchy impedes the flow of information up, down, and across the organization.	
Recommendations	
■ Test whether business units are hiring temporary employees to fill gaps during the wait for hiring or are utilizing other less desirable methods to obtain their production goals. Methods could include: unapproved (or inadequately reviewed and approved) outsourcing to third parties, illegal labor, pushing junior personnel into positions they are not trained to execute. ■ Determine whether HR directors have a grasp of the nature and importance of the positions they are asked to fill. ■ Measure/monitor associated KRIs, such as injury-free days, production performance, overdue projects, reserve accounting results, vendor exception reports (accounts payable), denied purchase orders, etc.	

Other additional procedures to integrate cultural risk factors into regular audits for testing in this manner may include:

- Reviewing the results of employee surveys for the area or process under consideration.
- Gathering documentation regarding ethics complaints, whistleblowing situations, or other incidents involving management as individuals or as a group for the area or process under consideration.
- Gathering documentation illustrating management taking ownership of recommendations issued by internal audit and ensuring the associated action plans are completed timely and with quality.
- Recording observations regarding management's complete and timely participation in audit engagement interviews and/or document requests, etc.

2. Targeted Approach

A targeted engagement may consist of choosing a key process related to culture and building an engagement around the culture-related controls. Areas to cover under the targeted approach may include:

Tone at the Top

- Congruence between the discussions occurring at regularly scheduled meetings (and/or analyst calls) and to employees in internal meetings when executive management presents financial and performance results.
- Reviewing senior management's employee presentations to ensure slides on the organization's desired culture and "doing the right thing" are included.

- Reviewing the results of employee surveys paying particular attention to the questions related to ethical behavior, organizational culture, management expectations, tone at the top, and responses to open-ended questions.
- Reviewing comments obtained in recent exit interviews.

Accountability

- Examine performance review documents for assurance that disciplinary actions are invoked as outlined in the organization's code of conduct, employee manual, and/or compensation policy.
- Review complaint management processes and assess or determine:
  - How complaint information is gathered, stored and reported including those investigated, where action was taken and complaints that are pending accompanied by their aging status.
  - Whether proper segregation of duties and access controls are in place and functioning.
  - The quality and timeliness of complaint information reported to management.
  - If complaint information results in organizational change.
- Review exception reports for applicable processes and/or controls to determine:
  - If management overrides of controls are recorded on exception reports.
  - If management overrides are consistently reviewed and approved by an independent party.
  - If one unit has more management overrides than other similar units. If so, determine the cause.
- Review how many audit issues are open or past due or re-opened since the last audit. If managers are closing audit issues or action plans to meet deadlines without fully resolving issues that should be noted in terms of culture and conduct.

Ethics Programs and Code of Conduct

- Assess the process(es) used to develop and/or update the organization's ethics program and code of conduct including:
  - Subject matter coverage is reviewed and updated according to good practices.
  - Appropriate parties are included in the review process.
  - Input is obtained from the board and executive management.
  - Input from related committees (ethics, risk, compensation, etc.) is considered.
  - Audit committee review and approval is documented and validated.
- Review documentation demonstrating ethics complaints, whistleblowing situations, or other incidents involving management as individuals or as a group are investigated and addressed promptly and in a manner consistent with the organization's ethics policies, escalation protocols, code of conduct, etc.

- Internal auditors should consider the presence of evidence of management or other employees retaliating against those who report issues.
- Statistical trending of complaints, whistleblowing situations, or other incidents to determine the effectiveness of controls in place.

- Review rates of completion and pass rates for electronic training programs including ethics, code of conduct, core values, etc.

Whistleblowing/Complaint Audit

Internal audit's primary objective in an audit of an organization's culture is to evaluate governance, how it manifests within the culture, and how employees conduct business and themselves. Questions to ask include:

- Are questionable issues reported?
- If issues are reported, is there a defined escalation protocol depending on the type of issue (ethics, sexual harassment, etc.)?
- Are issues escalated according to an established protocol?
- Is there a "speak up" culture that makes employees comfortable escalating issues that may occur on any level of the organization?

At the conclusion of an audit engagement, the internal audit activity is advised to praise positive conduct. Standard 2410.A2 states "Internal auditors are encouraged to acknowledge satisfactory performance in engagement communications." For example, after a culture audit and obtaining permission from the parties involved, one bank chose to publish case studies of complaints that had positive outcomes. These were posted in elevators, break rooms, and other areas where employees gather to foster an atmosphere of transparency.

