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](http://www.globaliia.org/standards-guidance).
# Table of Contents

Executive Summary .................................................................................................................. 2
Introduction ................................................................................................................................. 2
The Regulatory Landscape in Financial Services ................................................................. 4
  Internal Audit Interactions with Regulators ................................................................. 5
The Risk Landscape in Financial Services ............................................................................ 8
  The IIA’s Financial Services Risk Framework ............................................................. 15
  Performing Risk Assessments in Financial Services Organizations ..................... 18
Key Principles of Sound Risk Governance .......................................................................... 19
  Risk Appetite ......................................................................................................................... 19
  Risk Governance Roles and Responsibilities ............................................................... 20
Working with the First and Second Lines of Defense ......................................................... 21
  Leveraging Interactions with Business Lines, Second-line Functions, and Internal Audit ...... 22
Internal Audit Responsibilities ............................................................................................... 25
  Sourcing Engagements ........................................................................................................ 25
  Engagement Planning ........................................................................................................... 27
  Audit Execution .................................................................................................................... 28
  Reporting .............................................................................................................................. 29
  Monitoring Recommendations and Remediation of Findings .................................... 30
Balancing Risk and Regulatory Requirements .................................................................... 30
Managing the Internal Audit Activity in Financial Services Firms .................................... 31
  Organizational Structure ..................................................................................................... 32
  Hiring Strategies .................................................................................................................. 34
  Obtaining Specialty Skill Sets ............................................................................................. 35
  Rotation ............................................................................................................................... 36
  Training ............................................................................................................................... 36
  Quality Assurance and Improvement Program ............................................................... 37
Appendix A. Related IIA Standards and Guidance ............................................................... 38
Appendix B. Glossary ................................................................................................................ 40
Appendix C. Key Regulatory Principles for Financial Services Organizations .................. 42
Appendix D. Acronym Guide ................................................................................................. 45
Appendix E. The Role of Central Banks .............................................................................. 47
Appendix F. Sample Risk Categories — Financial Institutions ........................................ 48
Appendix G. Sample Risk Categories — Insurance Companies .......................................... 49
Appendix H. References and Additional Reading .............................................................. 50
Acknowledgements ................................................................................................................ 52
Executive Summary

The demand for internal auditors with financial services knowledge and experience is growing rapidly, propelled by regulatory pressures to appropriately staff internal audit programs with the right volume and caliber of resources. This has led many internal audit activities within the highly regulated financial services industry to increase their staff in accordance with the new global operating environment and in terms of quality and quantity.

Among other abilities, internal auditors must be skilled in assessing how well an organization’s operations align with its risk appetite, customer, and regulatory expectations. They must also be able to provide the insight key stakeholders seek to do their jobs.

There is a gap in internal audit-specific guidance supporting the education and training of financial services auditors. The industry requires its practitioners to have specific knowledge that addresses functions in a unique atmosphere, such as requirements and expectations of regulators, complexity of products, and the role internal auditors can perform in safeguarding the organization, stakeholders, customers, and employees, and the community itself. Managing these requirements and expectations and assuring priorities are addressed requires a high level of proficiency and competence, but also creativity and innovation.

Much is at stake, because these requirements result in an exponentially diverse and synergistic environment for the financial services auditor when combined with additional expectations, such as knowledge and impact of culture, conduct, remuneration, and linkages to specific bank and other financial services regulations.

This guidance informs and educates internal auditors who may be new to the financial services industry about the regulatory environment in which these organizations operate. This guide also provides internal auditors and other key stakeholders with an overview of how managing an internal audit function within the financial services industry differs from other industries in terms of regulatory interaction, governance, and risks.

Introduction

Without appropriate guidance, training, and education, and a code of ethics by which to abide, the financial services industry may be challenged to find enough capable, competent internal auditors to fulfill the responsibilities across this unique landscape. This may lead to unidentified and unmitigated risks, which may increase the risk exposure of financial services firms, increase regulator enforcement actions, and erode consumer confidence.

Note: Terms in bold are defined in the glossary in Appendix B. In addition, acronyms used in this guide are spelled out in Appendices C and D.
Managing the internal audit activity properly and with a forward-looking view in this field of high expectations is key. This guidance will highlight the importance of managing an effective internal audit activity within the financial services industry, including:

- The risk landscape in financial services.
- The regulatory landscape in financial services.
- Key principles of sound risk governance.
- Collaboration with other assurance providers.
- Internal audit coverage.
- Internal audit activity management in the context of financial services.

After reading this guidance, internal auditors should be able to:

- Understand the financial sector environment, including key objectives, business areas, and related risks as well as the impact of globally accepted principles that provide the foundation for laws and regulations within the industry.
- Identify industry-specific risks relevant for the jurisdiction in which a company operates and commonly used frameworks.
- Understand the main principles of organizational governance in financial services organizations.
- Identify the roles and assurance activities of the second line of defense functions within financial services that provide coverage of sector-specific risks.
- Understand the relationship internal audit has with its external regulator/supervisor and how to effectively manage expectations of the regulator while maintaining a reporting relationship to the board.
- Identify the organization’s level of maturity in regard to working across risk and control functions (from completely siloed to fully integrated).
- Understand how the second-line functions can integrate with internal audit activities such as risk assessment, planning, leveraging engagement work and conclusions, and reporting results.

It may help to read this guide in conjunction with other practice guides available on the topic of financial services:

- Practice Guide “Auditing Capital Adequacy and Stress Testing for Banks.”
- Practice Guide “Auditing Model Risk Management.”

Readers are also encouraged to review The IIA’s Code of Ethics and the International Standards for the Professional Practice of Internal Auditing.
The Regulatory Landscape in Financial Services

Two types of regulators oversee financial services organizations. Prudential regulators require financial services organizations to manage risks and hold adequate capital as defined by capital requirements (e.g., safety and soundness). Supervisory regulators examine the financial condition of individual financial services organizations and evaluate compliance with laws and regulations, including consumer protections laws. In the United States, for example, the Federal Reserve Board (FRB or the Fed), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) are prudential regulators that also have supervisory authority. Regulators performing only supervisory roles along with consumer protection include the Consumer Financial Protection Bureau (CFPB) and the U.S. Securities and Exchange Commission (SEC), among others.

These organizations frequently share information among themselves. International, national, regional, and local regulators can and do contact other agencies to share examination results, risk information, and other intelligence.

When examining financial services organizations, regulators employ various techniques, such as:

- Using self-assessments to gather information.
- Outsourcing certain examinations in their entirety or in part.
- Asking internal auditors within the subject financial services firm to conduct audits for them.
- Executing joint examinations with other agencies.
- Sending auditors to observe examinations conducted by other regulatory bodies.

Trends indicate that prudential and supervisory regulators are spending more time with organizations’ second-line functions, such as financial controls, risk management, compliance, and others, working directly with businesses to gather information and perform examinations with the functions that execute the transactions in real time. In the United States, the FRB expects proficiency in second-line functions, looking at individual business lines’ control self-assessment work and evaluating risk escalation protocols. The expectation is that an organization’s management is doing its job in terms of owning their risk issues and control testing.

Unlike prudential regulators who tend to have a more active examination schedule, supervisory regulators are unlikely to approach a financial services firm unless there is an issue. In the United States, for example, the SEC and the Financial Industry Regulatory Authority (FINRA) may not visit or examine an institution unless a situation arises that affects consumers and reaches a certain
threshold of damage. However, in public commentary these agencies have both stated they will be increasing their onsite visits in the future. Contrary to the practices of the SEC and FINRA, the CFPB actively performs reviews of financial services firms above $10 billion in assets.

There is no consistent rule regarding the performance of examinations that can be applied to all regulators. Timing of examinations may be on a regular schedule chosen by the regulator, driven by risk assessments done by the regulator, or mandated by law.

**Internal Audit Interactions with Regulators**

Internal auditors are generally familiar with regulators’ language, so are often called upon to organize examinations including kickoff and closing meetings. They may participate in or observe kickoff meetings because it is helpful to understand what regulators are communicating to management. Anecdotally, it appears to be unusual for internal auditors to sit in on the individual meetings between managers and the examiner, but it is common for the examiners to meet with internal auditors separately to obtain an understanding of what they know regarding known open issues, process changes, new products, and/or other issues. In most organizations, internal auditors will attend closing meetings, and any issues that result from an external examination may be incorporated into their audit scope.

Regulators communicate directly with management, but internal audit may be heavily involved, especially if asked to provide the regulators with their work on fraud, credit, risk management, and other areas of focus. Examiners will take information directly from business units and from internal audit, too. In some situations internal audit acts as an extension of the regulatory body. For example, the European Central Bank (ECB) can request auditors in member national central banks to perform audits on their behalf.

Regulators differ in how much they will rely on the work and information they obtain from internal auditors. In the United States regulators will rely on internal audit’s work to varying degrees; however, they will also conduct full scope examinations of internal audit.

It is recommended that internal audit activities follow up on findings of external auditors and regulators, especially if external auditors review regulatory issues in addition to their own audit scope. There may be a collaboration between the external auditors and the supervisory authority, in which the external auditor may send its reports to the authority and may wield some of the supervisory entity’s authority.

It is important that there be transparent communication between the supervisory authority and the internal audit function to avoid problems. Regulators have noted that before the 2008 global financial crisis, internal auditors were not necessarily as independent as they should have been nor were they adequately resourced; however, supervisors and regulators typically now grant the internal audit role an authority and an importance previously unseen. The reliance of the supervisors and regulators on the work and insight of internal auditors makes meetings and
communication between the entities of critical importance. In turn, the internal audit activity also has a responsibility to maintain confidential supervisory information that may be learned/used during examinations. The IIA’s Code of Ethics offers guidance to internal auditors on the topic of confidentiality, among others.1

Here are some examples of interactions for the various types of regulated financial services organizations, including nonbank financial institutions.

**Banks**

*Example 1:* A large bank in the United States is overseen by two primary regulators: the Fed and the OCC, which coordinate their examinations and share results between them. Recently, the Fed and the OCC conducted a joint examination covering anti-money laundering (AML) and other topics related to the U.S. Bank Secrecy Act (BSA). Advantages of this arrangement include avoiding duplicating work and better enabling management of resources because internal auditors often perform procedures for or help the regulators with gathering/understanding information for the examination.

*Example 2:* A community bank in the United States is regulated by the FDIC and the state’s department of banking. From the bank’s perspective, expectations can change from examiner to examiner but from a general viewpoint, bank regulators expect internal audit to have a risk-based audit plan while still covering regulatory requirements in its audits. To meet this goal, the chief audit executive (CAE) transformed the internal audit department by adding cutting-edge skill sets and personnel to provide more value to the bank. Then the CAE discussed this plan with the regulators to obtain their agreement. Afterward, the CAE stated, “If you are transparent with (regulators) and say how you will take the path forward, they will measure your progress against the goals you have shared with them.” During scheduled updates with the regulator, the CAE made sure his transformation plan was linked to quality results, exam results, and best practices. His experience

---

of managing change and meeting the expectations of the organization and its regulators was positive due to his proactive approach.

In general it is incumbent upon financial services organizations and their internal audit activities to establish good working relationships with their regulators. This may enable auditors to understand and anticipate changing expectations.

