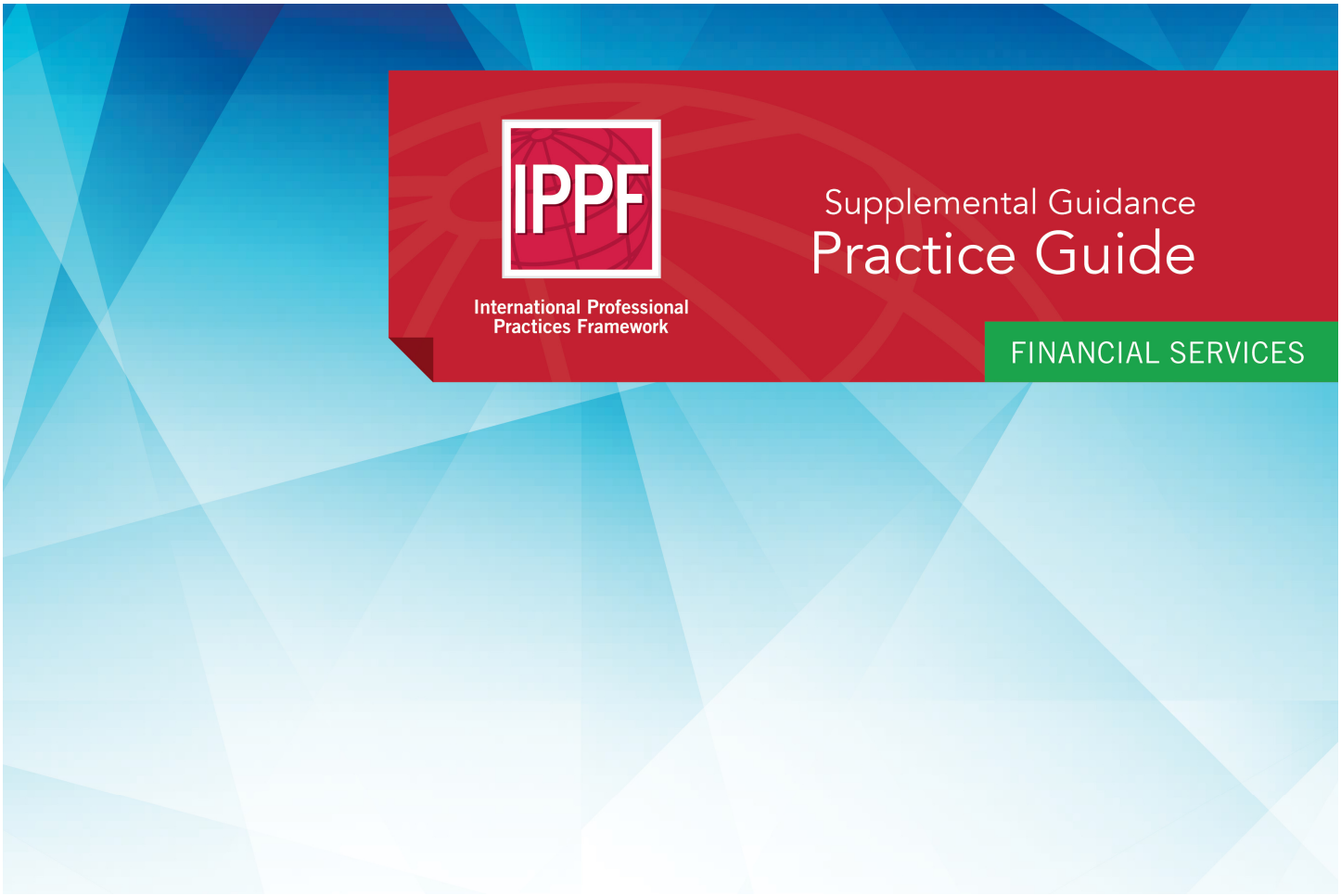
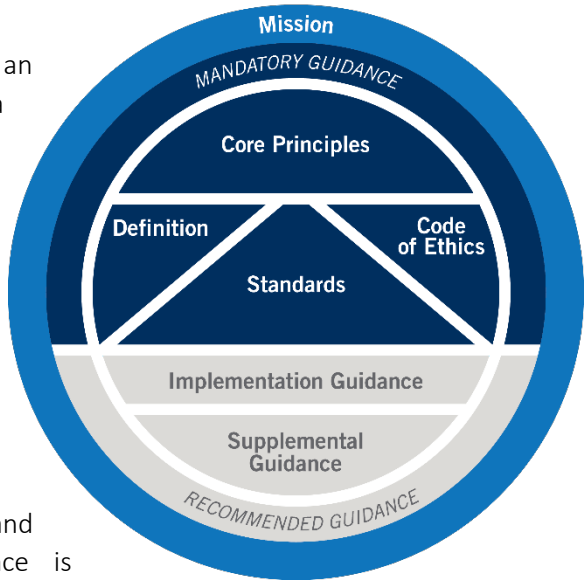


Auditing Conduct Risk

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

Organizational culture — and how an organization comports itself with regard to conduct — drives how business is done. It also underlies the effectiveness of the control environment, which supports the achievement of an organization's objectives.

Poor culture and ineffective management of employee conduct has contributed to numerous business failures and has been identified as a root cause of a number of serious issues. In response, key financial services stakeholders, including boards and regulators with responsibility for oversight of the control environment, have heightened their focus on the appropriateness of organizational culture and the effectiveness of conduct risk management.

One core role of internal audit is to assess the adequacy and effectiveness of the internal control environment. The purpose of this guidance is to assist internal auditors in understanding and evaluating the management of conduct risk.

Introduction

The issue of conduct is not easily separated from an organization's culture; rather, it is a distinct segment of culture as a whole.

Regulators and other key stakeholders expect organizations to operate with strong ethical values that underlie an effective control environment. Audit teams operating in certain industries and/or jurisdictions are expected to assess and regularly report on the appropriateness of their organization's culture and the effectiveness of conduct (used throughout this guide as a noun rather than a verb) risk management activities. Some financial services regulators, specifically, have formalized these expectations in standards and other guidance.

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

Resource

For more information about organizational culture and approaches to include culture and conduct risks in audit engagements, see IIA Practice Guide "Auditing Culture."

