Connect › Support › Advance

The Institute of Internal Auditors Australia

White Paper

Auditing your entity's Compliance Framework

UPDATED 2020

Level 7, 133 Castlereagh Street, Sydney NSW 2000 | PO Box A2311, Sydney South NSW 1235
T +61 2 9267 9155 **F** +61 2 9264 9240 **E** enquiry@iia.org.au **www.iia.org.au**

Auditing your entity's Compliance Framework

Contents

Background

Purpose

An entity's compliance framework is designed to ensure that the entity achieves compliance with both externally and / or internally imposed requirements, and includes governance structures, programs, processes, systems, controls and procedures.

Background

Entities across all sectors - private, public and not-for-profit - need to comply with obligations associated with their establishing legislation or constitution, as well as broader legislative and regulatory obligations on how they operate, account and report.

Compliance continues to be a primary concern for the boards and senior management of most entities with reputation risk pushed to new levels as a consequence of the complexity and pace of legislative and regulatory change, coupled with an increase in regulatory scrutiny and enforcement.

A compliance framework is an important element in the governance of entities for:

- Preventing, identifying and responding to breaches of laws, regulations, codes or standards,
- Demonstrating a solid compliance regime to regulators,
- Promoting a culture of compliance, and
- Assisting the entity to be a good corporate citizen.

Regulators have the right to independently validate that an entity in their jurisdiction is compliant with legislation and regulations by conducting documentary and/or onsite reviews of the entity's policies, procedures, operations, activities, systems, premises and related information. The outcomes of the regulatory review might be reported publicly and/or to parliament.

Auditing compliance is one of the basic elements of internal auditing. Many issues identified during 'traditional' internal audits of an entity's policies, external reporting, safety, security, and environmental areas can relate to directly to compliance obligations. The outcomes of internal audit's compliance reviews are reported internally.

This paper does not cover instances where public sector entities are regulatory bodies that monitor compliance of other public, private, and not-for-profit entities.

Discussion

Issue

Audit committees are looking to internal audit to evaluate the overall compliance framework, not just micro-level 'bits and pieces' of compliance.

These evaluations are required to address identified criteria and are expected to cover all elements that reflect an effective compliance framework, including identification, risk assessment, awareness, monitoring, handling breaches, continuous improvement, the compliance register, reporting, and cross-border obligations.

History

The Chief Audit Executive (CAE) is directed by Standard 2010 of the International Professional Practices Framework (IPPF) to establish a risk-based plan to determine the priorities of internal audit, consistent with the entity's goals.

Auditing your entity's Compliance Framework

The strategic risks of entities often include compliance-related obligations for external reporting, safety, security and environment/sustainability (amongst others).

There are numerous layers of compliance obligations within entities.

- At the top level, there may be specific regulatory and licensing obligations that allow entities to operate in their discrete industries (from financial institutions through to energy, aviation, and rail providers and many in-between).
- Within different jurisdictions there may be requirements over privacy, freedom-of- information/transparency, taxation, anti-bribery and corruption.
- Service providers need to demonstrate compliance with contractual conditions.
- Motor vehicles in the entity's fleet will have compliance plates, and software licences underpin technology solutions.
- At an individual level, train drivers, security guards, forklift operators and so forth need to be personally licensed.

The international standard for compliance management AS/ISO19600[i] was rolled out in December 2014 and serves as a global standard and benchmark for compliance management programs.

According to the IPPF glossary, 'compliance' encompasses adherence to policies, plans, procedures, laws, regulations, contracts or other requirements.

The importance of auditing compliance has been emphasised in global studies. For instance:

- The results of a survey of audit committees reflected that over 70% of respondents believe internal audit's role should extend beyond financial reporting and controls, and one of the top four areas that respondents would like internal auditors to devote more time to is compliance/ regulation (45%).
- A separate study relating to audit committee focus areas identified compliance/regulatory as one of the top three ranked areas of focus (ranked behind strategic business risks and operational, but ranked ahead of information technology and risk management effectiveness).

Internal auditors are encouraged to adopt a structured risk based approach to auditing compliance. Internal audit is able to 'step-up' its compliance activities in line with its resourcing, objectives, and capability, as illustrated in Exhibit 1. Examples of these maturing compliance-focused activities are contained in Exhibit 3 and Exhibit 4.