**Insurance**

*Example:* A U.S.-based insurance company has a group in London that is regulated by the Prudential Regulation Authority (PRA). The CAE of this company has to sign certifications stating their organizations comply with relevant regulations every year. This CAE reports the internal audit teams enjoy an open communication relationship with the regulators. Her team often performs work for the PRA, which is open about their questions for and expectations of the internal audit function. The PRA in turn values internal auditors’ perspectives on the business and the results of their audit engagements.

If the PRA kicks off a strategic review of a business line, they will interview the CAE. Occasionally, this insurance company’s state-based regulator will jointly participate with the PRA on informational meetings and discussions around work previously completed by internal audit. The PRA also receives copies of progress reports, organizational information, and internal audit’s annual plans.

Internal auditors should seek to develop a partnership approach to their communications with regulators and work with them to ensure information flows appropriately throughout the organization and to/from the regulator. Some regulators have published guidance on the role of internal audit and on the communication standards between internal audit and regulators. See SR 13-1 issued by the FRB in the United States and “Final Report on Guidelines on Communication Between Competent Authorities and Auditors” issued by the European Banking Authority (EBA).2,3

**Asset Management**

Even in financial services areas such as asset management that (in some cases) are less rigorously regulated than banks, there are still multiple regulators with differing perspectives, mandates, and procedures to navigate. Internal auditors should be aware of the regulators and regulatory networks applicable at global, regional, national, and local levels. (See Appendices C and F for more information.)

---


The Risk Landscape in Financial Services

Financial services industries are highly regulated on a global basis and subject to contagion and systemic risks. Many financial services organizations offer a wide variety of products and services (e.g., insurance companies may operate banking functions, and banks may offer services of insurance companies or asset managers). This complicates the categorization of financial organizations, and in turn, complicates the regulatory environment in which they function.

At a high level, the financial services industry includes these areas of focus:

- **Banks** — There are differing types of banks of varying asset sizes with global, national, and community footprints. These institutions have their own charters and mandates. For example, in the United States, there are mutual banks, savings and loans, credit unions, and more. Around the world there are retail banks and investment banks, among others. Each type is subject to discrete sets of regulations that vary at the global, national, and regional level. Different regulators become involved based on the products and services each institution offers its customers.

- **Nonbank financial institutions (NBFIs)** — A multitude of organizations that perform such services as providing traveler’s checks, retail foreign currency exchange, money transmission, check cashing, and money orders come under this heading. This category also includes some insurance organizations, venture capitalists, micro loan organizations, and even pawn shops, according to the World Bank. These entities do not have banking licenses and are not necessarily supervised by any national or international banking regulatory agency, although they may require permits and other documentation to operate in certain jurisdictions.

- **Insurance companies** — These are generally divided by product lines offered, such as life and health insurers, property and casualty insurers, and reinsurance providers. Numerous subcategories are included as well:
  - Health: providing payment of benefits as a result of sickness or injury, including losses from accident, medical expense, or accidental death and dismemberment.
  - Life: paying designated beneficiaries upon the death of an insured person. Certain products can include the risk of terminal illness or critical illness.
  - Annuities: providing streaming payments as insurance against the possibility that a retiree will outlive his or her financial resources.
  - Property and Casualty: providing a wide range of coverages to help individuals and companies manage their risk of loss. Commercial coverages include property, workers’ compensation, employment practices liability, general liability, directors’ and officers’ liability, automobile, cyber, surety bonds, errors and omissions, medical

---

professional liability, crime and fidelity, equipment breakdown, and agricultural crops. Personal lines coverages include property (homeowners), flood, automobile (property and liability), mortgage, boats, and pets.

- Reinsurance: insurance coverage purchased by an insurance company, in which some part of its own insurance liability is passed on or ceded to another company.
- Pensions and retirement accounts: considered to be within the insurance sector. In the United States, insurers are regulated at the national and state level. In the European Union (EU), the European Insurance and Occupational Pensions Authority (EIOPA) plays the key role regarding the legal framework in which they provide input into the European Commission’s policymaking.5

- **Asset management** – In the financial services context, asset management is the direction of client investments by a bank or a special investment company that makes the investment decisions in the interest of the client, but at its own discretion. The investments are kept in segregated client accounts or investment funds. Typical asset classes are equities, fixed income, real estate, and private equity.

These sectors are regulated in a manner similar to a matrix organization in which one organization is supervised by several regulators depending on the products and services being offered and/or their location.

**Global Standard Setters**

The Bank for International Settlements (BIS), representing countries around the world, states, in part, that its mission is to serve central banks in their pursuit of monetary and financial stability.6 It hosts nine international organizations, including the Basel Committee of Banking Supervision (BCBS), the primary global standard setter for the prudential regulation of banks. It is vital for internal auditors to recognize different regulatory authorities and supervisory agencies all over the world. BIS provides a list of authorities on its website.7

While some supervisory authorities regulate both insurance companies and banking institutions, it is important to those who work in the insurance industry to understand the purpose and duties of the International Association of Insurance Supervisors (IAIS). According to their website, “Established in 1994, the IAIS is a voluntary membership organization of insurance supervisors and

---

regulators from more than 200 jurisdictions, constituting 97% of the world’s insurance premiums. It is the international standard-setting body responsible for developing and assisting in the implementation of principles, standards, and other supporting material for the supervision of the insurance sector. The IAIS mission is to promote effective and globally consistent supervision of the insurance industry ... to develop and maintain fair, safe, and stable insurance markets for the benefit and protection of policyholders and to contribute to global financial stability.”

**Structure of Banking Regulatory Supervision in the United States**

The structure of regulatory supervision over banking in the United States is illustrated in Figure 1 using a fictional banking institution, Bank ABC in the state of New York, as an example.

**Figure 1: Sample Regulatory Supervision Entities for Mid-sized Bank in the U.S.**

<table>
<thead>
<tr>
<th>International Standard-setting Bodies</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Basel Committee on Banking Supervision</td>
<td></td>
</tr>
<tr>
<td>2. International Organization of Securities Commissions</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Federal Regulators</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Consumer Financial Protection Bureau</td>
<td></td>
</tr>
<tr>
<td>4. Federal Deposit Insurance Corporation</td>
<td></td>
</tr>
<tr>
<td>5. Federal Emergency Management Agency</td>
<td></td>
</tr>
<tr>
<td>6. Federal Financial Institutions Examination Council</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ABC Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>New York, NY, USA</td>
</tr>
<tr>
<td>$20 billion in assets</td>
</tr>
</tbody>
</table>

**Business Lines**

- Capital Markets
- Commercial Banking
- Payments
- Retail Banking
- Wealth Management

<table>
<thead>
<tr>
<th>State of New York Regulators</th>
</tr>
</thead>
<tbody>
<tr>
<td>13. Department of Financial Services</td>
</tr>
<tr>
<td>14. Department of State</td>
</tr>
<tr>
<td>15. Bankers Association</td>
</tr>
</tbody>
</table>

Source: The Institute of Internal Auditors.

This fictional U.S. bank, depending on asset size, is subject to examination from 15 supervisory bodies, assuming the bank only has branches in the state of New York. If the bank had branches in all 50 states, then the regulatory bodies for all 50 states would be included. If the bank participated in insurance markets, the insurance regulatory bodies would be involved as well. As the financial services firm’s business lines, assets, and geographical footprint expand, so does the regulatory burden.

---

Structure of Banking Regulatory Supervision in EU Countries

The structure of regulatory supervision over banking in one EU country is illustrated in Figure 2 using a fictional banking institution, Bank DEF in the Netherlands, as an example.

Figure 2: Sample Regulatory Supervision Entities for Mid-sized Bank in the Netherlands

<table>
<thead>
<tr>
<th>International Standard-setting Bodies</th>
<th>National Regulators</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Basel Committee on Banking Supervision</td>
<td>4. Dutch Central Bank (De Nederlandsche Bank)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>European Regulator</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3. European Central Bank</td>
<td></td>
</tr>
</tbody>
</table>

The European System of Financial Supervision (ESFS) is an integrated network of national and European supervisory authorities. The European Banking Authority (EBA) is an independent EU authority that works to ensure effective and consistent prudential regulation and supervision across the European banking sector. Its overall objectives are to maintain financial stability in the EU and to safeguard the integrity, efficiency, and orderly functioning of the banking sector. The ECB is the direct supervisor of banking institutions ensuring the sector follows the directives of the EBA.

As mentioned above, the ECB is responsible for regulating the larger banks in the EU. This is accomplished through the Single Supervisory Mechanism (SSM). The main aims of the SSM are to contribute to the safety and soundness of credit institutions and the stability of the European financial system and to ensure consistent supervision. As illustrated in Figure 2, in the Netherlands the ECB works in cooperation with the Dutch Central Bank (De Nederlandsche Bank) and the Netherlands Authority for the Financial Markets (Autoriteit Financiële Markten) to supervise banks.

Structure of Insurance Regulatory Supervision in the United States

Insurance companies tend to be regulated more heavily on the state level than banking institutions are in the United States. The IAIS sets global standards, but those standards are combined with national and state regulations and directives to form the total regulatory regime.

---

for insurance companies. State regulators are given authority by state governments to oversee the insurance industry and implement insurance regulations. State regulators (all of whom are members of the National Association of Insurance Commissioners (NAIC)) are responsible for ensuring insurance companies are financially solvent, and that claims are paid out fairly and as required in policy contracts.

The two main federal regulatory bodies for the insurance industry in the United States are the Financial Stability Oversight Council (FSOC) and the Federal Insurance Office (FIO). Both bodies were established by the Dodd-Frank Act. The FIO is housed within the Treasury Department and is headed by a director appointed by the Secretary of the Treasury. The FIO advises the United States government on insurance matters and engages in international discussions relating to insurance. The FIO director serves as an advisory member to the FSOC.

FSOC monitors the overall financial system in the United States including the insurance industry. The FSOC is responsible for identifying risks that could lead to a systemic crisis, promoting market discipline, and responding to emerging risks to the stability of the United States’ financial system. FSOC is authorized to identify NBFIs and assign them a systemic designation that brings those companies under supervision of the Fed. The FSOC has used its authority to identify certain insurance companies as NBFIs.

At the state level, insurance companies must comply with state securities departments and the NAIC, which comprises chief insurance regulators from all 50 states. The NAIC serves as a forum for individual state regulators to coordinate their activities and share resources. The NAIC also functions as an advisory body and service provider for state insurance departments to assist them in their oversight responsibilities.

**Figure 3: Structure of Insurance Regulatory Supervision in the United States**

<table>
<thead>
<tr>
<th>International Standard-setting Bodies</th>
<th>State Regulators</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. International Association of Insurance Supervisors</td>
<td>4. State securities departments</td>
</tr>
<tr>
<td>2. Financial Stability Oversight Council</td>
<td>5. National Association of Insurance Commissioners (Chief Insurance Regulators from all 50 states)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Federal Regulators</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Financial Stability Oversight Council</td>
<td></td>
</tr>
<tr>
<td>3. Federal Insurance Office</td>
<td></td>
</tr>
</tbody>
</table>

Source: The Institute of Internal Auditors.