Internal auditors can add value through the assessment and reporting of the organization's conduct risk management. The **internal audit activity** can help drive strong internal control risk management frameworks (including conduct risk) that align with stakeholder expectations, supporting boards, audit committees, and executive management in their oversight roles. After reviewing this guidance, internal auditors should be able to:

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

- Understand key stakeholder (including regulator) concerns and expectations related to conduct risk.
- Understand internal audit's role in assessing and reporting on organizational culture and management of conduct risk.
- Understand an approach to assess and report on an organization's culture and management of conduct risk.

Business Significance: Risks and Opportunities

An individual's conduct at work can differ from their behavior anywhere else. For many, an organization lacking a strong ethical culture or presence of management accountability is akin to a license to misbehave, or at least look the other way while others do so. According to an article from *Harvard Business Review* referring to a study conducted by two research organizations:

> One-third of survey respondents believe their company doesn't consistently hold people responsible for misconduct. When employees are under the impression that there are no consequences, or that consequences are handed out unevenly, they may use it as both a justification for not reporting poor behavior (why bother?) and as a reason to be less careful about their own actions.[1]

Further, the article cited the original study's point that "28% of employees strongly agree that there is alignment between their company's actions and its stated values." That leaves a substantial number of employees who could be viewed as a risk in terms of personal conduct to their organizations.

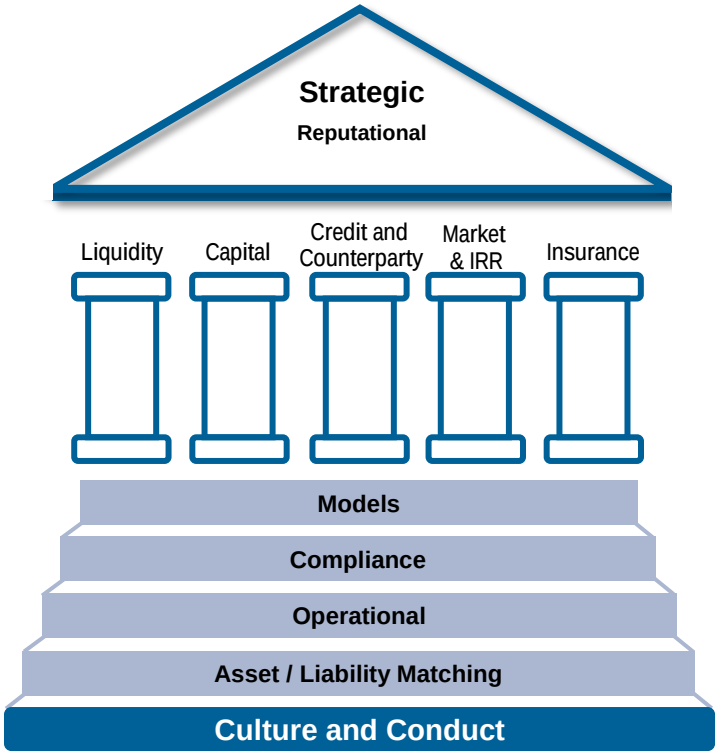
These numbers and the unspoken implications point to both risks and opportunities. An apathetic culture may leave an organization open to multiple risks — including conduct risk — while an organization boasting a strong ethical culture that is borne out by audits, employee surveys, and other tools to measure behavioral tendencies is on its way to mitigating a significant risk.

Speaking the Same Language

To understand the risks facing their organizations, employees must understand the terminology associated with risk management, compliance, and internal auditing. One tool to communicate risk information across an organization is a risk framework. The IIA's Financial Services Guidance Committee has developed a comprehensive risk framework specifically for financial services organizations. The risk framework depicted in Figure 1 considers the major areas of risk applicable to the financial services industry on a global basis, with culture and conduct featured prominently as a foundational support.

1. Sarah Clayton, "6 Signs Your Corporate Culture Is a Liability," *Harvard Business Review*, December 5, 2019, https://hbr.org/2019/12/6-signs-your-corporate-culture-is-a-liability.

Figure 1: The IIA's Financial Services Risk Framework



Source: The Institute of Internal Auditors.

The IIA's Financial Services Risk Framework utilizes the definition of conduct risk as presented in the article "Conduct Risk" published by the Chartered Institute of Internal Auditors in the United Kingdom. The definition of *conduct* used in this publication is "the term used by financial services organizations to describe risks associated with the way organizations, their staff, agents, and advisors relate to customers and the wider financial markets."[2]

Resource

For more information on The IIA's Financial Services Risk Framework, see IIA Practice Guide, "Foundations of Internal Auditing in Financial Services Firms."

Financial services regulators and organizations use numerous definitions for conduct risk, though they generally concur that an organization's culture drives its employees' conduct.

The New York Federal Reserve Bank recognizes "misconduct risk" is gaining prominence in financial institutions and that if controlled, could serve to make institutions more resilient to a broader range of risks. It describes employee misconduct risk as "the potential for behaviors or business practices

2. Chartered Institute of Internal Auditors, *Conduct risk*, October 2, 2019, https://www.iia.org.uk/resources/sector-specific-standards-guidance/financial-services/conduct-risk/?downloadPdf=true.

that are illegal, unethical, or contrary to a firm's stated beliefs, values, policies and procedures."[3] This interpretation applies to actions adversely affecting individuals such as customers or stakeholders, or causing harm to individuals within the organization.

Misconduct can occur at any and every level of an organization. It can be rare, sporadic, or pervasive. It can occur at any time in nearly any circumstance. Misconduct occurs for various reasons, and sometimes the link between misconduct and culture is clear. An organization could have a rebellious or disruptive faction within its culture, in which misconduct may not manifest in its business practices. Another organization may appear to have a solid culture, but may have instances, or pockets, in which conduct is less than ideal. The unfortunate possibilities and configurations are endless. Vigilance is key, and that is where internal audit can help.

Loyalty Penalties in UK Insurance Markets

"[The Financial Conduct Authority] found that [home and auto insurance] markets are not working well for all consumers. While many people shop around, many loyal customers are not getting a good deal. We believe this affects around 6 million consumers, who would have saved £1.2 billion if they had paid the average for their risk."

Source: "Citizens Advice supercomplaint to the CMA – update," *Financial Conduct Authority*, Jan. 9, 2020, https://www.fca.org.uk/news/news-stories/citizens-advice-supercomplaint-cma-update.

Just as culture and conduct are not synonymous, there is a difference between misconduct and reputational damage. Misconduct can result in reputational damage if an employee's behavior violates rules or regulations or harms a customer or a colleague, and that information becomes public knowledge, perhaps via news outlets or social media. Not all conduct risks by default result in reputational damage, but they can still jeopardize an organization's achievement of its objectives.

