**Chapter 7**

**Compliance Auditing and Internal Auditing**

**Compliance Auditing**

**What Is a Compliance Audit?**

A compliance audit is an independent evaluation to ensure that an organization is following external laws, rules, and regulations or internal guidelines, such as corporate bylaws, controls, and policies and procedures. Compliance audits may also determine if an organization is conforming to an agreement, such as when an entity accepts government or other funding. Although most people are familiar with financial audits, such as those for public companies through the Sarbanes-Oxley Act (SOX) or individual or corporate tax audits through the Internal Revenue Service (IRS), compliance audits are not merely financial. Audits may also review [IT and other security issues](https://www.smartsheet.com/understanding-it-compliance" \t "_blank), compliance with HR laws, quality management systems, and other areas. Compliance is one leg in the tripod of GRC, which stands for governance, risk, and compliance.

Compliance is important for many reasons. Aside from signifying levels of professional standards, like the ISO 9000, ISO 14000, and other guidelines, noncompliance with regulatory guidelines may bring sanctions and penalties. Penalties for noncompliance with federal regulations, such as Sarbanes-Oxley, are specified through the Federal Sentencing Guidelines Act and apply fines based on a formula that calculates the most recent offenses and determines whether the organization employs a compliance officer who communicates regulatory needs to the organization.

Boards of directors are also often accountable for operations and need to see audit reports. If a regulatory agency does investigate, proof of a compliance program is important to show that the organization has controls and other mechanisms that can detect deficiencies and even illegal activity.

Depending on the circumstances, the audit may be conducted by an employee, such as an internal auditor, a certified public accountant, a third-party auditor, or a government auditor. In many circumstances, auditors may seek the expert advice of outside specialists, such as lawyers.

Audits provide recommendations on ways to make improvements or corrective actions and to prevent future deficiencies or nonconformities. Audits review for effectiveness to determine the number of compliant versus non-compliant processes. Audits also help organizations to stay in compliance with frequently changing federal regulations. In addition, audits identify areas of risk for noncompliance within the organization and report these appraisals to management and the appropriate regulatory entity as applicable.

Essentially, a compliance audit asks if you are doing what you said you would do.

**What Is the Purpose of a Compliance Audit?**

A compliance audit gauges how well an organization adheres to rules and regulations, standards, and even internal bylaws and codes of conduct. Part of an audit may also review the effectiveness of an organization’s internal controls. Different departments may use multiple types of audits. For example, accounting may use internal, compliance, and operational audits. Audits may be required by different levels of government.

* **Internal Audits:** Although some conflate the notions of compliance audits and internal audits (often using personnel from an internal audit team), these two types of audits represent separate approaches. Internal audits ensure that an organization follows process, procedures, and guidelines — in other words, its own internal controls. This type of audit also guarantees that these controls prevent and detect errors or illegal acts. A compliance audit, on the other hand, ensures that the organization is fulfilling outside obligations, such as rules and regulations, agreements, or standards. Internal audits may be operational, IT, financial, or regulatory, but are conducted using formal audit methodologies appropriate to the subject area. Internal audits are not available to regulators and tend not to be made public, although sometimes social compliance audit results are released as part of a company’s rebranding. Internal audits may be conducted prior to an outside compliance audit to ensure that the organization is following standards.
* **Compliance Audits:** Compliance audits differ from internal audits in that they are outward-facing, ensuring that the company complies with regulations or codes of conduct. Ideally however, both internal and compliance audit functions share the same language (and even software) to make sure that reviews are comprehensive.
* **Operational Audits:** Operational audits determine how efficient and effective different departments and activities are and whether these areas function in alignment with the mission and intent of the organization.