---

Structure of Insurance Regulatory Supervision in EU Countries

Insurance companies in the EU are governed by a harmonized prudential framework known as Solvency 2. Similar to Basel III for the banking industry, Solvency 2 requires insurance companies to hold capital in relation to their risk profiles to guarantee they have the resources to withstand financial difficulties. Solvency 2 also outlines requirements for corporate governance, risk management practices, and supervisory reporting and public disclosure. The European Commission issued the Solvency 2 directive and EU countries must translate the directive into national law. The European Commission then supports EU countries in this process and monitors the adoption of the national measures individual countries have decided to require. In Germany, for example and as shown in Figure 4, Solvency 2 has been adopted and is monitored by the Bundesanstalt fuer Finanzdienstleistungsaufsicht (BaFin). BaFin reports results of examinations back to the EC and to the EIOPA.

Figure 4: Structure of Insurance Regulatory Supervision in Germany

<table>
<thead>
<tr>
<th>International Standard-setting Body</th>
<th>Country Regulator</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. International Organization of Securities Commissions</td>
<td>4. Bundesanstalt fuer Finanzdienstleistungsaufsicht (BaFin)</td>
</tr>
<tr>
<td>European Regulators</td>
<td></td>
</tr>
<tr>
<td>2. European Commission</td>
<td></td>
</tr>
<tr>
<td>3. European Insurance and Occupational Pensions Authority</td>
<td></td>
</tr>
</tbody>
</table>

Source: The Institute of Internal Auditors.

EIOPA provides the EC with technical advice regarding Solvency 2 and any amendments to the law. EIOPA’s responsibilities are similar to the FSOC in the United States. EIOPA’s responsibilities are also to support the stability of the financial system, transparency of markets, and financial products as well as the protection of policyholders, pension recipients, and beneficiaries. EIOPA also monitors risks that could lead to systemic issues in the EU’s financial systems.

Structure of Asset Management Regulatory Supervision in the United States

Regulation of asset managers in the United States has not changed significantly since the 1930s. The Securities and Exchange Commission (SEC) is the primary regulator of investment companies and investment advisers in the United States. The primary law that governs U.S. investment companies is the Investment Company Act of 1940. The SEC has adopted various regulations under the Investment Company Act that further govern investment company operations. These regulations are published in Title 17 of the Code of Federal Regulations (CFR), Part 270. Investment companies are also subject to other federal securities laws (e.g., the Securities Act of 1933 and the Securities Exchange Act of 1934). The SEC has also adopted various regulations generally applicable to investment companies under these laws.12

Generally, individuals who manage the portfolios of registered investment companies must register with the SEC as investment advisers under the Investment Advisers Act of 1940. The Advisers Act, and regulations adopted by the SEC under the Investment Advisers Act, govern registered investment advisers. The regulations are published in 17 CFR, Part 275.

FINRA is not part of the U.S. government; it is overseen by the SEC. It is a not-for-profit entity, and the largest self-regulatory organization (SRO) in the securities industry in the United States (an SRO is a membership-based organization that creates and enforces rules for members based on federal laws). FINRA is involved in licensing and regulating broker-dealers. They are also part of the insurance regulatory environment as representatives must have the appropriate FINRA license to sell annuities.

Structure of Asset Management Regulatory Supervision in European Union

In the EU the fund management sector covers a wide range of entities and activities, including fund administrators, depositaries, specialist providers (e.g., risk management consultants), and valuers. There are also many types of funds, some of which area covered by bespoke legislation, including the Regulations and European Venture Capital Funds (EuVECA), European Social Entrepreneurship Funds (EuSEF), and European Long-term Investment Funds (ELTIF).

In general, the three main directives having the most effect on EU asset managers are:


The European Securities and Market Authority (ESMA) is active in the area of collective investment management, commonly known as fund management. ESMA’s role with respect to UCITS and AIFMD has included issuing technical advice to the European Commission, developing guidelines

to market participants, preparing regulatory and implementing technical standards, and issuing opinions. Although most of ESMA’s work in the fund management area relates to UCITS and AIFMD, ESMA also carries out work in relation to venture capital funds, social entrepreneurship funds, and long-term investment funds.

MiFID II comprises several laws passed by the European Union intended to reform the entire financial services industry. MiFID affects all financial services organizations; however, it has two main objectives that affect asset managers more than other organizations:

1. Regulates off-exchange and OTC trading, essentially pushing it onto official exchanges.
2. Increases transparency of costs and improves record keeping of transactions.

As an example, in Germany asset managers are directly supervised by BaFin. BaFin generally adopts guidelines issued by the EBA, the ESMA, and the EIOPA, collectively known as the European supervisory authorities (ESAs). As a joint committee, these three regulators also issue guidance. BaFin has been examining large asset management companies approximately every three years; however, at least once a year, the regulator meets with company management.

**The IIA’s Financial Services Risk Framework**

To properly manage the risks facing their organization, employees must understand the terminology associated with risk management, compliance, and internal auditing. One tool to communicate risk information across organizations is a risk framework. The IIA’s Financial Services Guidance Committee has developed a comprehensive risk framework specifically for financial services organizations. This risk framework, depicted in Figure 5, considers the major areas of risk applicable to the financial services industry on a global basis.

Organizations may establish a risk framework according to their structure, product mix, size, and other factors. Each risk area should be defined and customized according to the financial services organization applying it. Developing a common language regarding risk is a key component of having a functioning risk governance process within an organization. The IIA offers the model shown that may be adopted or adapted as needed.
Organizational Risk Drivers

Strategic and reputational risk are at the top of the framework because they are overarching drivers of organizational risk.

**Strategic Risk** – The risk of decline in net income, below a set limit, due to unforeseeable changes in either revenues or fixed costs that may be caused by external trends in financial organizations’ competitive environment or the extent to which an organization could timely adapt to these trends.\(^\text{13}\)

**Reputational Risk** – Reputational risk can be defined as the risk arising from negative perception on the part of customers, counterparties, shareholders, investors, debt-holders, market analysts, other relevant parties or regulators that can adversely affect a bank’s ability to maintain existing or establish new business relationships and continued access to sources of funding. Reputational risk is multidimensional and reflects the perception of other market participants.\(^\text{14}\)

---


Financial Execution Risks

The five risk pillars constitute the major execution risks faced by financial services firms.

**Liquidity Risk** – A financial organization’s inability to meet financial demands, often due to the failure to convert other assets to liquid capital without incurring additional losses.

**Capital Risk** – Failure to retain enough capital to run the business while still absorbing the risk and volatility of its credit, market, and operational threats.

**Credit and Counterparty Risk** – The potential that a financial organization, borrower, or counterparty will fail to meet its obligations in accordance with agreed terms.\(^\text{15}\)

**Market and Interest Rate Risk (IRR)** – Potential for losses in on- and off-balance sheet positions arising from adverse movements in market prices. Includes pricing and interest rate risks.\(^\text{16}\)

**Insurance Risk** – Likelihood of loss due to outcomes emerging unfavorably from original expectations during an insurance product’s design and pricing. This results from incorrect assumptions built into the policy price (i.e., how long the policy remains in force without lapsing/replacement [persistency], how healthy the insurance company assumes the policyholder will be [morbidity], and miscalculating the policyholder’s life expectancy [mortality], etc).

Enterprisewide Risk Areas

The four horizontal risks beneath the pillars may occur across them, possibly affecting the entire organization.

**Model Risk** – The potential for adverse consequences from decisions based on incorrect or misused model outputs and reports.\(^\text{17}\)

**Compliance Risk** – The risk of legal or regulatory sanctions, material financial loss, or loss to reputation a financial organization may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, or codes of conduct applicable to its financial activities.\(^\text{18}\)

---


Operational Risk – The risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events.  

Asset/Liability Matching Risk – Practice of managing risks that arise due to mismatches between the assets and liabilities. Includes risk exposure generated by strategies employed to optimize assets (e.g., liquidity, maturities, interest rate environment, mix of asset classes) so future cash flows of assets match future obligations in the most efficient way.

Foundation

Culture and Conduct Risk underlie the entire financial services organization. Culture determines the organization’s values while conduct illustrates the commitment to those values.

Culture and Conduct Risk – 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.

Performing Risk Assessments in Financial Services Organizations

According to Standard 2010 – Planning, “The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization’s goals.” That means internal audit engagements are to be driven by risk levels rather than regulatory requirements.

Ideally, internal auditors will assess risks on the same scale and in the same categories used in risk assessments in all areas of the business. Planning an internal audit engagement considering risks in these categories will often achieve compliance with many regulator expectations. However, these categories do not always include regulatory requirements regarding compliance issues or emerging risks to the industry.

Significant risks associated with disruptions and threats such as artificial intelligence, FinTech, robotic process automation, and others have not yet been fully addressed by regulatory bodies. Often financial services organizations must learn to identify, assess, and manage emerging risks in the absence of regulation to guide them while balancing their objective of covering known regulatory requirements.

As internal auditors conduct engagement-level risk assessments, they should review past audit or examination workpapers for the process, department, risk, or product they are planning to audit, and consider the last time an end-to-end engagement was completed, as well as the last time a targeted engagement was completed. In planning individual engagements involving strategic risks or risks that cross departments or business lines, internal auditors should consider information from the organizationwide risk assessment, if one exists.

As risk assessments are performed throughout the organization and second line of defense functions such as legal, compliance, and risk management pursue their testing and monitoring duties, risk information should flow throughout the organization freely.  

Key Principles of Sound Risk Governance

Internal auditors in financial services should recognize the importance of an effective risk governance structure’s key elements. A clear risk appetite and risk governance framework are central to a financial services firm’s performance.

Risk Appetite

The IIA defines risk appetite as the level of risk that an organization is willing to accept. Organizations should include their definition of risk appetite in their risk strategy. According to the EBA, management’s responsibilities include setting, approving, and overseeing the implementation of the organization’s overall risk strategy. This includes their risk appetite, its risk management framework, and measures to ensure that the management body devotes sufficient time to risk issues.

---


Financial services firms should be proficient at articulating, communicating, and ensuring conformance with an agreed-upon risk appetite; however, this may not always be the case. For some organizations, key risk indicators (KRIs) are set and tracked at the executive level but are not shared with the business-line level. This can result in a conflict between the stated risk appetite and loss aversion, as illustrated in Figure 6.

**Figure 6: Risk Appetite versus Loss Aversion**

Organizations may have difficulty linking risk appetite to metrics used to manage to that appetite. Financial services organizations usually have complex types of risks and a correspondingly complex risk limit structure. This can be further complicated by the need to communicate these metrics to appropriate personnel throughout the organization to aid in sufficient means of monitoring and reporting on them. It seems reasonable for an organization to concentrate on top-level metrics to simplify communications with the audit committee, management, and employees regarding risk appetite and risk metrics. However, as shown in Figure 6, an organization can accomplish this correctly and still fail to manage to the stated risk appetite.

Internal audit’s role is to determine objectively if risk appetite statements exist, are appropriate, and are executed and monitored consistently.