Assessing and evaluating culture, reputational risks, or incidents that have caused reputational damage are all elements of assessing an organization's conduct risk. Internal auditors should not rely solely on past culture-related risk events to provide a thorough assessment of conduct risk, however. Conduct risk covers much more territory, including scenarios for misconduct, incentives, and other risks that will be reviewed in the Risk Assessment section of this guide.

Regulatory Environment of Conduct

While the phrase "conduct risk" in regulations has become more prevalent, regulators have always considered conduct risk in their examination programs, though the word "conduct" may not have been used. Global regulators appear to be leading the way in terms of "conduct risk" guidance, requirements, and expectations.

3. Stephanie Chaly, James Hennessy, Lev Menand, Kevin Stiroh, and Joseph Tracy, *Misconduct Risk, Culture, and Supervision* (New York: Federal Reserve Bank of New York, 2017), 3, https://www.newyorkfed.org/medialibrary/media/governance-and-culture-reform/2017-whitepaper.pdf.

In the interest of the financial services industry's safety, soundness, and resilience, it is prudent that regulatory bodies are and have been exploring ways to identify and, possibly, prevent misconduct. The financial services industry affects nearly every person in the world in some way, so it is appropriate that conduct risks and related controls would be a key focus for firms engaged in the business of selling products and managing money.

The challenge for regulatory bodies is defining conduct risk. Currently, conduct risk is represented by Pillar 2 capital add-ons per the Basel III standards, a component of operational risk, which is a universal category for hard and soft risks that are difficult to measure in financial services firms.[4]

Conduct can be defined narrowly as compliance with regulatory requirements or broadly, as in touching every phase of the customer and employee lifecycle. Considering the logistics of managing any multi-jurisdictional organization across countries, cultures, and time zones, the challenge is clear.

Questionable Sales Practices

In addition to creating millions of fake accounts in an effort to meet unreasonable sales targets, Wells Fargo also admitted it charged as many as 570,000 consumers for auto insurance that they did not need.

Additionally, some 20,000 of those borrowers may have had their cars repossessed as a result. Wells Fargo agreed to pay $80 million in remediation.

Source: Emily Glazer, "Wells Fargo to Refund $80 Million to Auto-Loan Customers for Improper Insurance Practices," *Wall Street Journal*, July 28, 2017, https://www.wsj.com/articles/wells-fargo-to-refund-80-million-to-auto-loan-customers-for-improper-insurance-practices-1501252927.

Regulatory bodies across the world have a variety of definitions for culture and conduct risk, some of which are shown as excerpts from larger works in Figure 2. Full texts from which each excerpt is taken are offered in Appendix C. References and Additional Reading.

Figure 2: Examples of Regulatory Definitions of Culture and Conduct

Australian Securities and Investment Commission
Outline of ASIC's Approach to Corporate Culture
Culture is a set of shared values or assumptions. It can be described as the mindset of an organization. This is not a new concept. It was actually captured in the Criminal Code over 20 years ago, where it is defined as including an organization's attitude, policy, rule, course of conduct, and practice. Risk culture, to be more particular, describes the norms of behavior that determine how an organization identifies, understands, discusses, and acts on risks.
Hong Kong Monetary Authority
Bank Culture Reform
In this context, "culture" can be regarded generally as a set of professional and ethical values which defines attitude and behaviors as pursued and observed by a bank's shareholders, board members, and staff.

4. Basel Committee on Banking Supervision, *Overview of Pillar 2 supervisory review practices and approaches*, Basel, Switzerland: Bank for International Settlements, June 2019. https://www.bis.org/bcbs/publ/d465.pdf.

Figure 2: Examples of Regulatory Definitions of Culture and Conduct (continued)

Monetary Authority of Singapore

"Culture and Conduct – A Regulatory Perspective"

Definitions and descriptions abound in the literature but in the main, we see it as the shared values, attitudes, and norms that guide behavior in an organization. Culture reflects the underlying mindset of an organization and affects how an organization and its staff act and make decisions, oftentimes without thinking consciously about it.

United Kingdom

Banking Standards Board

There are numerous descriptions and definitions of culture, with one of the most frequently cited being that it is "the way things get done when no one is looking." While this nicely conveys the sense of deep-rootedness and innateness that we instinctively associate with culture, it does not quite capture its entirety. More accurate, albeit considerably less catchy, would perhaps be to say that we can learn a great deal about a group's culture from observing what gets done when no one in authority is looking; although it would also be correct to say that we can also learn about the culture from what gets done when lots of people in the group happen to be looking.

More formally, culture can be said to refer to the collective assumptions, values, beliefs, and expectations that shape how people behave in a group.

United Kingdom

Financial Conduct Authority

To make sense of "culture" from an FCA perspective, we start by defining it as the habitual behaviors and mindsets that characterize an organization.

United States

Office of the Comptroller of the Currency: Comptroller's Handbook, Corporate and Risk Governance

Corporate culture refers to the norms and values that drive behaviors within an organization. An appropriate corporate culture for a bank is one that does not condone or encourage imprudent risk taking, unethical behavior, or the circumvention of laws, regulations, or safe and sound policies and procedures in pursuit of profits or business objectives. An appropriate corporate culture holds employees accountable. This starts with the board, which is responsible for setting the tone at the top and overseeing management's role in fostering and maintaining a sound corporate culture and risk culture. Shared values, expectations, and objectives established by the board and senior management promote a sound corporate culture.

United States

Office of the Comptroller of the Currency: Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches

While there is no regulatory definition of risk culture, for purposes of these Guidelines, risk culture can be considered the shared values, attitudes, competencies, and behaviors present throughout the bank that shape and influence governance practices and risk decisions.