Exhibit 1 – Stepping-up the maturity level of audit's compliance activities

Baseline Control	Maturity Level of Internal Audit Function		
IA Maturity	Foundation	Positioning for Success	Mature Practice
→	Potential Internal Audit Activities		
Auditing your entity's compliance framework	- Compliance activities (micro -level 'bits and pieces')	- Compliance committee meetings - Compliance governance	- Compliance framework (overall) - Central regulatory coordination

Discussion

Effective compliance programs ensure that entities are adhering to laws, regulations, standards, licences, policies, plans, procedures, contracts, guidelines, specifications or other requirements relevant to their business.

Some compliance obligations are mandatory (eg legislation, licences, permits) whereas others are voluntary (eg internal codes of conduct, industry codes).

An entity's reputation can be severely impacted when serious non-compliances occur and lead to prosecution, fines, or imprisonment of company officials. According to a global survey, approximately 87% of executives across the world see reputation risk as the most important strategic risk.

In 2018, the Commonwealth Bank reached agreement with the national regulator for a $700 million penalty relating to serious breaches of anti-money, laundering and counter-terrorism financing laws. [ii]

The core elements of a typical compliance framework are outlined in Exhibit 2.

Auditing your entity's Compliance Framework

Exhibit 2 - Core elements of a typical compliance framework

- Well-defined policies and procedures for identifying and updating compliance obligations, including escalation and/or reporting arrangements for breaches.
- Staff training and awareness programs, including arrangements to identify, create awareness, promote compliance, build a compliance culture, deliver associated training courses, and foster continuous improvement.
- Establishment and maintenance of a comprehensive compliance register to record relevant laws, regulations, standards, licenses, policies, plans, procedures, contracts, guidelines, specifications or other requirements.
- Risk assessment of compliance obligations, and identification of appropriate compliance strategies that reflect the impact on key business activities and drive a compliance culture.
- Clear allocation of responsibilities for ensuring that effective controls are embedded within key business processes to maintain compliance, monitor and record any changes, provide assurance and report exceptions, and maintain quality control.
- Well-established monitoring and reporting arrangements internally (including the board, CEO and responsible executives) with periodic sign-offs by management and external third party outsourced service providers as to compliance with obligations.
- A compliance governance structure that establishes oversight of compliance control activities including periodic compliance reporting to the audit committee and / or others charged with governance.
- Well-defined internal processes for identifying, assessing, rectifying and reporting potential or actual compliance incidents and breaches to the regulators.

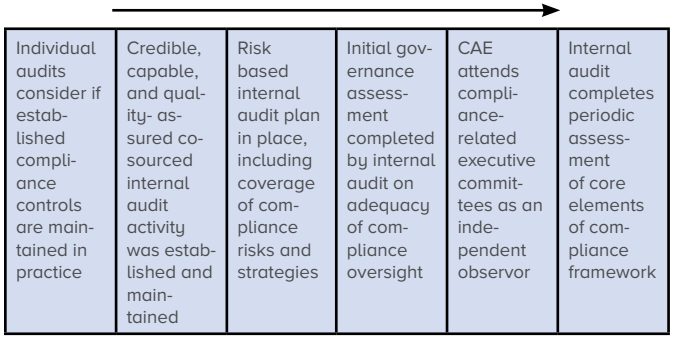
The availability of an up-to-date and complete compliance register is pivotal to all other elements of a structured compliance framework. Depending on the nature of the entity and its specific obligations, a compliance register might include information on laws, regulations, standards, licenses, policies, plans, procedures, contracts, guidelines, specifications or other requirements.

Effective monitoring mechanisms aimed at identifying changes to legislation, regulations, standards and other under-pinning content are critical to maintaining an up-to-date compliance register.

In framing internal audit's coverage of the compliance framework, the CAE will need to draw on available information gained from assurance maps (which will often identify the related 'lines of defence') and insights from stakeholder relationship management.

The following diagram (Exhibit 3) illustrates the various compliance-focused activities of an experienced CAE in a regulated industry.

Exhibit 3 – Example of a CAE's compliance focused activities



Internal audit's stakeholder relationship program is likely to include relevant compliance specialists, such as 'watchers' (person or entity conducting directed compliance assessments), 'advisors' (qualified person or entity providing advice on compliance achievement), 'assurers' (qualified person or entity providing expert advice and guidance to achieve assurance), and 'capability partners' (entity providing prescriptive direction and assistance that helps to achieve compliance and enhance capability).