**Risk Governance Roles and Responsibilities**

Board-level visibility and reporting of risk information is important to regulators because they want assurance that boards receive transparent and understandable reports that are timely. It is important to have a documented risk governance structure by which the organization
communicates risk information. For more information on internal audit’s role in corporate governance, please see The IIA Position Paper, Internal Audit’s Role in Corporate Governance.²⁴

Working with the First and Second Lines of Defense

Financial services organizations vary widely on how well the second-line functions (e.g., financial controls, legal, compliance, risk management) work together. Some financial services organizations are still operating in silos with internal audit stepping in to audit the business (first line) and second-line functions in a traditional manner.²⁵ Sometimes historical organizational structures add even more complexity.

In Europe some financial services organizations split compliance into two departments: one is focused on regulatory compliance and the other is focused on investment compliance, which monitors limit violations. This structure adds a level of complexity as the functions are segregated, with each function having a separate reporting line through management and to the board. This creates a situation requiring internal audit to perform audit engagements on both areas of compliance and analyze them independently. However, in the present regulatory environment, these approaches are becoming costly and less effective. Many financial services organizations are developing ways for second-line functions to communicate proactively with each other to reduce audit fatigue and ensure adequate risk coverage across the organization.

Globally, smaller financial services organizations may have a risk management committee. Some are required to have an audit committee, and all must have a risk manager and a compliance officer. However, because of limited resources and the number of people within the organization, the risk and audit committees are often combined. In some banks, the executive manager (e.g., CEO/president) also serves as the head of risk management. This structure creates a situation in which the internal auditor must examine risk management across the enterprise more closely because the executive manager is monitoring work they also authorize, which can create a conflict of interest. Internal auditors must be more involved, conduct more testing, and gain a deeper


insight into what types of risk management should be present in financial services organizations that operate under this managerial structure.

One approach to improving interaction between second-line functions and internal audit may be the creation of a document stating the roles and responsibilities of each team throughout the second and third lines of defense (e.g., risk management, compliance, legal, and internal audit). One global insurance company created a document outlining distinct roles and responsibilities for each of the three lines of defense regarding risk and control. It is submitted for approval by their executive team and is regularly presented to the board. Quarterly meetings between the second and third line of defense discuss projects in each business line or risk area. Legal and compliance will conduct more thorough inquiries of their own and may ask internal audit for results from relevant audits that may be helpful. The second-line functions and internal audit also coordinate their work during plan setting and modification to help support comprehensive coverage of key risks and avoid audit fatigue within the business. Further, this company’s internal audit activity includes compliance, legal, and risk in their annual risk assessment interviews with executives.

Assuming the internal audit activity retains their independence and objectivity, reducing siloed functions that favor specific expertise and narrow scopes of work, and increasing interaction (such as general communication, sharing results, and partnering during audits to evaluate areas together) provides better insight. A wider view with diversity of thought allows thematic and systemic issues to be identified more quickly.

This type of coordination is unusual but as awareness grows that it is possible, more financial services organizations are exploring how they can begin to foster interdepartmental cooperation to better assess risk areas and serve the business.

**Leveraging Interactions with Business Lines, Second-line Functions, and Internal Audit**

Standard 2050 – Coordination and Reliance states that the chief audit executive should share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimize duplication of efforts. Encumbering obligatory requirements for the regulators and relevant supervisory authorities makes this provision of the standard very important. As addressed in The IIA Practice Guide “Coordination and Reliance, Developing an Assurance Map,” “various providers of assurance services contribute to an overall, organizationwide risk and control structure, together assuring that risks are identified and addressed to an acceptable level.” To fulfill requirements, documentation of an assurance map should always be a part of internal audit’s planning process.

---

In theory an organization should be able to operate without second-line functions or an internal audit activity. In smaller organizations, a hybrid compliance team may also have risk management responsibilities. However, if an organization starts combining more functions, it may risk developing a conflict of interest that damages the control environment. Figure 7 illustrates various combinations and considerations of each.

**Figure 7: Control Structure Variations**

<table>
<thead>
<tr>
<th>Scenario 1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Personnel</strong></td>
<td>Management</td>
</tr>
<tr>
<td><strong>Second-line Functions</strong></td>
<td>Compliance + Risk Management + Data Privacy Officer (required by GDPR regulations in Europe) + Anti-Money Laundering</td>
</tr>
<tr>
<td><strong>Internal Audit</strong></td>
<td>Internal Audit</td>
</tr>
</tbody>
</table>

**Considerations**

This is the most common structure found in smaller organizations. If risk, compliance, data privacy (in the EU) and anti-money laundering are combined, risk and compliance are providing insight and assistance. Also, risk and compliance are providing the framework used by management when they execute risk and control self-assessments (RCSAs) within the business. This still allows the second-line functions, including the data privacy officer and AML staff to build processes to manage compliance risk and understand what is expected from regulators. It also allows risk management staff to design and operate the financial services firm’s risk and control activities. Internal audit provides oversight and is able to test and evaluate the work of those in the risk, compliance, data privacy, and AML areas.

**Scenario 2**

<table>
<thead>
<tr>
<th>Scenario 2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Personnel</strong></td>
<td>Management</td>
</tr>
<tr>
<td><strong>Second-line Functions</strong></td>
<td>Risk Management + Data Privacy Officer (required by GDPR regulations in Europe) + Anti-Money Laundering</td>
</tr>
<tr>
<td><strong>Internal Audit</strong></td>
<td>Internal Audit + Compliance</td>
</tr>
</tbody>
</table>

**Considerations**

If compliance and internal audit are combined, then management’s responsibility to execute its controls and manage risks is more critical. Further, internal audit would be unable to perform audit engagements on the organization’s compliance activities, which leaves a significant area of risk uncovered. This structure also inhibits compliance specialists from designing and implementing compliance management systems to assist management in dealing with heavy regulatory activity. Compliance personnel would be confined to a purely testing-focused role.

---

27 General Data Protection Regulation (GDPR) legislation requires the data privacy officer be independent of management and internal audit.
Figure 7: Control Structure Variations (continued)

### Scenario 3

<table>
<thead>
<tr>
<th>Business Personnel</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second-line Functions</td>
<td>Data Privacy Officer (required by GDPR regulations in Europe) + Anti-Money Laundering</td>
</tr>
<tr>
<td>Internal Audit</td>
<td>Internal Audit + Compliance + Risk Management</td>
</tr>
</tbody>
</table>

**Considerations**

This scenario offers no layer of monitoring and prevention between management and internal audit beyond the data privacy officer and AML personnel. Internal auditors would be working in second-line functions and internal audit’s areas of responsibility. Internal audit would be prevented from testing and evaluating compliance and risk management activities or risk compromised perceptions of their work because they could not avoid auditing their own areas of responsibility. Even if the internal audit function was outsourced, someone within the organization would have responsibility for oversight of the outsourced function, meaning the service provider would report to that entity and likely lack direct access to the audit committee. In this scenario the financial services company typically outsources or cosources its reviews of risk management and compliance activities to a third party for a more objective/independent appraisal.

The only situation in which this combination may work is if the internal audit function is outsourced and that firm has direct access to the audit committee. In that case, the structure would resemble the first scenario variation with the compliance/risk manager providing limited administrative support to the outsourced internal audit firm.

### Scenario 4

<table>
<thead>
<tr>
<th>Business Personnel</th>
<th>Management + Compliance + Risk Management + Anti-Money Laundering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second-line Functions</td>
<td>Data Privacy Officer (required by GDPR regulations in Europe)</td>
</tr>
<tr>
<td>Internal Audit</td>
<td>Internal Audit</td>
</tr>
</tbody>
</table>

**Considerations**

Again, there is no second layer of protection between management and internal audit beyond the data privacy officer who must be independent per regulation. Many financial services organizations have employees who technically report to management but perform second-line function duties. Many organizations also have employees who technically report to the second-line functions but perform management duties. In this structure the second-line function is embedded within management, which eliminates their ability to be an objective challenger of management and dilutes their ability to act as a check on management. This leaves internal audit as the organization’s only means of testing and identifying issues.

Another conflict of interest that may arise is making internal audit responsible for the implementation of a new system or process. Internal auditors may be involved in a consulting capacity, highlighting risks and considerations. However, if internal audit is responsible for the design and implementation of a system or process, they would be disqualified from testing and evaluating that system or process under Standard 1100 – Independence and Objectivity.

Assuming an organization has the appropriate separation of duties regarding internal audit and the second-line functions, there are certain actions and characteristics that may make the relationship among the two functions and management run efficiently.

If the second-line functions and internal audit work together, the synergy should result in greater efficiencies in scanning for new regulations and guidance in the industry or other developments to
consider for methodology improvement. For example, in Portugal, a bank’s compliance function is usually responsible for identifying new regulations or changes to existing regulations. This is information needed not only by management but also by internal audit so they may adjust their audit plans and programs accordingly. Regulations such as GDPR, IFRS9, ECB Anacredit, AML, MiFID II, etc., changed radically in a two-year time period, requiring organizations to have timely and accurate information on new requirements to implement process changes properly.

Another key area of coordination is risk assessment. In most financial services organizations, risk management officers perform risk assessments. Each department may have a risk officer who reports to the risk management department and is responsible for maintaining and keeping the database of operational risk assessments current. Risk officers evaluate risks and the sufficiency and quality of controls.

If an organization includes the risk of natural disasters or incidents such as an IT disruption or pandemic incident in the operational risk category, risk officers could be responsible for the evaluation of a business impact analysis that is an essential part of the business continuity plan. The risk management department’s role is to ensure all other business risks (e.g., market, liquidity, credit, IT, reputation) are monitored. Only the compliance risks (legal and AML) are monitored by the compliance function, which makes communication between risk management, other second-line functions, and internal audit imperative.

**Internal Audit Responsibilities**

Standard 2000 – Managing the Internal Audit Activity states “the chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organization.” Further, the interpretation of the Standard states, “The internal audit activity adds value to the organization and its stakeholders when it considers strategies, objectives, and risks; strives to offer ways to enhance governance, risk management, and control processes; and objectively provides relevant assurance.” To add value, internal audit must identify and understand stakeholder expectations, perform a risk assessment resulting in an audit plan, and provide assurance over key risk areas to management and the audit committee.

Internal audit activities approach engagement planning according to the needs of the organization. CAEs must cover an organization’s high-risk areas that may imperil achievement of its objectives if they are not well-managed. In addition, CAEs must also adhere to regulatory requirements, maintain cyclical audit areas, and manage their available resources properly.

**Sourcing Engagements**

Annual audit plans are typically grounded in risks associated with the organization’s objectives. Financial services organizations may have overarching strategic objectives and operate toward objectives set by business lines, countries, or regions. If no strategic objectives are available,
internal auditors may contact management directly to document the goals they are expected to achieve for the year. Internal auditors may also read minutes from meetings of senior management and the board, and review the latest regulations to determine how changes may affect their organizations.

Other internal audit activities conduct audit risk assessments that detail key areas of the enterprise, looking at inherent risk, other indicators in the control environment, and residual risk. There will usually be a cyclical component to consider while risk-based audits may change. In this approach, high-risk areas would be covered annually as well as a percentage of low-risk areas, given available skill sets and resources. Internal audit must work with executive management and the board to determine the priorities of the activity, consistent with the organization’s objectives. With that information, according to Standard 2010—Planning, the CAE must establish a risk-based plan. More specifically, Standard 2010.A2 requires that the CAE must identify and consider the expectations of senior management, the board, and other stakeholders for internal audit opinions and other conclusions. Additionally, Standard 1111—Direct Interaction with the Board requires that a CAE must communicate and interact directly with the board. This process may be helpful in alerting internal audit to regulatory requests management has received and/or to new products and processes that are not yet implemented.