In addition, examples of regulatory guidance regarding conduct risks appears in Figure 3 below:

Figure 3: Conduct Risk Regulatory Programs

Australia
Australian Prudential Regulation Authority: Banking Executive Accountability Regime
https://www.apra.gov.au/banking-executive-accountability-regime
Australian Securities & Investments Commission: Close and Continuous Monitoring Program as part of the ASIC Corporate Plan 2019–23
https://download.asic.gov.au/media/5248811/corporate-plan-2019-23-published-28-august-2019.pdf
European Union
European Central Bank: European Banking Authority is mandated by Article 74 of Directive 2013/36/EU
https://eba.europa.eu/sites/default/documents/files/documents/10180/1972987/eb859955-614a-4afb-bdcd-aaa664994889/Final%20Guidelines%20on%20Internal%20Governance%20(EBA-GL-2017-11).pdf
European Insurance and Occupational Pensions Authority: Framework for Assessing Conduct Risk Through the Product Lifecycle
https://www.eiopa.europa.eu/sites/default/files/publications/reports/2018.6644_en_03_mod-gp.pdf
Hong Kong
Hong Kong Monetary Authority: Bank Culture Reform/Manager-in-Charge regime
https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2018/20181219e1.pdf
Netherlands
DeNederlandscheBank and Dutch Authority for the Financial Markets: Supervision of Behaviour and Culture
https://www.dnb.nl/en/binaries/Book%20Supervision%20of%20Behaviour%20and%20Culture_tcm47-380398.pdf
Norway
Norwegian Ministry of Finance/ The Financial Markets Department: Revised Strategy for Combating Work-related Crime
https://www.regjeringen.no/contentassets/7f4788717a724ef79921004f211350b5/a-0049-e_revised-strategy-for-combating-work-related-crime.pdf
United Kingdom
Bank of England/ Prudential Regulation Authority: Senior Managers Regime
https://www.bankofengland.co.uk/prudential-regulation/authorisations/senior-managers-regime-approvals
United States
Federal Reserve: SR 12-17 / CA 12-14: Consolidated Supervision Framework for Large Financial Institutions
https://www.federalreserve.gov/supervisionreg/srletters/sr1217.htm
New York State Department of Financial Services: Regulation 60: Market Conduct Profile
https://www.dfs.ny.gov/docs/insurance/reg60/mc_profile_2017.pdf

Companies in many industries follow regulations that govern aspects of conduct. For example, United States laws include the Foreign Corrupt Practices Act, the Equal Employment Opportunity Act, the Americans with Disabilities Act, among others. However, for financial services firms, the United Kingdom's Prudential Regulation Authority (PRA) has a comprehensive and tested culture and conduct risk management program referred to as the Senior Managers Regime. This program requires designated senior managers to directly oversee the adoption of a firm's risk culture and ensure that countermeasures are in place to prevent the firm from being used to further financial crime. All members of a firm's governing body must undergo suitable training and professional development, which is monitored by appropriate personnel within the organization.

Figure 4 illustrates some sample scenarios in which the U.K.'s PRA may consider taking disciplinary action against non-executive director (NED) functions, which are in scope of the senior managers regime (SMR).

Figure 4: Sample Disciplinary Scenarios

NEDs in Scope of the SMR Potentially Accountable
A skilled person's review reveals that a firm's risk committee has not advised the board on the firm's **risk appetite** nor assisted it in overseeing the implementation of the firm's risk strategy by executive management in contravention of risk control 3.1(2). In this situation, the PRA might consider whether there could be grounds to sanction the chair of the risk committee.
During a board effectiveness review, the PRA discovers that the remuneration committee has failed to prepare any decisions regarding remuneration for consideration and decision by the board. In this situation, the PRA may consider whether there could be grounds to sanction the chair of the remuneration committee.
A firm's chair and NEDs in scope of the SMR have serious concerns about an overly dominant CEO. These concerns are not addressed, recorded, or discussed by the board or with PRA or FCA supervisors.
Executive Senior Management Functions Potentially Accountable
A firm breaches its capital requirements as a result of a major loss in a key business unit that has repeatedly breached its risk limits. The risk limits were discussed and set by the risk committee and the board. In this situation, the PRA might primarily consider whether there are grounds to sanction the appropriate executive senior managers, including heads of the key business areas and the chief risk officer. If, however, the breaches are reported to the board and/or the risk committee, the PRA may also enquire whether the board/risk committee discussed them and made any recommendations.
In an attempt to obtain board approval for a new, riskier lending strategy, a firm's senior executives submit incomplete and misleading management information to the board that significantly downplays the risks of such a strategy. The CEO also suppresses any negative or questioning advice on this issue, and consequently the board approves the strategy which, six months later, causes the firm to breach a number in the Risk Control section of the PRA rulebook.
A firm's management fails to monitor the provision of services by a third party under an outsourcing agreement resulting in an operational risk crystalizing in (a) breach of outsourcing 2.1 in the PRA rulebook.

Source: Source: Bank of England, Prudential Regulation Authority, Strengthening individual accountability in banking, Supervisory Statement | SS28/15, July 2018. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2018/ss2815update.pdf?la=en&hash=39EC46AE5FD217724BB307C420B80A4E09F42A24.

The U.K.'s Financial Conduct Authority has also set out Individual Conduct Rules (aka COCON 2.1) that define the regulators' expectations of financial services firms as follows:

1. You must act with integrity.
2. You must act with due skill, care, and diligence.
3. You must be open and cooperative with the FCA, the PRA, and other regulators.
4. You must pay due regard to the interests of customers and treat them fairly.
5. You must observe proper standards of market conduct.[5]

The FCA accompanies these rules with five questions when examining banking institutions with wholesale banking business lines:

1. What proactive steps do you take as a firm to identify the conduct risks inherent within your business?
2. How do you encourage the individuals who work in front, middle, back office, control, and support functions to feel and be responsible for managing the conduct of their business?
3. What support (broadly defined) does the firm put in place to enable those who work for it to improve the conduct of their business or function?
4. How does the board and executive committee (ExCo) (or appropriate senior management) gain oversight of the conduct of business within their organization and, equally important, how does the board or ExCo consider the conduct implications of the strategic decisions that they make?
5. Has the firm assessed whether there are any other activities it undertakes that could undermine strategies in place to improve conduct?[6]

Financial services firms should expect regulatory bodies to be asking these questions and including rules of this type in their examinations if they are not already doing so.

Conduct Risk Management Framework

To manage conduct risk in an organization, there must be agreement on both the definitions of culture and conduct risk(s) and the components involved in managing these risks. The organization must be committed to defining what conduct is appropriate and clear about the consequences of misconduct.

Effective conduct risk management frameworks typically consist of at least three components as shown in Figure 5.

5. *FCA Handbook*, COCON, COCON 2 (London: Financial Conduct Authority, last updated March 7, 2016). https://www.handbook.fca.org.uk/handbook/COCON/2/?view=chapter.
6. *Progress and Challenges: 5 Conduct Questions* (London: Financial Conduct Authority, 2019). https://www.fca.org.uk/publication/market-studies/5-conduct-questions-industry-feedback-2018-19.pdf.