3. Top-down approach

Performing a top-down approach to auditing culture may be a difficult task in most organizations due to the sensitivity of the topic and the difficulty of obtaining reliable information. However, there are internal audit activities developing culture audit programs and covering the key aspects of their organizational culture as shown in this case study:

A Case Study

One global bank chose to blend all three approaches to obtain a comprehensive top-down audit of its culture. The first step was to distribute questionnaires to assess the level of cooperation, openness, and ethical standards as perceived by employees at all levels of the organization. A quarterly snapshot of the state of the organization's culture was gleaned from the questionnaire results, which were then presented to management.

Subsequently, internal audit integrated information gathered from the questionnaires into audits that were not culture focused by including a statement regarding the same factors (cooperation, openness, and ethics) in every audit. For planning purposes, they gathered all the questionnaires and snapshots completed within the last audit cycle and aggregated the responses. Responses were included in the top-down culture audit report.

At the senior management level, a Conduct and Values Committee assessed situations such as internal fraud risks, harassment claims, and more. This committee also examined risk management, compliance, compensation, and sales practices, and used metrics they evaluated on a monthly basis.

To compile their top-down culture audit report, the CAE took the committee's information and integrated it with the questionnaire results and other culture-related audit activities as explained.

In the end, the organization had a comprehensive view of its cultural risks and how the organization managed those risks. Data trends from these activities are now analyzed on an ongoing basis, enabling the organization to determine its success rate or failure to improve according to its own cultural metrics.

Additional Considerations

In testing culture risk management activities, CAEs should ask, "What is the objective of this control? Is it to investigate the incidents and find a solution, or is it to institute better controls to prevent the behavior?" The objective should be to institute better controls to prevent bad behavior.

Information and testing protocols regarding these culture risk management activities may not be obvious. The CAE should ensure the auditors' workpapers include sufficient information to support the audit. The IPPF states, in part, "Sufficient information is factual, adequate, and convincing so that a prudent, informed person would reach the same conclusions as the auditor," and "Relevant information supports engagement observations and recommendations and is consistent with the objectives for the engagement."

Reporting

Standard 2400 – Communicating Results is self explanatory in that results of an engagement must be communicated. According to the interpretation of Standard 2410 – Criteria for Communicating, "Opinions at the engagement level may be ratings, conclusions, or other descriptions of the results. Such an engagement may be in relation to controls around a specific process, risk, or business unit. The formulation of such opinions requires consideration of the engagement results and their significance."

CAEs should be aware that the *Standards* do not require a specific reporting format. Not all internal audit reports must be written or include ratings. Alternatives to a traditional report may be considered specifically for issues of culture. Reporting on these issues may be sensitive, but the CAE has a responsibility to openly communicate to senior management and the board.

Communicating Results of a Culture-focused Audit

Aggregating results is challenging. How do you report results when it's a more conceptual, less tangible audit?

Internal auditors might conduct a session with the board to discuss culture-related observations once a year. This session could be an informal discussion, but CAEs should preview results with management before any discussion with the board.

An organization's culture can be an intangible, fluid thing, and the CAE must be free to communicate issues that may not rise to the level of a formal control deficiency/recommendation, in addition to any formal, written recommendations identified in the report.

Appendix A. Related IIA Standards and Guidance

The following IIA resources were referenced throughout this practice guide. For more information about applying the *International Standards for the Professional Practice of Internal Auditing*, please refer to The IIA's Implementation Guides.

Code of Ethics
Principle 1: Integrity
Principle 2: Objectivity
Principle 3: Confidentiality
Principle 4: Competency
Standards
Standard 1100 – Independence and Objectivity
Standard 1120 – Individual Objectivity
Standard 1130 – Impairment to Independence and Objectivity
Standard 2050 – Coordination and Reliance
Standard 2100 – Nature of Work
Standard 2110 – Governance
Standard 2120 – Risk Management
Standard 2130 – Control
Standard 2210 – Engagement Objectives
Standard 2220 – Engagement Scope
Standard 2230 – Engagement Resource Allocation
Standard 2240 – Engagement Work Program
Standard 2310 – Identifying Information
Standard 2330 – Documenting Information
Standard 2400 – Communicating Results
Standard 2410 – Criteria for Communicating
Guidance
Practice Guide "Engagement Planning: Establishing Objectives and Scope," 2017.
Practice Guide "Engagement Planning: Assessing Fraud Risks," 2017.
Practice Guide "Evaluating Ethics-related Programs and Activities," 2012.
IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control, 2013.