Internal audit activities in smaller organizations may have to further narrow their focus, perhaps by conducting an analysis of “critical functions,” or those that have potential gaps in oversight, are controlled by a select few, and could have a significant impact on the organization if something goes wrong. These functions may not always contain the highest rated risks, but the risks they represent may be the components of higher rated risks.

For example, an internal audit activity may have found historically that a bank’s smaller branches are not a high-risk area because they are closely managed and diligent about implementing internal controls. In this situation, internal audit may choose to conserve resources by auditing the low-risk small branches digitally and perform onsite audits of only larger branches. This should be a flexible plan if, for example, a small branch is implementing a new product (e.g., onsite credit card issuance) or taking other actions that qualify as high risk. In this case, the internal audit activity may choose to conduct an on-site audit of the branch. Flexible plans permit internal auditors to conduct fieldwork when necessary.

Some internal audit activities have the advantage of an audit system integrated into the core administrative system. Having this type of integrated audit system can provide significant efficiencies. Here are a few examples of financial services organizations using software to aid in the development of an integrated audit system:

- In a large mortgage servicing organization, under mortgage credit, an audit might reveal up to 1,500 control points. Software allows internal audit to determine whether management and risk management are matching the acceptable margins at any given time. It also allows internal audit to see the most repeated errors and, through data analytics, investigate to
determine if those errors are related to a lack of process efficiency. This may enable the activity to propose actions to correct the errors.

- In an organization with 2,500 branches, the internal audit activity maintains all branch audit data on their system to see current and past information in real time. They filter previous audit findings and look at a macro view of what is occurring in the branches of the bank holistically.

- If internal audit is using an integrated system that also contains compliance information, they may have access to contracts, new regulations, or new products. Internal auditors can then study areas relevant to planned audit(s) and work with scenarios using past related data. This analysis may assist internal auditors in identifying the existence and effectiveness of key control points. This analysis may lead to internal auditors altering their procedures since they have established confidence in management’s activities.

- Integrated systems can also track individual auditors who have previously performed engagements in the area under consideration. A CAE may save resources by assigning auditors familiar with the area’s processes. In doing so, the CAE must assure that Standard 1130 – Impairment to Independence or Objectivity is not breached, or if resources are constrained, disclose impairments in fact or appearance to appropriate parties.

- Systems may also contain notes after each audit in which control points that contain high-risk elements or other recommendations, issues, and more can be available for subsequent auditors.

Audit systems can be useful but even when there is no unique software supporting the second-line functions, it is important that internal audit be able to access any IT software in the institution including those that support risk management and compliance. This is essential when developing the audit plan and during the analysis phase.

**Engagement Planning**

Audit planning is the response to the risk assessment built on internal audit’s understanding of the business and discussions with stakeholders. Sound understanding of the business helps internal audit identify auditable units and strategies as a foundation for further information gathering to identify risks and formulate the audit universe. Even though the identification and prioritization of the financial organization’s risk is often determined from internal audit’s perspective, the use of other risk assessments performed by the business or risk function can prove helpful and effective in forming the basis of the risk universe. It can also reduce or avoid duplication of efforts. This information can be especially helpful for internal audit activities working with limited budgets and resources.

When the internal audit activity develops its annual engagement plan, it may obtain necessary information from the organization’s management and second-line functions. Standard 2201 – Planning Considerations states (in part) “the significant risks to the activity’s objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level”
must be considered in engagement planning. The last audit evaluation, the period of time since the last engagement, the depth of the last evaluation, or even the status of remediation items are examples of risk factors that can be considered. In financial services organizations’ business units, there are other risk factors such as nonperforming loans, earlier recommendations, implementation effectiveness, the number of claims, and more. Internal audit should ask other departments and the board for their opinions on other organizational risks, too.

When planning an engagement, reports from the regulators, second-line functions, and others must be considered as well as the recommendations and risk scores, applicable legislation, powers and tasks, and procedures manuals. At the kick-off meeting, internal audit should ask the director of the department being audited if there are any situations that should be added to the audit engagement. If possible and pertinent, add requested topics to the engagement and document the request in the workpapers.

Internal audit engagement workpapers and conclusions, self-assessments performed by management, and examinations conducted by second-line functions can be important inputs for projects that may be operating throughout the institution or even under consideration. Improvements or recommendations can be considered in similar future projects, which may result in a greater degree of effectiveness when fully implemented.

**Audit Execution**

An audit’s execution should be designed to meet stakeholder’s expectation and add value to the organization. One project may only amount to conducting a walk-through assessment to fulfill the requirements for proficiency and due professional care while another project may be examined in greater detail using various methods such as walk-through assessments, control testing, observation, root cause analysis, and more.

The following standards help guide this phase of an engagement:

- **Standard 2100 – Nature of Work** states that the internal audit activity must evaluate and contribute to the improvement of the organization’s governance, risk management, and control processes using a systematic, disciplined, and risk-based approach. Internal audit credibility and value are enhanced when auditors are proactive and their evaluations offer new insights and consider future impact.

- **Standard 2110 – Governance** states that the internal audit activity must assess and make appropriate recommendations to improve the organization’s governance processes for:
  - Making strategic and operational decisions.
  - Overseeing risk management and control.
  - Promoting appropriate ethics and values within the organization.
  - Ensuring effective organizational performance management and accountability.
- Communicating risk and control information to appropriate areas of the organization.
- Coordinating the activities of, and communicating information among, the board, external and internal auditors, other assurance providers, and management.

- **Standard 2120 – Risk Management** states that the internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

- **Standard 2130 – Control** states that the internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

### Reporting

To satisfy Standards 2400 – Communicating Results and 2410 – Criteria for Communicating after completion of an engagement, the internal audit activity must communicate the engagement’s objectives, scope, and results. **Standard 2410.A** states that engagement results must include applicable conclusions, as well as applicable recommendations and/or action plans. Where appropriate, internal auditors’ opinions should be provided, taking into account the expectations of senior management, the board, and other stakeholders and must be supported by sufficient, reliable, relevant, and useful information.

Internal auditors may wish to preface the report with a brief executive summary that includes:

- An explanation of why the engagement took place (it was in the internal audit plan; it was a request of the board or the department’s director; it was a CAE’s decision based on risks imposed upon the institution).
- The scope of the engagement work.
- Relevant conclusions and recommendations or corrective actions.
- Final management action plan.

It may also include a short review of the personnel involved and the audit’s methodology, including interviews, sources of data and documents analyzed, and sampling dimensions and methods.

Following the executive summary, findings can be presented with a brief description of each risk, process, product, and so on, followed by potential impact(s) if not remediated, the recommendation and its owner (the department responsible for implementation), the risk type (i.e., operational risk, credit risk, liquidity risk) and the evaluation of the risk involved (low, medium low, medium high, high).

CAEs must communicate results to the appropriate parties, according to **Standard 2440 – Disseminating Results**. Different stakeholders may prefer different forms of reporting aligned with their function and expectations. Senior management must receive timely reports, with opinions (if issued) supported by sufficient, reliable, relevant, and useful information (**Standard 2450 – Overall**...
Opinions). Audit committees typically request detailed reporting, while the board of directors may be satisfied with the executive summary.

**Monitoring Recommendations and Remediation of Findings**

Supervisors in the financial services industry do not seek perfection, but they are concerned that second and third line functions (risk management, compliance, and internal audit) are working together and ultimately effective. To many boards, however, the investment of time, effort, and money devoted to internal controls to mitigate low-risk findings is less important when there are other business priorities and investments that take precedence.

There may come a time when a regulator or supervisory agency inquires as to why recommendations regarding low-risk regulatory issues have not yet been implemented. After every examination, regulators usually discuss findings with management and in doing so, anticipate that all failings or shortcomings discovered in an examination are addressed and remediated.

Internal audit should have a policy in place detailing how follow-up reviews are performed. Ideally there will also be a plan to periodically revisit engagement recommendations with respective business unit owners to understand any difficulties with implementation and help determine alternative ways to mitigate risks, if necessary. If numerous recommendations result from an audit engagement, it may be helpful to prioritize findings and pursue actions that would result in immediate satisfaction – or “quick wins” – and to help devise action plans for any remaining issues that require more attention. Action plans should include all identified irregularities, regardless of the risk level.

**Balancing Risk and Regulatory Requirements**

After the 2008 global financial crisis, many international standard-setting bodies and national/local regulators increased regulatory requirements on financial services organizations in an attempt to correct the internal control weaknesses that were perceived as causal. As a result, today’s regulatory environment for financial services organizations is more complicated and resource intensive than ever.

Internal audit activities with limited resources can save time and effort by coordinating with management and the organization’s second-line functions. Implementing software and using data analytics can help. Programs can be designed to digitally audit branch operations. None of this, however, changes regulators’ expectations or an institution’s obligation to abide by regulations. Financial services organizations typically operate in an environment requiring they postpone dealing with risks they would prefer to audit in favor of meeting regulatory requirements. This can be more difficult when expectations change from examiner to examiner or when examiners arrive unannounced. In these instances, examiners may not see internal audit working on issues they expect to see.
The lesson is that internal audit should be ready and able to defend their internal audit plans to regulators while still ensuring that they allocate enough time and resources annually to meet the examiners’ key expectations.

**Issues for Smaller Audit Activities**

One area smaller internal audit activities often struggle to cover to the satisfaction of regulators is IT. Examiners often expect coverage of a large portion of the IT risk universe on an annual basis. CAEs of smaller financial services organizations must often negotiate with examiners, explaining that performing this scale of audit is not efficient or risk-based.

Examiners assigned to a variety of institutions with varying levels of assets and resources may also expect smaller institutions to have processes, documentation, and analysis commensurate with larger multinational institutions.

**Example: Coverage of IT for Small Organizations**

A community bank adopted the National Institute of Standards and Technology (NIST) cybersecurity standard and evolved that to the Cybersecurity Assessment Tool (CAT). Internal auditors sat with examiners to show how their audit risk universe mapped to NIST, CAT, and COBIT and how auditable units were linked to each ranked by risk.

Every year the CAE completes a risk-based audit plan and will show the examiner which areas were audited. Areas not audited will undergo a control assessment (e.g., control maintenance testing with a wrapper opinion). This approach ensures the internal audit activity addresses the letter and spirit of the regulations while remaining risk-based.

**Managing the Internal Audit Activity in Financial Services Firms**

Financial services internal auditors have a duty to not only protect stakeholders, customers, and employees, but also the community itself. In this environment, financial services internal auditors must consider a more comprehensive risk universe including items such as culture, conduct, remuneration, and linkages to relevant regulations. This can result in a broader risk assessment and often a more thorough evaluation of the risks and controls than might be warranted in other industries. Further, regulators expect a certain level of proficiency and experience in specialized areas such as:

- Mathematical skills for actuarial and model reviews.
- Credit experience for lending.
- Agile and project management approaches.
- Organizational psychology for culture risk reviews.
- Computer science skills for data analytics and programming.
- Cybersecurity/data privacy.
- Compliance.
Complying with these elements requires more resources, specialized skill sets, and tools to fulfill responsibilities than may be found in typical internal audit activities.