Figure 5: Conduct Risk Management Framework Components

Source: Stacey Schabel, "Maximizing Organizational Value: Auditing Conduct & Culture," presentation delivered at The IIA's 2019 Financial Services Exchange, Washington, D.C., September 16, 2019.

Expectations Defined

Clear definitions of culture and conduct risks are required for an organization to ensure all employees are aware of and can execute business processes in line with the organization's expectations of them. As previously mentioned, the New York Federal Reserve Bank defines conduct risk as "the potential for behaviors or business practices that are illegal, unethical, or contrary to a firm's stated beliefs, values, policies and procedures."[7]

This definition may be a starting point for an organization to determine what conduct means to them in the context of their business. Other documents containing explanations of the organization's expectations of employee conduct may include:

- Values statements.
- Codes of conduct.
- Ethics policy and training materials.
- Risk appetite statements or frameworks.
- Compensation practices.
- Segregation of duties requirements.

7. Stephanie Chaly, James Hennessy, Lev Menand, Kevin Stiroh, and Joseph Tracy, *Misconduct Risk, Culture, and Supervision* (New York: Federal Reserve Bank of New York, December 2017). https://www.newyorkfed.org/medialibrary/media/governance-and-culture-reform/2017-whitepaper.pdf.

Measurement and Reporting

There are many key performance indicators in the financial services industry that may be useful in determining how management is — or is not — monitoring the level of conduct risk. KPIs may include such items as:

- Electronic training completion rates.
- Complaints.
- Management overrides.
- Fraud occurrences and associated losses.
- Negative compensation changes resulting from conduct-related violations.
- Employee survey results.
- Client satisfaction survey results.
- Control environment survey results.

Reviews of these KPIs and others that may be organizationally relevant over time can provide insight to how conduct risk exposure is changing over time and what types of activities might affect exposure levels.

Consequences of Misconduct

Perhaps the most important question to ask is whether and how management is held accountable for both their personal actions and for the actions of people under their span of control. If conduct violations/issues are not linked to identifiable consequences, there is less incentive for employees to align activities to the organization's conduct rules. Unclear linkage of violations to consequences can also affect an organization's culture, as employees may see that not following the rules is acceptable.

Role of Internal Audit

An organization's requirements and expectations of conduct are normally stated through a series of formalized documents and related training, including codes of conduct, values statements, ethics policies, investigation committees and related mandates, and other guidance. Many financial services organizations review, update, and publish their codes of conduct on a regular basis.

The internal audit activity should determine whether the organization has a conduct risk management framework that states its values, expectations, and the mechanisms that measure how well employees are performing against those criteria. Internal auditors should also conduct inquiries across the organization to ascertain the level of employee understanding of conduct requirements and expectations. Internal auditors should discern whether the employees are aware of the potential consequences of noncompliance.

Do employees ask themselves questions such as those shown below when making business decisions and, if so, does the conduct risk management framework help them answer those questions effectively?

What if I were a customer?

- Treating customers fairly, openly, and honestly.
- Providing and promoting products and services that meet customer needs, are clearly explained, and deliver real value.
- Putting the customer at the heart of what we do.

What if I owned the business?

- Seeing through the shareholders' eyes.
- Driving business that delivers long-term, sustainable value.
- Taking ownership of new opportunities and the risks we take.
- Asking yourself what you would do if this were your money at risk.

How do I work with my colleagues?

- Working collaboratively with colleagues, both in our own teams and around the world.

What do I tell my family and friends?

- Our obligation to the community.
- We should be proud to tell our friends and family what we do.

Source: Paraphrased from Prudential, PLC Code of Business Conduct, December 2019, https://www.prudentialplc.com/investors/governance-and-policies/code-of-business-conduct.

If a conduct risk management framework exists, and employees are generally aware of it, then internal auditors should assess the design and effectiveness of controls in place to support alignment of business activities with the framework's requirements. This includes policies, procedures, management information, governance, breach management, second-line oversight, and other activities supporting alignment with requirements.

If the organization's conduct risk management activities are implemented but communicated inaccurately, it may foster an environment of fear. For example, managers suspect a certain employee reported an incident to the organization's ethics hotline. While the incident is kept confidential and the whistleblower is not identified, management assumes (for whatever reason: personal dislike, access to information, previous discussions regarding the practice reported, etc.) this employee is the culprit. As a result, management moves that employee to a position of less responsibility in which they no longer have access to people, information, or other knowledge relevant to the complaint.

Whether the employee reported the incident or not, the message to employees is clear: whistleblowers or those who report issues to ethics hotlines will be subject to retaliation, retribution, or punishment of some sort. If management suspects but does not know it was a certain individual, they may still inflict negative consequences on that person. Internal auditors should be aware of whether the conduct risk management activities have an adverse effect on the organization's culture.

Planning and Performing the Engagement

This guide will consider the approach of selecting a set of key processes and controls related to an overall conduct risk management framework, developing an engagement plan, and performing targeted testing on the selected areas. Testing may be supplemented with employee interviews in which auditors ask questions focused on assessing how conduct risks are addressed. Refer to Standard 2300 – Performing the Engagement for specific details.

Gather Information

Internal auditors must identify the expectations of management related to employee conduct. The Conduct Risk Management Framework section of this guide offers an overview of the type of information that should be gathered and considered when constructing an engagement program to audit conduct risk.

Sources of information regarding the organization's expectations of employee conduct may be found in these documents and compared to the results of testing employees' actual conduct when executing their duties:

- Values statements.
- Codes of conduct.
- Ethics policy and training materials.
- Risk appetite statements or frameworks.
- Results of employee culture surveys (matching reported scores to individual answers to questions and any free text comments provided by employees).

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 and conduct 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."

Risk Assessment

Conduct risk can be defined many ways, but there are common actions that generally come under the umbrella of conduct risk including:

- Mistreatment of customers.
- Misleading customers.
- Violation of rules and regulations.
- Fraud.
- Wrongdoing against employees.
- Conducting business in a way that does not align with the organization's stated risk appetite.
- Implementing strategies or actions that distort the natural market environment.

In a general sense, conduct risk is generated by any action that may cause harm to customers, employees, or other stakeholders.

Conduct risk assessments, if done well, should see beyond what has happened in the past to consider what may happen in the future. Consideration of the inherent risks related to products and services offered by the organization is essential (e.g., retail banking risks are different than commercial risks which are different than universal life insurance risks). Further, the consideration of scenarios where misconduct could occur and the controls in place to mitigate those risks may be an effective method to identify the interrelationships between risks and controls related to conduct.