Appendix B. Glossary

All terms identified here are taken from The IIA's *International Professional Practices Framework* "Glossary," 2017 edition.

board – The highest level governing body (e.g., a board of directors, a supervisory board, or a board of governors or trustees) charged with the responsibility to direct and/or oversee the organization's activities and hold senior management accountable. Although governance arrangements vary among jurisdictions and sectors, typically the board includes members who are not part of management. If a board does not exist, the word "board" in the *Standards* refers to a group or person charged with governance of the organization. Furthermore, "board" in the *Standards* may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an audit committee).

chief audit executive – Describes the role of a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the mandatory elements of the International Professional Practices Framework. The chief audit executive or others reporting to the chief audit executive will have appropriate professional certifications and qualifications. The specific job title and/or responsibilities of the chief audit executive may vary across organizations.

conflict of interest – Any relationship that is, or appears to be, not in the best interest of the organization. A conflict of interest would prejudice an individual's ability to perform his or her duties and responsibilities objectively.

governance – The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

impairment – Impairment to organizational independence and individual objectivity may include personal conflict of interest, scope of limitations, restrictions on access to records, personnel, and properties, and resource limitations (funding).

independence – The freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner.

objectivity – An unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others.

risk appetite – The level of risk that an organization is willing to accept.

Appendix C. References and Additional Reading

References

Cohn, Alain, Ernst Fehr, and Michel André Maréchal. "Business culture and dishonesty in the banking industry," *Nature, International Journal of Science*, 516 (November 19, 2014): 86–89. https://doi.org/10.1038/nature13977.

Cressey, Donald R. "The Criminal Violation of Financial Trust," *American Sociological Review*, 15, no. 6 (1950): 738-743. https://doi.org/10.2307/2086606.

Raaijmakers, Mirea, Wieke Scholten, Mélanie Rouppe van der Voort, Anousha Wajer, Wijnand H.J.M. Nujits, Moritz Römer, Jildau Piena, Melanie de Waal, and Ingeborg Rademakers. *Supervision of Behaviour and Culture: Foundations, practice & future developments*. DeNederlandscheBank, Eurosysteem. Netherlands: DNB Repro & Post Department, 2015. https://www.dnb.nl/en/binaries/Book%20Supervision%20of%20Behaviour%20and%20Culture_tcm47-380398.pdf.

St-Onge, Elizabeth; Ege Gürdeniz, and Elena Belov. *Measuring Conduct and Culture: A How-To Guide for Executives.* New York: Oliver Wyman, 2018. https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/april/Conduct_and_Culture_Measurement_Oliver_Wyman.pdf.

The Institute of Internal Auditors. The IIA's Position Paper: *The Three Lines of Defense in Effective Risk Management and Control*. Altamonte Springs: The Institute of Internal Auditors, 2013. https://global.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf.

Additional Reading

Fountain, Lynn. *Raise the Red Flag: An Internal Auditor's Guide to Detect and Prevent Fraud*. Altamonte Springs, FL: Institute of Internal Auditors Research Foundation, 2015. https://bookstore.theiia.org/raise-the-red-flag-an-internal-auditors-guide-to-detect-and-prevent-fraud.

Jex, Susan, and Eddie J. Best. *A Journey Into Auditing Culture: A Story and a Practical Guide.* Lake Mary, FL: Internal Audit Foundation and Grant Thornton – United Kingdom, 2019. https://bookstore.theiia.org/a-journey-into-auditing-culture.

Appendix D. Sample Culture Monitoring and Reporting Formats

Consulting Service Provider (Europe) – Culture Risk Monitoring and Reporting

A European provider of professional services developed a plan, which is revised and documented annually, to communicate business plan objectives to its employees. All employees have access to this plan on the company's intranet.