Organizational Structure

Standard 1110 – Organizational Independence states “The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity.” It is crucial that the CAE have access to the audit committee even if the position does not directly report to the audit committee chair.

In many cases, the CAE has a dotted line relationship to the CEO or other member of the executive management team for administrative purposes (such as overseeing budgets and expense reports), but reports functionally to the audit committee chair. It is considered good practice to employ this parallel reporting structure. The executive to whom the CAE reports administratively should not have unilateral power to terminate the CAE’s employment. That should remain a function of the audit committee.

Beyond the CAE, internal audit activities generally follow a standard organizational structure. Figure 8 depicts a hypothetical organizational structure for a bank’s internal audit activity.

This chart is an example. Smaller organizations may have simpler segregation of duties and larger organizations may have additional levels, but financial services organizations’ internal audit activities should be structured in a way that is conducive to covering the entire audit risk universe in addition to its unique regulatory requirements.

For example, internal audit will ideally have IT specialists to provide support in obtaining data independently in addition to being able to perform IT audit engagements. Smaller organizations may only have one person in-house, so much of the internal audit function must be cosourced, usually to an independent audit firm. In these cases, the in-house audit staff must ensure the third-party audit firm provides the knowledge, skills, and other competencies needed to address executive management’s expectations as well as that of regulators and supervisors.
Figure 8: Sample Internal Audit Department Structure

**Team Responsibilities**

**Team 1**  
Responsible for internal audit engagements related to centralized departments (i.e., HR, Marketing, Finance).

**Team 2**  
Responsible for branch audits.

**Team 3**  
Responsible for audits of the IT function.

**Team 4**  
Responsible for fraud analysis.

**Team 5**  
Responsible regulation related audits including risk management, AML, ICAAP, ILAAP, stress testing, remuneration policy, etc.

Source: The Institute of Internal Auditors.
Hiring Strategies

Recruiting new hires depends on skills the department needs to fulfill its mandate. In searching for a junior staff auditor, consider recruiting from within the organization. Because no specific experience is required, an internal candidate could bring knowledge of the organization’s business processes, which may fulfill gaps in the department’s skill sets.

In general, recruiting experienced internal auditors can present challenges. Financial services organizations may consider sponsoring an internship program, which can serve to groom future talent. An internship can take several forms: the human resources department can help develop a structured summer internship in which interns may serve as part-time help doing high volume, low complexity work. The intern program coordinator may work with local colleges and universities to attract students taking courses in internal auditing or pursuing degrees in areas such as accounting, data analytics, or finance.

Example: In a medium-sized insurance organization, the CAE coordinates with the intern program coordinator to fulfill the equivalent of two full-time positions to work on areas such as Sarbanes-Oxley compliance work. The CAE stated, “People in this program can work for us for years, as long as they are in school. Some of them will do a summer internship in a public accounting firm and then come back to our company during the school year.” Since implementing this program, this company easily attracted new internal audit candidates who are already familiar with the organization.

Regulators routinely ask about internal audit staff expertise, so it may be beneficial to conduct periodic skill gap analyses when positions become available. This can help ensure the internal audit function is providing competent coverage relevant to risk-based auditing as well as areas of regulator focus.

Generally, there are few requirements besides business acumen and knowledge of a relevant academic field, such as finance, accounting, information technology, or mathematics for newly hired internal audit staff members. For growth opportunities within financial services organizations or promotion to managerial roles, certification in a relevant field may be required. Increasingly, regulators are expressing the need for internal auditors to have relevant certifications (e.g., CIA, CRMA, CISA, CPA, CA, CFE), and may question senior managers in internal audit who have yet to pursue credible certifications.

In some countries students who wish to apply for an internal audit position after completion of a university degree may be required to take an entrance examination. These examinations may also be required for experienced new hires. Country-level regulations may also mandate the level at
which new internal auditors may begin their careers, whether they are a recent graduate or an experienced hire, going so far as to require new hires to start as assistant auditors. Regulations may also mandate certain certifications for particular skill sets (e.g., the CISA for IT auditors). Internal audit managers should be aware of any regulations that could impact their selection of employees.

**Obtaining Specialty Skill Sets**

Occasionally, an engagement requires very specific knowledge in the financial services environment. To fulfill this obligation and to abide by IIA standards and its Code of Ethics in regard to competency, internal audit can and should request internal or external support if a knowledge gap exists among its staff. Cosourcing may be an option for small organizations or when internal audits only require a specialty skill set once every two or three years.

As an example of changing skill set requirements in the United States, the FDIC instituted new requirements for smaller institutions to audit financial models. In the past, institutions were only required to look at inputs, outputs, and policies. Verifying the accuracy of data feeds, the proper use of data, and that policies were followed fulfilled the requirement for internal audit activities.

Small internal audit activities (even those with only one or two internal auditors) are now required to conduct an enterprisewide inventory of models in use. If they do not have the skills to perform detailed audits of model risk management, a plan must be created outlining how this new requirement will be handled. Small financial services organizations may be required to include risk managers in internal audit engagements and coordinate closely with the entire second line of defense to ensure proper coverage. Alternatively, they may resort to cosourcing internal audit services, which carries additional, unknown risks.

Boards, and specifically audit committees, must be aware of the internal audit staff’s human resources needs. Understanding the skill sets required to fulfill the internal audit mandate and expectations of regulators may make approval of special training programs or appropriation of funds for engagements requiring specific knowledge from external sources more likely. CAEs may wish to perform annual benchmarking analyses to present to the audit committee including specialized training, certifications, and continuing professional education (CPE) costs. Audit committees have a vested interest in internal auditors performing engagements in a professional and competent manner and may be persuaded to allocate a budget with sufficient information from the CAE.

**Reliance on Organizational Control Functions**

For information on working with the organization’s other lines of defense, see IIA Practice Guide “Internal Audit and the Second Line of Defense.”
Rotation

In many organizations internal audit function roles are filled on a rotational basis. People who may not have an audit and risk management background rotate into internal audit from a business line or another function, and, according to Standard 1210 – Proficiency – “Internal auditors must possess the knowledge, skills and other competencies needed to perform their individual responsibilities.” This standard requires new auditors to receive extensive training to qualify as “proficient” in conformance with the Standard. The knowledge of “how to audit” is often temporary for those in a rotational role and may be offset by the specialized knowledge and experience these associates offer, such as understanding of credit, market, investment, trade, IT, back office operations, and more. In this model personnel may rotate to other areas of the organization after a few years. This is common practice in Japan, where people often remain with one company for their entire career. These lifetime employees obtain development and promotion opportunities by rotating through the company to various roles.

Training

Ongoing training is not only required for most certifications as CPE or continuing professional development (CPD), but is also important for new internal auditors and internal auditors moving into previously unfamiliar subject areas within the organization. Providing educational opportunities helps organizations fulfill Standard 1230 – Continuing Professional Development. Here are two examples of how this obligation may be met.

Example 1: An internal audit program within a European bank pairs new hires with senior auditors for a three- to six-month “welcoming and hosting program.” The new auditor will typically spend the first week participating in a multiday training about the function’s role in the institution. The new internal auditor is expected to read essential documents, such as The IIA’s International Standards for the Professional Practice of Internal Auditing, including the Code of Ethics, the organization’s internal audit charter, and notices issued by the institution’s primary regulator in which the internal audit function’s responsibilities are clearly defined. The senior auditor mentors the associate and works with other departments to schedule time for the new auditor to learn other areas of the business.

Example 2: An insurance company based in the United States encourages and supports internal auditors in obtaining relevant certifications. The organization sponsored classes in which each internal audit associate obtained a COSO certification. The CAE invites business teams to train auditors on what they do and reciprocates by having associates conduct awareness training in the business lines.
Quality Assurance and Improvement Program

Quality assurance and improvement programs (QAIPs) are required of internal audit activities by The IIA’s Standard 1300 series. To assure adherence with the series, it may be appropriate to perform a gap analysis, with each resulting gap becoming a topic for resolution. An example follows of how this method can be implemented.

Example: Depending on the size of the team, divide into groups and assign each group one of the identified gaps. Teams may consist of only two or three individuals, depending on the size of the internal audit function. After working together to brainstorm resolutions, convene a meeting of the entire department to share what each group is working on, what difficulties they may be having or finding, and encourage discussion among teams to review proposed solutions. After achieving consensus, resolutions may be implemented and monitored to ensure success. This type of exercise motivates team members and encourages individual commitment, which can be beneficial because these resolutions may impact daily tasks and routines of the whole team.

Larger internal audit functions and groups to which internal audit activities may be cosourced may have their own internal quality assurance activity. This is often a separate group that does not perform audits. Instead, this group works with the internal audit activity to review workpapers, ensure appropriate methodology is used, and other actions. Performance metrics for the internal audit activity are included in the scope of the QAIP. The CAE should ensure the function is performing self-assessments and evaluating its quality and performance as a departmental management strategy.

Internal audit activities are required to obtain an independent quality assessment review (QAR) as required by Standard 1312 – External Assessments every five years. Conducting periodic self-assessments and addressing issues that arise will help assure success of an external assessment.

Many financial services organizations have a separate professional practices function to aid in this pursuit. Because many financial institutions are large and employ a large audit group, they must manage their activities to promote consistency. The internal audit activity should have procedures for each type of engagement as well as documented practices for all other activities (risk assessment, follow up, independence/objectivity practices, etc.) to guide auditors in all locations.

An internal professional practices function would be the owner of the internal audit activity’s key methodology documentation, performing regular reviews of the activity’s work to ensure process, policies, and procedures are executed in conformance with that methodology. The professional practices function may also advise internal audit on methodology improvements and manage administrative functions of the audit department, such as budgets, metrics, strategy, improvement projects, and more.
## 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 1110 – Organizational Independence
- Standard 1111 – Direct Interaction with the Board
- Standard 1130 – Impairment to Independence or Objectivity
- Standard 1200 – Proficiency and Due Professional Care
- Standard 1230 – Continuing Professional Development
- Standard 1300 – Quality Assurance and Improvement Program
- Standard 1312 – External Assessments
- Standard 2000 – Managing the Internal Audit Activity
- Standard 2010 – Planning
- Standard 2050 – Coordination and Reliance
- Standard 2100 – Nature of Work
- Standard 2110 – Governance
- Standard 2120 – Risk Management
- Standard 2130 – Control
- Standard 2201 – Planning Considerations
- Standard 2400 – Communicating Results
- Standard 2410 – Criteria for Communicating
- Standard 2440 – Disseminating Results
- Standard 2450 – Overall Opinions
### Guidance


Appendix B. Glossary

Terms identified with an asterisk (*) are taken from the “Glossary” of The IIA’s International Professional Practices Framework®, 2017 edition.

Key terms in addition to select definitions are contained within this glossary. Some of these items may appear in the appendices:

**capital** — According to Basel III, consists of the sum of Tier 1 capital (going-concern capital) and Tier 2 Capital (gone-concern capital). For each category there is a single set of criteria that instruments are required to meet. Those requirements are described in Basel documentation.

**capital adequacy** — Enough capital to run an institution’s business while still absorbing the risk and volatility of its credit, market, and operational threats.