In more sophisticated programs, financial services organizations are assessing conduct risk exposure not only looking at each individual incident, but at the correlations and trends of misconduct over time. If one person is getting expense reports rejected, not following the required absence policy, not taking code of conduct training, etc., is there a process in place to more closely look at these actions? Are incidents involving recorded phone calls, trade monitoring, control overrides, and so on, flowing through the performance review and incentive programs? Are these issues isolated to a person? If multiple people are involved in wrongdoing, do they have a common manager, department, or business line? Also, who knew what when? Did they report it timely or at all?

If these risk factors and corresponding correlations and trends are present in an organization, internal auditors have a responsibility to identify them and report them to senior management and the board as appropriate and in accordance with Standard 2060 – Reporting to Senior Management and the Board. In addition, under The IIA's Code of Ethics principle of Integrity and the Rules of Conduct, 1.2 indicates that "Internal auditors shall observe the law and make disclosures expected by the law and the profession." Audit findings and subsequent investigations may require bringing matters to the attention of authorities.

The ultimate scope and objectives of an audit should inform how the preliminary risk assessment is focused and performed.

Planning the Engagement

To satisfy Standard 2201 – Planning Considerations, Standard 2210 – Engagement Objectives, and Standard 2220 – Engagement Scope, the CAE may use accessible information from past audits and key processes and controls related to conduct to develop an audit engagement plan. This engagement plan could be constructed in a variety of ways. This guide will consider the approach of selecting a set of key processes and controls related to an overall conduct risk management framework, developing an engagement plan, 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 focused on assessing how conduct risks are addressed.

The engagement objectives should be tied to the organization's definition of conduct risk. As mentioned previously, this could be narrow, or it could be broad. Once the definition of conduct risks is known, testing should focus on assessing the processes and controls that support alignment of organizational activities to this definition.

In scoping an audit engagement focused on the conduct risk management framework (Standard 2220 – Engagement Scope), and the processes and controls in place to comply, a helpful first step is mapping where audit (or other) assurance coverage has been obtained in relevant areas.

Resources

For examples of techniques to integrate culture and conduct risks into audits conducted by the internal audit activity, see IIA Practice Guide, "Auditing Culture."

For more information on building an assurance map, see IIA Practice Guide "Coordination and Reliance: Developing an Assurance Map."

Resource Allocation

Certain skills sets are needed for those assigned to conduct-related risk audit engagements. In conformance with Standard 2230 – Engagement Resource Allocation, the **chief audit executive** 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 conduct-related risks.

A key factor in determining resource allocation is integrating new auditors into audits where conduct 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 brief new auditors on these issues and include them early into the engagement planning. For instance, have them sit in on interviews conducted by more experienced audit team members, especially when sensitive conduct-related 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, making an agenda with targeted questions important. 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 conduct. 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.

If work regarding conduct 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.

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).

Performing the Engagement

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 which, if used in the audit, must be documented, as per Standard 2330 – Documenting Information:

- 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).
- Mapping of where previous assurance coverage has been obtained.

Given the sensitivity of some of the views expressed during an audit of conduct-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 those represented). This relates to the Code of Ethics principle of Confidentiality.

If the CAE chooses to approach the engagement by selecting a set of key processes and controls related to compliance with the conduct risk management framework and developing an engagement plan that tests those processes across the organization, it may be helpful to construct the engagement to test the various components of the Conduct Risk Management Framework in use within the organization. For the purpose of this discussion, the components of the framework shown in Figure 5 will be followed:

- Expectations defined.
- Measurement and reporting.
- Consequences of misconduct.

Expectations Defined

It may be preferable to determine first the existence of documents defining the organization's expectations of employees, but internal auditors should also examine the effectiveness of those documents among employees. Techniques to obtain this information could include:

- Examining employees' perception of the "tone at the top" regarding conduct through interviews or surveys. Analyzing results of employee culture surveys including matching reported scores to individual answers to questions and any free text comments provided by employees can be a useful way to identify disconnects between what executive management thinks they are communicating versus what employees are actually hearing and understanding.
- Examining how value statements are constructed and communicated. Is the value statement simple and clear? Do employees physically see the value statement posted around the office? Is the value statement on the website? Do executives reinforce the value statement in their written and verbal communications?
  - An example of a simple and clear value statement comes from Uber's "Cultural Norms" document: WE DO THE RIGHT THING. PERIOD.
- Confirming that the organization's code of conduct is updated regularly. If so, are employees required to demonstrate their acceptance of the code of conduct following new updates? Does the code of conduct provide scenarios to educate employees on

Risk Appetite and Tolerance for Conduct Risk

What is the organization's tolerance for misconduct?

If an employee is a big revenue generator and has all the good clients, what is the propensity for the organization to turn a blind eye when they do something wrong?

To what extent can there be modifications or exceptions to the process of monitoring and reporting on issues?

recognizing violations of the code? Are consequences of violations listed in the code of conduct?

- Examining the organization's ethics policy and its associated training materials. As mentioned, are employees required to complete training on the organization's ethics programs? If so, how is their completion documented? If a passing score on a final test of employees' comprehension of the program is not required, how can the organization demonstrate employees' levels of comprehension?
- Assessing the effectiveness of the organization's risk appetite statement and framework in managing conduct risk. Financial services organizations usually have risk appetite statements or frameworks to govern a variety of business operations. However, internal auditors may want to examine whether or not those risk appetite statements or frameworks extend to nonfinancial risks such as conduct risk. If not, why not?

Measurement and Reporting

If an organization has all of the required documentation relevant to their conduct risk management framework, the next step is for internal auditors to understand how the organization is monitoring employees' actual behavior. Some audit considerations to determine compliance could include:

- Confirming measurable KPIs (as discussed in the Conduct Risk Management Framework section of this document) are tracked and escalation protocols are followed when metrics deviate from expected parameters.
- Examining a sample of incidents that should have resulted in disciplinary action or compensation impact for the effectiveness of related processes.
- Examining the communication activities of management regarding reportable incidents.
- Auditing the organization's whistleblowing and complaint handling procedures.
- Confirming the organization is following regulatory and internal conduct-related requirements that impact compensation.
- Confirming that individual processes where conflicts of interest or segregation of duties violations may occur are adequately structured and monitored to avoid these risks.

Audit Consideration

Any engagement plan considering conduct risks for a financial services firm should include an examination of compensation policies and practices and their relationship to the defined expectations of management and the board regarding employee conduct. Having articulated the norms individuals should follow, internal auditors should test incidents from occurrence to reporting to compensation/incentive impact to confirm the relevant policies and procedures are enforced.