**Who Participates in Compliance Audits?**

Depending on the type of audit, many departments in one firm may be subject to an audit, from finance to payroll to production to IT to sales. Auditors may interview employees throughout the hierarchy. However, particular emphasis is placed on managers. AU 801, for example, holds management responsible for understanding compliance requirements, ensuring that adequate controls are in place to sustain compliance, regularly checking to certify that compliance is met, and then implementing corrective actions to mitigate deficiencies or nonconformities. With SOX compliance audits, CEOs and CFOs must attest to the integrity of controls and the accuracy of financial reports. PCI compliance audits may interview CIOs, CTOs, and IT admins to determine how users are tracked and to review the audit trail from IT event log and change management software.

How Are Compliance Audits Conducted?

An auditor may work alone or in collaboration with other functions, like human resources, IT, legal and security. An auditor must have access to records. In addition, auditing questionnaires and formal interviews provide a richer picture of the organization’s situation. Depending on the area of audit, statistical or judgemental sampling may be used. Statistical sampling provides an existing model of conformities and outliers. Judgemental testing may not allow for generalization to a wider sample, but the types and numbers of nonconformities and outliers may indicate risk areas.

Whether the audit is internal or for compliance, management must understand that they are ultimately responsible for creating internal controls and ensuring compliance. In general, most sources agree that all levels of management are responsible for creating appropriate policies and procedures and monitoring them to verify adherence.

Here are the steps in a compliance audit:

1. The organization contacts the auditor. The auditor and the organization decide if the auditor’s expertise is a good fit.
2. The auditing firm sends a proposal either to the company or to the attorney for instances where compliance audits should invoke client-attorney privilege.
3. At a preliminary meeting, the auditor describes the guidelines for the audit and what is required. The auditor may provide auditing checklists, so the client can prepare.
4. For a small organization, the auditor may work by phone. The organization completes audit questionnaires and supplies the auditor with needed documents. The auditor may work on site to view documents, walk through work spaces, study infrastructure and security features, and interview management and employees.
5. The report should be delivered within a relatively short time. In the case of social compliance audits of facilities, the turnaround may be as fast as the next day. At the  final meeting, the auditor presents and discusses the report and makes recommendations to address any areas of risk. Whether working under a regulatory deadline or not, organizations should generally remedy any deficiencies within 120 days to ensure that they complete corrective actions and don’t simply shelve them until the next audit. However, auditing firms usually also offer follow-up support to help organizations remedy any risks or deficiencies. Auditors then verify that measures have been met.

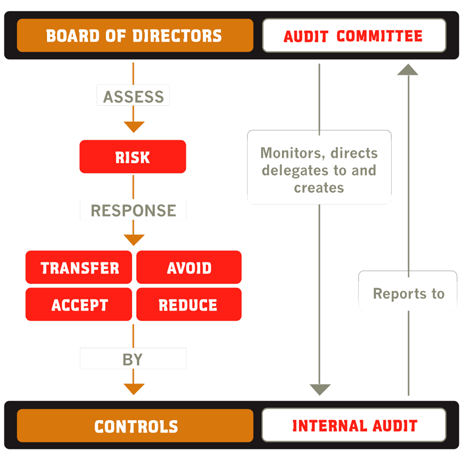
### Internal audit

#### Internal audit – the control of controls – can feature as a key part of the corporate governance framework of an organisation, and can be viewed as a high level control in response to risk or by considering the detailed work required of internal audit.

### Role of internal audit in corporate governance

Internal auditors are perfectly placed to assist management in the assessment of risks and internal controls. This task may include (Internal audit can help the directors to achieve these objectives)

* Have a defined process for the review of effectiveness of internal control
* Review regular reports on internal control
* Consider key risks and how they have been managed
* Check the adequacy of action taken to remedy weaknesses and incidents
* Consider the adequacy of monitoring
* Conduct an annual assessment of risks and the effectiveness of internal control
* Make a statement on this process in the annual report