**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.

**control** — Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient action to provide reasonable assurance that objectives and goals will be achieved.

**control environment** — The attitude and actions of the board and management regarding the importance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:

- Integrity and ethical values.
- Management’s philosophy and operating style.
- Organizational structure.
- Assignment of authority and responsibility.
- Human resource policies and practices.
- Competence of personnel.

**key risk indicators** — Relevant metrics that provide useful insights about potential risks that may have an impact on the achievement of the organization's objectives.28

---

**leverage ratio** – According to Basel III, the capital measure (the numerator) divided by the exposure measure (the denominator), with this ratio expressed as a percentage: Leverage ratio = Capital measure / Exposure measure.

**liquidity** – The ability of a bank to fund increases in assets and meet obligations as they come due, without incurring unacceptable losses.29

**risk** – The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

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

**risk appetite statement** – The written articulation of the aggregate level and types of risk that a bank will accept or avoid to achieve its business objectives. It includes quantitative measures expressed relative to earnings, capital, risk measures, liquidity, and other relevant measures as appropriate. It should also include qualitative statements to address reputation and conduct risks as well as money laundering and unethical practices.30

**risk limit** – Specific quantitative measures or limits based on, for example, forward-looking assumptions that allocate the bank’s aggregate risk to business lines, legal entities as relevant, specific risk categories, concentrations and, as appropriate, other measures.19

**risk profile** – Point-in-time assessment of a bank’s gross risk exposures (i.e., before the application of any mitigants) or, as appropriate, net risk exposures (i.e., after taking into account mitigants) aggregated within and across each relevant risk category based on current or forward-looking assumptions.19

**risk management** – A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization’s objectives.

**risk strategy** – The organization’s plan to achieve its mission and vision and apply its core value.

---


Appendix C. Key Regulatory Principles for Financial Services Organizations

Anti-bribery and corruption – Bribery is defined as offering, giving, or receiving anything of value with the intention of inducing a person to act or to reward a person for having acted. Most countries have laws and regulations making the offering and acceptance of bribes and the associated corrupt behavior illegal. Anti-bribery and corruption policies should contain clauses describing the consequences for seeking to influence others, either directly or indirectly, by paying or receiving bribes or kickbacks, or by any other means that is considered unethical, illegal, or harmful to the organization’s reputation for honesty and integrity. Items of value not only include money but could also include gifts, meals, travel, political contributions, job offers, etc.31

Anti-money laundering – AML programs consist of a set of procedures, laws, and regulations designed to identify and prevent individuals and organized crime to disguise illegally gained income as legitimate income by sending money through the banking system. Some countries include prohibitions regarding terrorist financing in these laws as well. Financial services firms are required to have policies and procedures to prevent the misuse of technological developments for money laundering, and the financing of terrorism, through channels such as electronic money, ATMs, or other deposit networks and nonpersonal transactions. They are also required to establish monitoring processes for all transactions in such a way as to determine whether the client’s transaction is adjusted to the transactional and behavioral profiles established.32

Board and officer qualification requirements – According to the FDIC, “various laws governing the election of board members emphasize the importance of a director’s position. Statutory or regulatory qualifications usually include taking an oath of office, unencumbered ownership of a specific amount of the bank’s capital stock, and residential and citizenship requirements. Other laws also pertain to the qualification and selection of directors. There are, for example, certain restrictions, prohibitions, and penalties relating to: interlocking directorates; purchases of assets from or sales of assets to directors; commissions and gifts for procuring loans; and criminal activities such as embezzlement, abstraction, willful misapplication, making false entries, and improper political contributions. These qualifications and restrictions have no counterpart in general corporate law and both illustrate and emphasize the quasi-public nature of banking, the unique role of the bank director, and the grave responsibilities of that office.”33

**Capital requirements** – The Basel standard requires banks to maintain minimum capital levels to cover losses in proportion to the risky assets held on their balance sheets. Each bank is responsible for maintaining a minimum **capital adequacy** ratio and should consider capital in every decision made. Banks with a regional or global presence should ensure they consider the capital requirements established by local regulations in addition to the Basel II and III requirements, as they may differ.

**Consumer protection** – Most countries have a consumer protection regime that includes a variety of laws, regulations, and enforcement agencies. The goal of consumer protection legislation and enforcement is to allow consumers to make informed choices and be protected from harmful business practices. One common regulatory approach is to require financial service providers to give customers a Key Facts Statement (a simple, comparable summary of product features and costs) when they are shopping for a financial product. Survey results show that 81 jurisdictions ... report some requirements are in place for financial service providers to give consumers a Key Facts Statement.34

**Data privacy** – There are various regulations globally that regulate customer data. In the United States, the Gramm-Leach-Bliley Act passed in 1999 requires depository institutions to create privacy policies and make disclosures to consumers regarding how depository institutions gather and share sensitive member information including name, address, and social security numbers among other information.35 The General Data Protection Regulation (GDPR) was developed by the European Union Parliament in 2016 with a global enforcement date of May 2018. GDPR requires companies to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. The GDPR also regulates the exportation of personal data outside the EU. Companies will need the same level of protection for data such as an individual’s IP address or internet browser cookie data as they do for name, address, and social security number. Failure to comply carries the potential of stiff penalties.36

**Financial statement regulations** – International Financial Reporting Standards (IFRS) accounting standards are a set of principles companies follow when preparing and publishing their financial statements, providing a standardized way of describing the company’s financial performance. Publicly accountable companies (those listed on public stock exchanges) and financial institutions are legally required to publish their financial reports in accordance with agreed accounting standards.”37

---


Know Your Customer (KYC)/Customer Due Diligence (CDD) – Tied to anti-money laundering compliance, KYC rules govern organizations’ ability to verify the identification of a customer. CDD explores the viability or possible risks associated once the customer is identified including due diligence requirements for entities.

Sanctions – Economic sanctions are commercial and financial penalties applied by one or more countries against a targeted self-governing state, group, or individual. Economic sanctions may include various forms of trade barriers, tariffs, and restrictions on financial transactions. According to the Charter of the United Nations, only the UN Security Council has a mandate by the international community to apply sanctions (Article 41) that must be complied with by all UN member states (Article 2,2). They serve as the international community's most powerful peaceful means to prevent threats to international peace and security or to settle them. Sanctions do not include the use of military force. UN sanctions should not be confused with unilateral sanctions that are imposed by individual countries in furtherance of their strategic interests. Typically intended as strong economic coercion, measures applied under unilateral sanctions can range between coercive diplomatic efforts, economic warfare, or as preludes to war. Many financial institutions use the Office of Foreign Assets Control (OFAC) sanctions list provided by the United States. The EU also puts out a list of sanctioned countries, entities, and people. Many financial services firms also use a list published by the United Kingdom’s HM Treasury. The lists are large and inconsistent, making transaction screening a monumental task for larger institutions.

## Appendix D. Acronym Guide

These are acronyms commonly used in the financial services industry.

### Financial Services Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Organization, Institution, Government Actions, &amp; Common Phrases</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIFMD</td>
<td>Alternative Investment Fund Managers Directive</td>
</tr>
<tr>
<td>AML</td>
<td>Anti-money laundering</td>
</tr>
<tr>
<td>AMLD 4</td>
<td>Anti-Money Laundering Directive (fourth)</td>
</tr>
<tr>
<td>AMLD 5</td>
<td>Anti-Money Laundering Directive (fifth)</td>
</tr>
<tr>
<td>BCBS</td>
<td>Basel Committee of Banking Supervision</td>
</tr>
<tr>
<td>BHCA</td>
<td>Bank Holding Company Act of 1956</td>
</tr>
<tr>
<td>BIS</td>
<td>Bank for International Settlements</td>
</tr>
<tr>
<td>BRRD</td>
<td>Bank Recovery and Resolution Directive</td>
</tr>
<tr>
<td>BSA</td>
<td>U.S. Bank Secrecy Act of 1970</td>
</tr>
<tr>
<td>CAT</td>
<td>Cybersecurity Assessment Tool</td>
</tr>
<tr>
<td>CCP</td>
<td>Central Counterparties</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
</tr>
<tr>
<td>CFPB</td>
<td>Consumer Financial Protection Bureau</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>COBIT</td>
<td>Control Objectives for Information and Related Technologies</td>
</tr>
<tr>
<td>COREP</td>
<td>Common Reporting</td>
</tr>
<tr>
<td>COSO</td>
<td>Committee of Sponsoring Organizations of the Treadway Commission</td>
</tr>
<tr>
<td>CRD IV</td>
<td>Capital Requirements Directive IV</td>
</tr>
<tr>
<td>CRR</td>
<td>Capital Requirements Regulation</td>
</tr>
<tr>
<td>EBA</td>
<td>European Banking Authority</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>ECB</td>
<td>European Central Bank</td>
</tr>
<tr>
<td>EIOPA</td>
<td>European Insurance and Occupational Pensions Authority</td>
</tr>
<tr>
<td>ELTIF</td>
<td>European Long-term Investment Funds</td>
</tr>
<tr>
<td>EMIR</td>
<td>European Market Infrastructure Regulation</td>
</tr>
<tr>
<td>ESAs</td>
<td>European Supervisory Authorities</td>
</tr>
<tr>
<td>ESFS</td>
<td>European System of Financial Supervision</td>
</tr>
<tr>
<td>EMSA</td>
<td>European Securities and Market Authority</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EuSEF</td>
<td>European Social Entrepreneurship Funds</td>
</tr>
<tr>
<td>EuVECA</td>
<td>European Venture Capital Fund</td>
</tr>
<tr>
<td>FDIC</td>
<td>Federal Deposit Insurance Corporation</td>
</tr>
<tr>
<td>FDICIA</td>
<td>Federal Deposit Insurance Corporation Act of 1991</td>
</tr>
</tbody>
</table>
### Financial Services Acronyms (continued)