An example of a Conduct Risk and Control Testing Matrix including these factors is shown in Figure 6.

Figure 6: Sample Conduct Risk and Control Testing Matrix

Conduct Risks
Improper segregation of duties for consumer lending.
Controls
▪ Written consumer lending policies and procedures have segregation of duties built into them. ▪ Loan processors cannot approve their own loans. ▪ Out-of-policy loans must be approved according to a delegation of authorities matrix approved by the board. ▪ Loan file review function must validate the loan file is complete and accurate before the loan is approved.
Potential Worksteps
▪ Review consumer lending policies and procedures to verify segregation of duties requirements are included, clear, and in compliance with regulations and the organization's code of conduct. ▪ Note deviations from regulatory requirements and/or the code of conduct provisions. ▪ Walk through key processes to assess how consistent actual practices are with policies/procedures. ▪ Obtain user access documentation to verify loan processors cannot/do not approve their own loans. ▪ If a lending processor or manager is found to have access to both processing and approval functions within the lending system, trace a statistically significant sample of loans to verify they have not abused their access. ▪ If abuse of access is identified or strongly suspected, follow formal escalation processes. ▪ Review past instances of abuse to ensure consequences were delivered appropriate to the magnitude of the violation. ▪ If no abuse is identified or suspected, recommend access be changed to ensure proper segregation of duties. ▪ Select a sample of out-of-policy loans and trace their approval process to verify they were approved at the right level of the organization according to set criteria. ▪ If sampling indicates out-of-policy loans are not escalated properly, investigate why (e.g., inappropriate access, lack of software controls, failure to review exception reports). ▪ Review board and executive committee/credit committee meeting minutes to identify discussions regarding out-of-policy loans and decisions reached. ▪ Walk through the exception review process to identify control weaknesses. ▪ Review past inappropriately approved out-of-policy loans to ensure consequences were delivered appropriate to the magnitude of the violation. ▪ Select a sample of loan files and re-perform the loan file reviewer's work to verify files that are approved are complete. ▪ Review overall testing results, control documentation, and walkthroughs to identify if any patterns of misconduct may be present. If so, expand audit scope and sampling as required.

Source: The Institute of Internal Auditors.

Consequences of Misconduct

In terms of enforcement, internal auditors should examine whether "punishments match the crime." Management should strike a balance between being too lenient and too harsh. Examples of misconduct that must have zero tolerance because they are criminal acts and/or specifically prohibited by regulation include, for example, lying to customers or clients.

Other ways to seek information to examine could include asking pertinent questions, such as:

- Are select employees, perhaps members of management, allowed to avoid taking required training on topics such as ethics, conduct, harassment, etc.?
- Are employees allowed to work directly with customers without required training?
- Do employees complete their expense reports on time and accurately without rejection?
- What happens if employees are charging inappropriate expenses to their reports?
- Does the organization require notification of employees' outside business interests and investments that could lead to conflicts of interest?
- Do employees selectively allow customers to breach their credit limits?
- Do employees involved in asset management and/or trading use their mobile phones to conduct sales calls that should be performed on a recorded line?
- Are instances of misconduct collected and correlated or trended over time to identify patterns either with individuals or with larger groups?
- Are monitoring and surveillance systems seeing everything they should be seeing and is that information being adequately analyzed?
- What are the consequences for noncompliance with regulations?
- Is "treating customers fairly" considered in product development activities?

If any of these situations are identified during an audit, internal auditors should examine what consequences, if any, resulted from the situation. If there are limited, inconsistent, or no consequences for violating the organization's values, then the values could be determined to be ineffective.

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."

Communicating Results of a Conduct Risk-focused Audit

Internal auditors may wish to conduct a session with the board to discuss conduct-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.

Reporting on conduct-related issues may be sensitive, but the CAE has a responsibility to clearly, concisely, and openly communicate to senior management and the board. Reports that focus on results of testing and are fact-based but accurately convey the audit team's conclusions are the most effective.

Appendix A. Relevant 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
Integrity
Confidentiality
Standards
Standard 2050 – Coordination and Reliance
Standard 2060 – Reporting to Senior Management and the Board
Standard 2200 – Engagement Planning
Standard 2201 – Planning Considerations
Standard 2210 – Engagement Objectives
Standard 2220 – Engagement Scope
Standard 2230 – Engagement Resource Allocation
Standard 2240 – Engagement Work Program
Standard 2300 – Performing the Engagement
Standard 2330 – Documenting Information
Standard 2400 – Communicating Results
Standard 2410 – Criteria for Communicating
Related IIA Resources
Practice Guide "Auditing Culture," 2019.
Practice Guide "Auditing Third-party Risk Management," 2018.
Practice Guide "Coordination and Reliance: Developing an Assurance Map," 2018.
Practice Guide "Engagement Planning: Assessing Fraud Risks," 2017.
Practice Guide "Engagement Planning: Establishing Objectives and Scope," 2017.
Practice Guide "Foundations of Internal Auditing in Financial Services Firms," 2019.

Appendix B. Glossary

Terms identified with an asterisk (*) are taken from The IIA's *International Professional Practices Framework* "Glossary," 2017 edition.

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.

competency – internal auditors apply the knowledge, skills, and experience needed in the performance of internal audit services.[8]

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.[8]

internal audit activity* – a department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.

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.

8. *International Professional Practices Framework* (Altamonte Springs, FL: The IIA, 2017), 34. https://bookstore.theiia.org/international-professional-practices-framework-ippf-2017-edition.

Appendix C. References and Additional Reading

References

Basel Committee on Banking Supervision, *Overview of Pillar 2 supervisory review practices and approaches*, Basel, Switzerland: Bank for International Settlements, July 2019. https://www.bis.org/bcbs/publ/d465.pdf.

Chaly, Stephanie, James Hennessy, Lev Menand, Kevin Stiroh, and Joseph Tracy. *Misconduct Risk, Culture, and Supervision.* New York: Federal Reserve Bank of New York, 2017. https://www.newyorkfed.org/medialibrary/media/governance-and-culture-reform/2017-whitepaper.pdf.

Chartered Institute of Internal Auditors. *Conduct risk.* October 2, 2019. https://www.iia.org.uk/resources/sector-specific-standards-guidance/financial-services/conduct-risk/?downloadPdf=true.