The plan lists each business objective and notes the corresponding communication objectives as shown in this excerpt:

Business Plan Objectives
1. Continuously improve the quality and productivity of the service we provide.
Communication Objectives
1.1 Ensure partners, clients, and employees (and directors and members) know and understand what standards of service are expected, as well as the actual standards they are providing/receiving.
1.2 Ensure partners, clients, and employees (and directors and members) have a means to tell the company what their expectations are for standards of service delivery.
1. 3 Ensure partners, clients, and employees (and directors and members) have a means to give and/or receive feedback on whether their expectations were met in the delivery of service.

This plan also identifies the different audiences for this communication including but not limited to employees, board of directors, partners, and clients. It further identifies which communication methods are most effective for each of those audiences individually. Some of the methods are noted in the following excerpt:

- Face to face (informal, or formal meetings and presentations).
- Telephone.
- Email.
- Social media.
- Website.
- Intranet.

Frequency of communications is described in the plan. All information is reflected in an additional document that lists processes the company has established to ensure its communication objectives are embedded within the organization as shown in the following excerpt:

Communication Process	Communication Objectives
Policies and procedures, guides, and manuals updated annually and available on the intranet for employees. Key messages posted for significant changes.	Ensure all partners, clients, and **employees** know and understand what standards of service are expected to deliver services as well as the actual standards they are providing/receiving. Ensure all partners, clients, and **employees** know and understand what we mean by sustainable. Ensure all **employees** know what working environment to expect.

Further, this communication plan extends to a manual for employees instructing them on how they are expected to communicate with each other and with the other audiences. For example, employees are coached to "respect each other's opinions" and to "rely on each other to act as critical friends."

Internal audit can use policies and procedures such as this in an audit program designed to assess the effectiveness of management's plans regarding communication of the company's core values.

Fintech Company (Global) – Risk Appetite

A fintech company focused on digital platforms to facilitate multi-asset market access for traders and other investors has a rigorous culture assessment embedded into its operational risk management processes. This company measures any breaches of its risk appetite parameters and has a system to facilitate reporting on the remediation status of internal audit or risk management's findings regarding these breaches.

A quarterly report on risk appetite breach indicators regarding culture is generated, and an excerpt is featured below.

These reports are used by a variety of control functions within the company including internal audit on a quarterly basis to monitor key risk indicators related to culture. These reports are also produced as part of the escalation protocol should a breach occur that exceeds certain parameters.

Risk Category: Risk Culture

Risk Appetite Statement

- This department has no appetite for violation of the company's code of conduct, policies and procedures.
- This department has a low appetite for high priority audit recommendations that are overdue.

Breach Indicators	Source	Status
Risk Appetite: Number of large events caused by failure to follow the code of conduct.	Operational Risk	
Training: Percentage of employees who have not completed mandatory ethics and compliance training.	Compliance	
Communication: Percentage of critical business activities where documentation has not been updated and approved according to policy.	Operational Risk	
Audit: Number of high priority audit recommendations more than 30 days overdue.	Internal Audit	
Number of violations resulting in disciplinary action.	Human Resources	1

Acknowledgements

Guidance Development Team

Jose Esposito, CIA, CRMA, Peru (Chairman)
Stacey Schabel, CIA, Project Lead, United States
Trevor Brookes, CIA, CRMA, Bermuda
Ian Stuart Lyall, CIA, CCSA, CGAP, CRMA, Australia
John J. Mickevice, CIA, CRMA, United States
Juergen Rohrmann, CIA, Germany
Teis Stokka, CIA, CRMA, Norway

Global Guidance Contributors

Thomas Bang van Dijk, CIA, CFSA, CRMA, Denmark
Tan Dang, CIA, Vietnam
Najeeb Haq, CIA, CFSA, Canada
Adrian Kyburz, CIA, CRMA, Switzerland
Silvia Tapia Navarro, Mexico

IIA Global Standards and Guidance

Jeanette York, CCSA, Director (Project Lead)
Jim Pelletier, CIA, CGAP, Vice President
Cassian Jae, Managing Director
Anne Mercer, CIA, CFSA, Director
Michael Padilla, CIA, Director
Chris Polke, CGAP, Director
Shelli Browning, Technical Editor
Lauressa Nelson, Technical Editor

The IIA would like to thank the following oversight bodies for their support: Financial Services Guidance Committee, Guidance Development Committee, Information Technology Guidance Committee, Public Sector Guidance Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, and International Professional Practices Framework Oversight Council.

About The IIA

The Institute of Internal Auditors (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 more than 170 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

Disclaimer

Copyright

November 2019

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.theiia.org