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Organization, Institution, Government Actions, &amp; Common Phrases</th>
</tr>
</thead>
<tbody>
<tr>
<td>FFEIC</td>
<td>Federal Financial Institution Examination Council</td>
</tr>
<tr>
<td>FinCEN</td>
<td>Financial Crimes Enforcement Network</td>
</tr>
<tr>
<td>FINRA</td>
<td>Financial Industry Regulatory Authority</td>
</tr>
<tr>
<td>FINREP</td>
<td>Financial reporting</td>
</tr>
<tr>
<td>FinTECH</td>
<td>Financial technology</td>
</tr>
<tr>
<td>FIO</td>
<td>Financial Insurance Office</td>
</tr>
<tr>
<td>FRB</td>
<td>Federal Reserve Board (also known as The Fed)</td>
</tr>
<tr>
<td>FSOC</td>
<td>Financial Stability Oversight Council</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>IAIS</td>
<td>International Association of Insurance Supervisors</td>
</tr>
<tr>
<td>ICAAP</td>
<td>Internal Capital Adequacy Assessment Process</td>
</tr>
<tr>
<td>IFRS</td>
<td>International Financial Reporting Standards</td>
</tr>
<tr>
<td>IOSCO</td>
<td>International Organization of Securities Commissions</td>
</tr>
<tr>
<td>IPPF</td>
<td>International Professional Practices Framework</td>
</tr>
<tr>
<td>KPIs</td>
<td>Key performance indicators</td>
</tr>
<tr>
<td>KRI s</td>
<td>Key risk indicators</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>MiFID II</td>
<td>Markets in Financial Instruments Directive</td>
</tr>
<tr>
<td>MiFIR</td>
<td>Markets in Financial Instruments Regulation</td>
</tr>
<tr>
<td>NACFU</td>
<td>National Association of Federally-Insured Credit Unions</td>
</tr>
<tr>
<td>NAIC</td>
<td>National Association of Insurance Commissioners</td>
</tr>
<tr>
<td>NBFI</td>
<td>Nonbank financial institutions</td>
</tr>
<tr>
<td>NCUA</td>
<td>National Credit Union Administration</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OCC</td>
<td>Office of the Comptroller of the Currency</td>
</tr>
<tr>
<td>OTC</td>
<td>Over-the-counter</td>
</tr>
<tr>
<td>OFAC</td>
<td>Office of Foreign Assets Control</td>
</tr>
<tr>
<td>OTF</td>
<td>Organised Trading Facility</td>
</tr>
<tr>
<td>PCAOB</td>
<td>Public Company Accounting Oversight Board</td>
</tr>
<tr>
<td>PEPs</td>
<td>Politically exposed persons</td>
</tr>
<tr>
<td>RCSA</td>
<td>Risk and control self-assessments</td>
</tr>
<tr>
<td>SEC</td>
<td>U.S. Securities and Exchange Commission</td>
</tr>
<tr>
<td>SRO</td>
<td>Self-regulatory organization</td>
</tr>
<tr>
<td>SSM</td>
<td>Single Supervisory Mechanism</td>
</tr>
<tr>
<td>SSM</td>
<td>Undertakings for Collective Investment in Transferable Securities</td>
</tr>
<tr>
<td>USA PATRIOT Act</td>
<td>Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001</td>
</tr>
</tbody>
</table>
Appendix E. The Role of Central Banks

A central bank, reserve bank, or monetary authority is the institution that manages the currency, money supply, and interest rates of a country or monetary union, and oversees their commercial banking system including payment and securities settlement systems. In the United States the Fed serves as the central bank; other central banks include the ECB, the Bank of England, and the People’s Bank of China. In some countries central banks and prudential/supervisory regulators are one entity, such as Saudi Arabia’s Saudi Arabian Monetary Authority (SAMA). Central banks in most developed nations are institutionally independent from political interference.

Central banks control the money supply in three ways:

- Requiring banks to hold reserves.
- Managing interest rates.
- Ensuring open market operations.

Banks are required to keep a certain percentage of all deposits in the bank, which is known as the “reserve requirement” or the “liquidity coverage ratio.” When reserve requirements rise, there is less money for banks to lend with the opposite also being true. Central banks are also in control of the “discount rate,” which is the rate the central bank charges banks that borrow from it. Lowering interest rates generally has the effect of increasing the money supply and adding liquidity to the economy. Central banks also participate in the market with government securities. Central banks will buy and sell treasury securities (in the United States, these are known as T-bills, T-notes, and T-bonds or collectively as “sovereign debt”). Central banks will decrease the money supply by selling treasury securities and increase the money supply by buying them.

The most common type of open market operation central banks engage in is an overnight repurchase agreement, or a "repo," which alters the money supply for a short time by temporarily buying or selling government securities.

Appendix F. Sample Risk Categories — Financial Institutions

This table lists some of the main risk areas internal auditors should consider when performing engagements in financial institutions. The list neither exhaustive nor meant to be used as an engagement work program or checklist.

Sample Risk Categories for Financial Institutions

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Risk Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy risk</td>
<td>Risk of not achieving the strategic objectives of the organization. For example: cost management; crisis management; governance; new business approvals and quality of management information; climate risk; fintech disruption; mergers and acquisitions; political instability.</td>
</tr>
<tr>
<td>Conduct and reputation</td>
<td>Risk of not complying with conduct requirements and effectively managing reputation risk. For example: affordability and vulnerable customers; anti-bribery; complaints; incentives; anti-money laundering; market abuse; sanctions; suitability; competition; lack of supervision.</td>
</tr>
<tr>
<td>Operational risk</td>
<td>Risk of not effectively managing people and processing. For example: end-user computing; operational risk management; outsourcing; performance management; training; contractual documentation; culture and behavior; data integrity; talent management.</td>
</tr>
<tr>
<td>IT</td>
<td>Risk of not effectively managing IT. For example: cybersecurity; data loss prevention; legacy systems; technology risk management; cloud computing; data protection; data retention; digital channels; resiliency; continuity.</td>
</tr>
<tr>
<td>Regulations and compliance</td>
<td>Risk of noncompliance with laws and regulations. For example: client assets/CASS regime; compliance risk management; transaction reporting; anti-money laundering directives; BCBS 239 – risk data aggregation; domestic and globally systemically important banks; European market infrastructure regulation; GDPR; MiFID II; payment services directive; recovery planning and resolution pack (also referred to as the Bank Recovery and Resolution Directive [BRRD]).</td>
</tr>
<tr>
<td>Geopolitical</td>
<td>Failure to adapt to changes to the environment and political landscape. For example: Brexit; macro economy; natural catastrophe; political interference; sanctions; terrorism; climate change.</td>
</tr>
<tr>
<td>Market risk</td>
<td>Risk of not effectively managing market risk. For example: market risk management; model risk; stress testing; fundamental review of the trading book; interest rate risk.</td>
</tr>
<tr>
<td>Credit risk and asset quality</td>
<td>Risk of not effectively managing credit risk. For example: collateral management; concentration; counterparty risk; credit risk management; credit sanctioning; model risk; provisioning; IFRS9: financial instrument; pricing.</td>
</tr>
<tr>
<td>Finance and tax risk</td>
<td>Failure to comply with tax regulations and manage tax effectively. For example: audit rotation; corporate criminal offense; funding costs; product pricing; transfer pricing; valuation; new accounting standards.</td>
</tr>
<tr>
<td>Capital and liquidity risk</td>
<td>Risk of not effectively managing capital and liquidity prudently. For example: stress testing; capital management; common reporting (COREP); financial reporting (FINREP); capital requirements directive IV (CRD IV); capital requirements regulation [CRR], and Basel III; internal capital adequacy assessment process (ICAAP); liquidity coverage ratio; liquidity management; Basel IV; leverage ratio.</td>
</tr>
</tbody>
</table>

Source: Adapted from PwC and BIS (The Bank for International Settlements) publications.
## Appendix G. Sample Risk Categories — Insurance Companies

This table lists some of the main risk areas internal auditors should consider when performing engagements in insurance companies. The list neither exhaustive nor meant to be used as an engagement work program or checklist.

### Sample Risk Categories for Insurance Companies

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Risk Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strategy risk</strong></td>
<td>Risk of not achieving the strategic objectives of the organization. For example: cost management; crisis management; governance; new business approvals and quality of management information; climate risk; mergers and acquisitions; political instability; governance; competition; operating model; takeover threat.</td>
</tr>
<tr>
<td><strong>Conduct and reputation</strong></td>
<td>Risk of not complying with conduct requirements and effectively managing reputation risk. For example: affordability and vulnerable customers; anti-bribery; complaints; incentives; anti-money laundering; market abuse; sanctions; suitability; competition; lack of supervision.</td>
</tr>
<tr>
<td><strong>Operational risk</strong></td>
<td>Risk of not effectively managing people and processing. For example: end-user computing; operational risk management; outsourcing; performance management; training; contractual documentation; culture and behavior; data integrity; talent management.</td>
</tr>
<tr>
<td><strong>IT</strong></td>
<td>Risk of not effectively managing IT: For example: complexity and obsolescence; fintech; technology resilience; digital disruption; third-party providers; optimizing investment; cybersecurity; data loss prevention; legacy systems; technology risk management; cloud computing; data protection; data retention; digital channels; resiliency; continuity.</td>
</tr>
<tr>
<td><strong>Regulations and compliance</strong></td>
<td>Risk of non-compliance with laws and regulation. For example: compliance risk management; anti-money laundering directives; BCBS 239 – risk data aggregation; GDPR; complaints; Solvency II asset rules; Solvency II reporting; IFRS4; MiFID II; standard formula review.</td>
</tr>
<tr>
<td><strong>Underwriting/reserving</strong></td>
<td>Failure to measure risk exposure and determine the premium that needs to charge given risk. For example: inadequate reserving; poor underwriting; underwriting strategy; emerging liability types; pricing agility.</td>
</tr>
<tr>
<td><strong>Geopolitical</strong></td>
<td>Failure to adapt to changes to the environment and political landscape. For example: Brexit; macro economy; natural catastrophe; political interference; sanctions; terrorism; climate change; life expectancy.</td>
</tr>
<tr>
<td><strong>Finance and tax risk</strong></td>
<td>Failure to comply with tax regulations and manage tax effectively. For example: audit rotation; corporate criminal offense; funding costs; product pricing; transfer pricing; valuation; new accounting standard.</td>
</tr>
<tr>
<td><strong>Market and customers</strong></td>
<td>Failure to adapt to changes in the market and customer behaviors. For example: distribution channels; annuity changes; brand erosion; customer behaviors; guaranteed products; shifting demographic; automation of society; litigation; long-tail liabilities; new entrants; innovation.</td>
</tr>
</tbody>
</table>

Source: Adapted from PwC and BIS (The Bank for International Settlements) publications.
Appendix H. References and Additional Reading

References


European Banking Authority. October 28, 2016. “Guidelines on internal governance (revised).”
https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-
governance-revised-/regulatory-activity/consultation-paper.


**Additional Reading**


Acknowledgements

Guidance Development Team

Mark Carawan, CIA, QIAL, United States (Chairman)
Keri Rogers, CIA, CRMA, United States (Team Lead)
Hazem Keshk, CIA, CRMA, Canada
Takuya Morita, CIA, Japan
Juergen Rohrmann, CIA, Germany
Stacey Schabel, CIA, United States

Global Guidance Contributors

Troy Damboise, CIA, CRMA, United States
Martin Falck-Hansen, CIA, Denmark
Audbjorg Fridgeirdottir, CIA, Iceland
Kivilcim Gündatti, Turkey
David Lin, CIA, CRMA, United States
Mariana Viegas, Portugal

IIA Global Standards and Guidance

Jeanette York, CCSA, Director (Project Lead)
Jim Pelletier, Vice President
Cassian Jae, Managing Director
Anne Mercer, CIA, CFSA, Director
Mike Padilla, CIA, Director
John Wszelaki, CIA, CRMA, Director
Shelli Browning, Technical Editor
Laurresa Nelson, Technical Editor

The IIA would like to thank the following oversight bodies for their support: Financial Services 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 200,000 members from more than 170 countries and territories. The association’s global headquarters are in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

DISCLAIMER
The IIA publishes this document for informational and educational purposes and, as such, is only intended to be used as a guide. This guidance material is not intended to provide definitive answers to specific individual circumstances. The IIA recommends that you always seek independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this guidance.

COPYRIGHT
Copyright © 2019 The Institute of Internal Auditors, Inc. All rights reserved. For permission to reproduce, please contact copyright@theiia.org.

August 2019