The internal audit function

### Decision to have an internal audit department

At each stage of the process the board faces a number of decisions: setting the firm’s risk appetite, assessing risks, and then choosing which risks accepting, transferring, reducing or avoiding. If a risk reduction response is adopted, the board must then design an appropriate set of controls, possibly including establishing an internal audit function. In most jurisdictions, especially where corporate governance is principles-based, IA departments are not required by statute or regulation, but are considered best practice. However, as soon as the task of reviewing the company’s internal control and risk management system reaches even a reasonably low level of complexity, the audit committee will find that they need to delegate this work. This is clearly a sensitive task, as it involves investigating and discovering how effective strategic and operational controls have been. It requires a skilled team of internal auditors, who can act independently and who will report back objectively to the audit committee. As you can imagine, it would be unusual for a company of any size (not just a listed company) to be able to dispense with the services of an IA department, which is why an explanation is required when there are no internal auditors.

One obvious issue to consider is what other factors apart from size would indicate that an IA department might be required. It is not hard to come up with some of the relevant factors by reflecting that a company needs a control when risk needs reducing. So factors giving rise to increased risk, such as complex or highly regulated transactions, might suggest the need for the IA control to be deployed. You would, therefore, expect banks to have IA departments since some of the transactions they handle are complex (accounting for financial instruments) and they operate in a regulated industry.

In some regulated industries it is mandatory to have an internal audit department, but even where this is not the case there may be close scrutiny of the company by the regulatory authority, which can apply significant sanctions such as the removal of operating licences. When a compliance failing (including timely reporting to the regulator) might mean that the company cannot operate at all, the case for an internal audit department becomes overwhelming. Companies in regulated industries may also need the information from internal audit to use in their reports and submissions to regulators and, so, reliable and accurate IA information is also needed to ensure the adequacy of this reporting.

Arising out of uncertainty, risk is fundamental to change. Any significant changes faced by the business will therefore inevitably create risk, and the organisation should consider its need for internal audit. The changes highlighted in the Turnbull report are changes in key risks and changes in the internal organisational structure.

Reporting to the audit committee

Let’s return to the idea that the internal audit department is carrying out the delegated work of the audit committee. This is a fruitful area to explore because it explains some of the characteristics of effective (and ineffective) IA. The audit committee is made up of independent non-executive directors (NEDs). This isn’t the place to explore the concept of independence in detail, but independence is central to an effective IA department. The work of IA becomes meaningless if it is compromised by management influence. Achieving independence is difficult, and made more so because internal auditors are usually employees of the company.

The audit committee is one of the vital parts of the committee structure of sound corporate governance. Its role in overseeing IA is important because it is the audit committee that ensures that the IA function actually supports the strategic objectives of the company (and doesn’t act purely on its own initiative). In addition, though, it is likely that the audit committee – at the strategic level – will not only provide the IA function with the authority it needs to scrutinise the internal controls, but also to ensure that its work is actually supporting and providing the compliance needs of the company. It is part of ensuring the hierarchical congruence or consistency necessary in sound governance and strategic management.

Members of the IA function may encounter ethical threats (such as familiarity, self-review, independence threats, and so on). An accountant working as an internal auditor, for example, may be unwilling to criticise the CFO if he believes the CFO has an influence on his future prospects with the company. Someone coming into IA from an operational position could also be exposed to a self-review threat. Even where external contractors are used to carry out the IA function, they are acting on behalf of management. To avoid this, and other ethical threats, internal audit work is one of the jobs expressly forbidden to external auditors under the terms of the Sarbanes–Oxley Act in the US, indicating just how valuable a characteristic independence is for all auditors (other codes have similar provisions).

There are some inherent limitations in what an IA department can achieve. Although corporate scandals sometimes arise from failings in operational level controls, there are also examples where the problem is a failure of strategic level controls, either arising from management override of controls (as at Enron) or through poor strategic level decisions (as at some of the banks that required state support in the 2008 banking crisis). Even in companies where excellent procedures are put in place to assess operational level controls, it is hard to imagine how IA can fully monitor strategic controls. It would be very hard to design a corporate governance structure in which even the most independent IA department had a mechanism to do much more than check that procedures have been followed at board level. The board ultimately has to be responsible for the proper working of strategic level controls. This is also illustrative of the way IA fits in to overall corporate governance. The corporate governance big picture has to be addressed if IA is going to be effective. A domineering CEO cannot be countered by the existence of an IA department. Indeed, interference in the work of internal audit would indicate broader corporate governance problems.