Auditing your entity's Compliance Framework

Exhibit 4 – Practical example of an internal audit function's compliance activities

Features	Key Elements of Corporation	Related Internal Audit Activities
Maturity Level - Foundation		
Compliance activities	A high-level policy and procedures register (aligned where necessary to the compliance register) listed all of the corporation's significant policies and procedures, approval dates, related legislation/regulations, accountabilities, and review dates.	Individual audits in the approved internal audit plan considered whether established controls over compliance risks were operating in practice in line with established policies and procedures.
Maturity Level – Positioning for Success		
Internal audit capability	CAE developed a Strategic Competency Plan (using the IPPF Practice Guide - Creating a Competency Process in the Public Sector).	Internal audit staff were suitably trained and developed to fulfil the full ambit of their responsibilities under their charter and in the risk-based internal audit plan. Internal resources were complemented with specialist technical resources from a service provider firm secured by the CAE through a co-sourcing arrangement.
	As an example, the CAE identified a competency gap in respect to the absence of recognised 'safety auditor' capabilities with suitable national accreditation.	A senior internal auditor undertook the safety training course and achieved accreditation as a 'safety auditor'.
Governance	There were four board committees, all of which covered different elements of compliance – audit and risk; retail trading risk; remuneration / human resources; and transaction approval. There were five executive committees, each with a substantial compliance focus – major contract review; environmental; network capital governance; occupational health and safety; and financial services licence.	CAE attended key executive committee meetings occasionally as an observer, and participant. Each of the committee charters contained suitable wording to preserve audit independence.
Maturity Level – Mature		
Compliance framework	The entity had a compliance frame-work consistent with the features in Exhibit 2.	A periodic high-level internal audit assessed the compliance baseline, the register of compliance risks, and the overarching compliance framework to determine how well the core elements were operating in practice. Internal audit's periodic assessment of the organisation's culture included consideration of the compliance culture. These audits focussed on arrangements for undertaking compliance risk assessments, identifying compliance strategies, creating awareness, promoting compliance, fostering continuous improvement, establishing monitoring mechanisms, maintaining the compliance register, and producing meaningful compliance reporting.
Regulatory reviews	Regulators have the right to independently assure themselves that the entity is compliant with legislation and egulations related to their jurisdiction. They have the right to periodically conduct documentary and/or onsite reviews of the corporation's policies, procedures, operations, activities, systems, premises and related information. In some situations, the outcomes of the regulatory review might be reported to the parliament and/or the public.	To ensure a smooth and seamless regulatory review, the CAE was assigned responsibility by the CEO to be the entity's central coordination point for the regulator's review team. At the request of the audit committee, the CAE included the monitoring of significant regulatory recommendations in the internal audit activity's process for monitoring and reporting on the implementation of recommendations.

Five Action Steps

Five compliance-related activities to consider for your annual audit plan through an appropriately credible and capable internal audit cohort:

1. Include individual audits in the approved internal audit plan to consider discrete 'at risk' compliance activities at a micro level, including whether established controls over compliance risks are operating in practice in line with established policies and procedures. (A high-level register

Auditing your entity's Compliance Framework

should list all of the entity's policies and procedures, approval dates, related legislation/regulations, accountabilities, and review dates).

2. Facilitate the CAE or a senior delegate to periodically attend key board or executive compliance committee meetings as an observer, and report on significant insights to the audit committee. (Each of the compliance committee charters should contain suitable wording to preserve audit independence).
3. Complete a high-level assessment of compliance governance to ensure adequate coverage of the entity's respective licence conditions, legislative / regulatory obligations, and elements of its sustainability platform. Assess the entity's related risk management arrangements covering compliance obligations and reporting.
4. Conduct a periodic high-level internal audit to assess the compliance framework at a macro level, including:
   a. benchmarking against the international compliance standard AS/ISO 19600,
   b. assessing the soundness of compliance policy and its alignment to the entity's strategies and business/ statutory objectives,
   c. determining how well the core elements are embedded into business processes and operating in practice,
   d. evaluating the availability of appropriate resources to develop, maintain and improve the compliance program,
   e. assessing the effectiveness of compliance reporting to the board, audit committee and senior management, and
   f. forming an opinion on the overall culture of compliance.
5. Provide a central regulatory coordination point for the regulator's review team for any high risk or high profile regulatory reviews. Then monitor the implementation of significant regulatory recommendations in the internal audit activity's process for monitoring and reporting on the implementation of recommendations.

Conclusion

Summary and Options

The board, audit committee and senior management have responsibilities to champion, comply, risk-manage, and oversight a range of mandatory and voluntary compliance obligations.