Clayton, Sarah. "6 Signs Your Corporate Culture Is a Liability." *Harvard Business Review*, December 5, 2019. https://hbr.org/2019/12/6-signs-your-corporate-culture-is-a-liability.

Financial Conduct Authority. *FCA Handbook, COCON, COCON 2.* Last updated March 7, 2016. https://www.handbook.fca.org.uk/handbook/COCON/2/?view=chapter.

Financial Conduct Authority. *Progress and Challenges: 5 Conduct Questions.* May 2019. https://www.fca.org.uk/publication/market-studies/5-conduct-questions-industry-feedback-2018-19.pdf.

The IIA. *International Professional Practices Framework*. Altamonte Springs: Internal Audit Foundation, 2017. https://bookstore.theiia.org/international-professional-practices-framework-ippf-2017-edition.

Additional Reading

Australian Securities and Exchange Commission. Market Supervision Update Issue 57. "Conduct Risk." Accessed April 17, 2020. https://asic.gov.au/about-asic/corporate-publications/newsletters/asic-market-supervision-update/asic-market-supervision-update-previous-issues/market-supervison-update-issue-57.

Chartered Institute of Internal Auditors. "Financial Services Code: Effective Internal Audit in the Financial Services Sector, Second Edition." September 2017. https://www.iia.org.uk/resources/sector-specific-standards-guidance/financial-services/financial-services-code/.

Chartered Institute of Internal Auditors. "Conduct risk." April 14, 2020. https://www.iia.org.uk/resources/sector-specific-standards-guidance/financial-services/conduct-risk/?downloadPdf=true.

Clayton, Jay. SEC. "Observations on Conduct at Financial Institutions and the SEC," speech delivered in New York, June 18, 2018. https://www.sec.gov/news/speech/speech-clayton-061818.

Department of the Treasury, Office of the Comptroller of the Currency (US). "OCC Guidelines stablishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of 12 CFR Parts 30 and 170." September 11, 2014. https://www.govinfo.gov/content/pkg/FR-2014-09-11/pdf/2014-21224.pdf.

European Banking Authority. "Guidelines for Common Procedures and Methodologies for the Supervisory Review and Evaluation Process (SREP) and Supervisory Stress Testing." Accessed April 17, 2020. https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-for-common-procedures-and-methodologies-for-the-supervisory-review-and-evaluation-process-srep-and-supervisory-stress-testing.

European Systemic Risk Board. "Report on Misconduct Risk in the Banking Sector." June 2015. https://www.esrb.europa.eu/pub/pdf/other/150625_report_misconduct_risk.en.pdf.

Financial Conduct Authority. "Progress and Challenges: 5 Conduct Questions." May 2019. https://www.fca.org.uk/publication/market-studies/5-conduct-questions-industry-feedback-2018-19.pdf.

Financial Conduct Authority (UK). "Transforming Culture in Financial Services" Discussion Paper. March 12, 2018. https://www.fca.org.uk/publication/discussion/dp18-02.pdf.

Financial Stability Board. "Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture." April 7, 2014. https://www.fsb.org/2014/04/guidance-on-supervisory-interaction-with-financial-institutions-on-risk-culture-a-framework-for-assessing-risk-culture-2/.

Financial Stability Board. "Recommendations for Consistent National Reporting of Data on the Use of Compensation Tools to Address Misconduct Risk." May 7, 2018. https://www.fsb.org/2018/05/recommendations-for-consistent-national-reporting-of-data-on-the-use-of-compensation-tools-to-address-misconduct-risk/.

FINRA. "Targeted Examination Letter on Establishing, Communicating, and Implementing Cultural Values." February 2016. https://www.finra.org/rules-guidance/guidance/targeted-exam-letter/establishing-communicating-and-implementing-cultural-values.

Glazer, Emily. "Wells Fargo to Refund $80 Million to Auto-Loan Customers for Improper Insurance Practices," Wall Street Journal, July 28, 2017. https://www.wsj.com/articles/wells-fargo-to-refund-80-million-to-auto-loan-customers-for-improper-insurance-practices-1501252927.

Monetary Authority of Singapore. "Framework for Impact and Risk Assessment of Financial Institutions." September 2015. https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/MAS%20Framework%20for%20Impact%20and%20Risk%20Assessment%20of%20Financial%20Institutions.pdf.

Ngiap, Lee Boon. Monetary Authority of Singapore. "Culture and Conduct – A Regulatory Perspective," speech presented to the 2017 Annual Luncheon of the Life Insurance Association of Singapore, March 6, 2017. https://www.mas.gov.sg/news/speeches/2017/culture-and-conduct.

Office of the Comptroller of the Currency (US). Comptroller's Handbook: Corporate and Risk Governance, p 15. Version 2.0, July 2019. https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/corporate-risk-governance/index-corporate-and-risk-governance.html.

Price, John. Australian Securities and Investments Commission. "Outline of ASIC's Approach to Corporate Culture," speech presented at the AICD Directors' Forum: Regulators' Insights on Risk Culture, Sydney, Australia, July 19, 2017. https://download.asic.gov.au/media/4393665/john-price-speech-aicd-regulator-insights-on-risk-culture-published-20-july-2017.pdf.

Risk.net. "Asia-Pacific Banks Grapple with Conduct Risk Rules." May 13, 2018. https://www.risk.net/risk-management/5595381/asia-pacific-banks-grapple-with-conduct-risk-rules.

Yuen, Arthur. Hong Kong Monetary Authority. "Bank Culture Reform." March 2, 2017, letter to the chief executive of all authorized institutions. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2017/20170302e2.pdf.

If a hyperlink is inoperable, copy and paste the link into a browser window.

Acknowledgements

Guidance Development Team

Jose Esposito, CIA, CRMA, Peru (Chairman)
Stacey Schabel, CIA, United States (Project Lead)
Mark Carawan, CIA, QIAL, 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

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

IIA Global Standards and Guidance

Jeanette York, CCSA, FS Director (Project Lead)
Jim Pelletier, CIA, CGAP, Vice President
Anne Mercer, CIA, CFSA, Director
P. Michael Padilla, CIA, IT Director
Chris Polke, CGAP, PS Director
Shelli Browning, Technical Editor
Lauressa Nelson, Technical Editor
Geoffrey Nordhoff, Content Developer, Technical Writer
Christine Janesko, Content Developer, Technical Writer
Vanessa Van Natta, Standards and Guidance Specialist

The IIA would like to thank the following oversight bodies for their support: Financial Services Guidance Development 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 200,000 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

May 2020

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 149
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.globaliia.org