### Day-to-day internal audit

### Day-to-day out tasks of internal auditors include

* value for money audits
* information technology audits
* best value audits
* financial audits
* Operational audits.

One of the key differences between internal and external audit is that the scope of internal audit work in an unregulated industry is determined by the company (specifically by the audit committee) while the scope of the external auditors’ work is determined by the fact that they are undertaking a statutory audit, a legal requirement. IA will mean something different in each organisation. In one company, the ‘internal audit’ department might only carry out quality control checks, while in another it is a sophisticated team of specialists with different expertise that reflect the risks faced by that organization, including the regulatory requirements placed upon it.

Whether the IA department is carrying out a review of the process of designing systems, or a review of the operation of controls within those systems, will depend on the current concerns of the organization. In an exam it would be wise to tailor the suggestions made for IA to the concerns hinted at in the scenario. For example, in a highly regulated business where compliance failures are a significant risk, monitoring compliance might be a key task assigned to IA. If safeguarding assets is a key concern you could discuss how IA might be involved in a review of the safeguarding of assets. You may have noted that the last two suggestions both relate to the Turnbull statements about a sound system of internal controls. Any of those could be related to the work of internal audit – for example, IA might need to review the implementation of corporate objectives.

**Internal Auditor and Social Responsibility**

IA is a resource that could be deployed to monitor how effective a company’s corporate social responsibility (CSR) policies are. This could mean monitoring how well the policies have been implemented or it could mean IA monitoring how well CSR policies and wider corporate objectives are aligned with each other. Schemes like the European Union’s Eco-Management and Audit Scheme (EMAS) provide an example of an instance where specific monitoring of targets (by IA) is an externally imposed requirement on a company. ISO 14000, another environmental standard, also explicitly requires internal audits and reports to management.

To sum up, internal audit is the control of controls. It can feature in SBL as a key part of the corporate governance framework of an organization, and it can be viewed through the lens of risk management as a high level control in response to risk or by considering the detailed work required of IA. Finally, as a key component of the control system, it is important to maintain the integrity of internal audit and, from this perspective; issues of professional ethics and characteristics such as independence come into play.

Internal audit plays a key role in corporate governance, providing objective assurance on control and risk management.

.

As stated one of the objectives of internal audit is risk assessment and management as companies face risks arising from their operational activities. Examples include

* Risk the company will go bankrupt
* Risks arising from regulations and law
* Risks arising from publicity

.

Risk awareness and management should be the role of everyone in the organization. The extended role of internal audit with regard to risk is the monitoring of integrated risk management within a company, and the reporting of results to the Board to enable them to report to shareholders.

Internal auditor relationships

Internal auditors have relationships with the following people.

* Management: by whom they are employed and may report to
* Audit committee: to whom they report
* External auditors: who may make use of their work

Internal auditors and risk management

The issue of the Turnbull guidance and internal audit's role in relation to risk management was touched on briefly above. Directors need to ensure three steps are taken in their business:

* Identify risks
* Control risks
* Monitor risks

It is not internal audit's primary role to manage risk in a company. It is the responsibility of the directors, usually delegated to individual managers in various departments.

The risks are identified and assessed, and a policy approach is taken in respect of each of them. To recap, this policy is usually one of four:

* Accept risk (if it is low impact and likelihood)
* Reduce risk (by setting up a system of internal control)
* Avoid risk (by not entering a market, accepting contract etc)
* Transfer risk (by taking out insurance)
* Give advice on the best design of systems and monitor their operation
* Be involved in a process that continually improves internal control systems
* Provide assurance on systems set up in each department

The involvement of internal audit as a monitoring unit will help to ensure that the process of risk identification and management in a business is a continual process rather than a one-off exercise.