Internal audit is well-placed to provide independent insights on the entity's compliance framework and culture, including how the entity:

- identifies, facilitates, creates awareness and promotes compliance;
- undertakes risk assessment and identifies strategies;
- establishes monitoring and assurance mechanisms;
- fosters continuous improvement;
- maintains a compliance register;
- handles compliance breaches (including escalation and/ or breach reporting); and
- provides internal and external compliance reporting.

Internal audit reviews of this nature help to minimise the risk of compliance failures and associated reputational risks, as well as the consequent potential impacts of fines, prosecution, complaints, and litigation for the entity and its senior officers, and potentially imprisonment for senior officers.

Conclusion

An effective compliance framework is a critical element of good governance. Given that almost nine out of ten executives across the world believe that reputation risk is the most important strategic risk, it is essential for the compliance framework to be factored into internal audit planning.

Bibliography and References

Bibliography

Coordination and Reliance: Developing an Assurance Map, IPPF Practice Guide, February 2018
Internal Audit Competency, IPPF Practice Guide, Creating an Internal Audit Competency Process in the Public Sector, February 2015
Standard on Assurance Engagements ASAE 3100, Compliance Engagements, Auditing and Assurance Standards Board, February 2017
Three Lines of Defence, IIA Position Paper - The Three Lines of Defense in Effective Risk Management and Control, January 2013
White Paper - Stakeholder Relationship Management, IIA-Australia, January 2020
White Paper - Reducing and Better Managing Red Tape, IIA-Australia, January 2020
Managing Culture - Good Practice Guide, IIA-Australia and Others, December 2017

Auditing your entity's Compliance Framework

References

[i] International compliance standard AS/ISO19600-2014

[ii] Australian Transaction Reports and Analysis Centre (AUSTRAC) Media Release, 5 June 2018 "AUSTRAC and CBA agree $700m penalty"; 1-2

Purpose of White Papers

A White Paper is an authoritative report or guide that informs readers concisely about a complex issue and presents the issuing body's philosophy on the matter. It is meant to help readers understand an issue, solve a problem, or make a decision.

Author's Biography

Written by: Bruce Turner AM
CRMA, CGAP, CISA, CFE, PFIIA, FFin, FIPA, FAIM, MAICD, JP

Bruce retired in 2012 after five years as Chief Internal Auditor at the Australian Taxation Office, one of the largest public sector entities in Australia. He previously held CAE roles at commercial service delivery entities - Integral Energy and StateRail.

Bruce has over thirty years practitioner and leadership experience in internal auditing, across the financial services (commercial, merchant and central banking), manufacturing, transport, energy, and government sectors. He has also held independent audit committee roles for over a decade in a range of entities, including construction, finance, services, health, environment, parklands, local government, infrastructure management, parliamentary services, central government and not-for-profit. He is a past chairman of the IIA Global Public Sector Committee.

Bruce remains active as an audit and risk committee chairman and company director. He was a member of the IIA-Australia Board from 2012 to 2018. Bruce is just the second professional internal auditor in Australia to receive Order of Australia honours. He was appointed a Member (AM) in the Queen's Birthday Honours of 2015 in recognition of his significant service to public administration through governance and risk management practices, and to the profession of internal auditing.

Bruce is a recipient of the 'Bob McDonald Award' from the IIA–Australia. This is the highest honour conferred on an Internal Auditor in Australia and recognised Bruce's significant contribution to the Internal Audit profession. He lives in Sydney, Australia.

This White Paper edited by:

Tim Kirby
MAppMgt, BCom, GradDipEnvMgt, CA, PFIIA, CIA, EMS-LA

About the Institute of Internal Auditors–Australia

The Institute of Internal Auditors (IIA) is the global professional association for Internal Auditors, with global headquarters in the USA and affiliated Institutes and Chapters throughout the world including Australia.

As the chief advocate of the Internal Audit profession, the IIA serves as the profession's international standard-setter, sole provider of globally accepted internal auditing certifications, and principal researcher and educator.

The IIA sets the bar for Internal Audit integrity and professionalism around the world with its 'International Professional Practices Framework' (IPPF), a collection of guidance that includes the 'International Standards for the Professional Practice of Internal Auditing' and the 'Code of Ethics'.

IIA–Australia ensures its members and the profession as a whole are well-represented with decision-makers and influencers, and is extensively represented on a number of global committees and prominent working groups in Australia and internationally.

The IIA was established in 1941 and now has more than 200,000 members from 190 countries with hundreds of local area Chapters. Generally, members work in internal auditing, risk management, governance, internal control, information technology audit, education, and security.