Chartered Institute of Internal Auditors

21 September 2020

Compliance

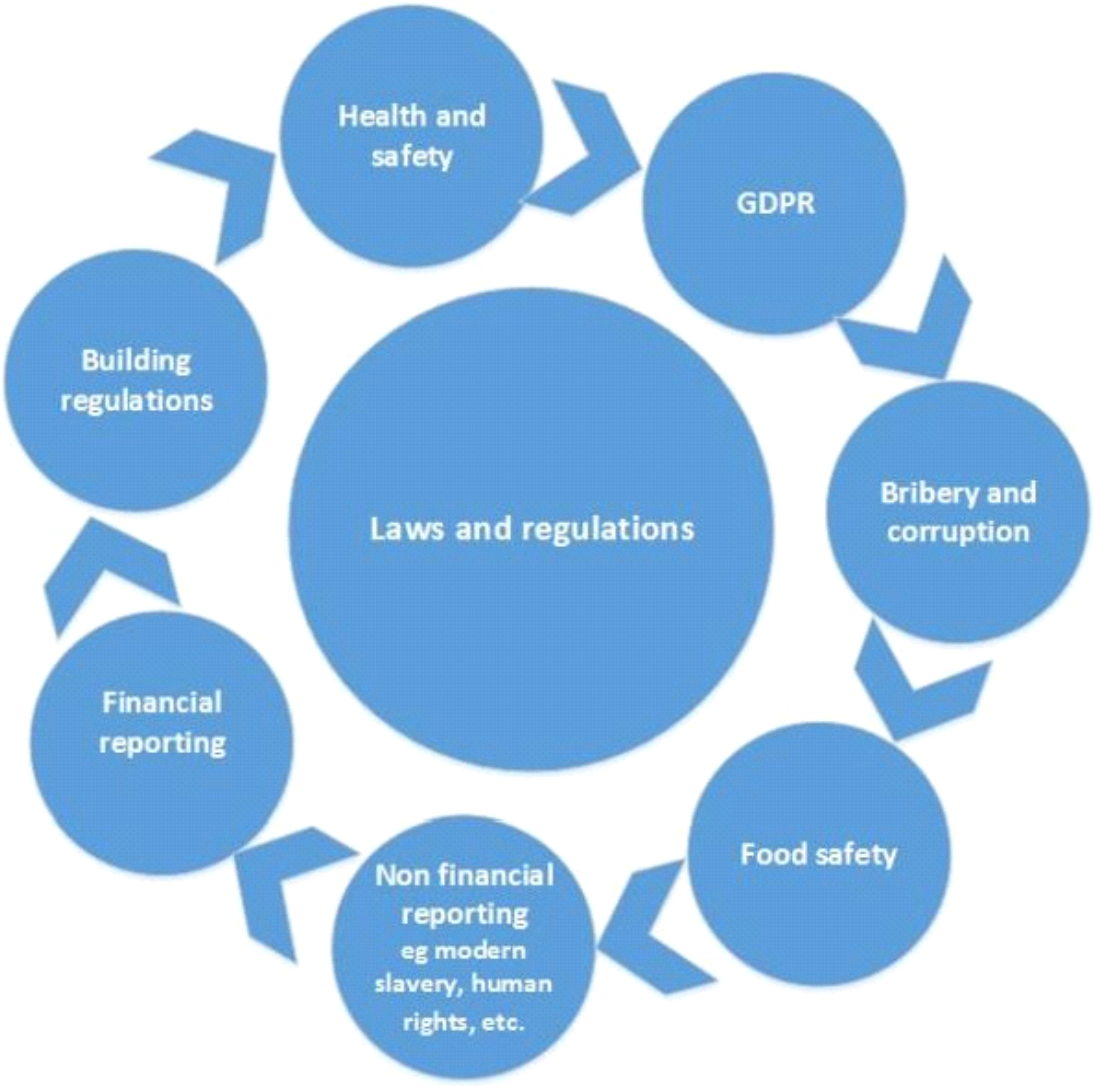
Chartered Institute of Internal Auditors

What is compliance?

Every organisation, no matter how small or large, in every sector must follow directives set by external bodies or through law.

Coupled with the external requirements, organisations will also have their own ways of working which they want employees to follow.

Compliance, put simply, is following the internal and external rules in place.



Examples of laws and regulations

Why is it important?

There are often penalties attached to non-compliance which can be financial or as severe as temporarily shutting the business down, plus the accompanying reputational damage, loss of customers, and for a public company, impact to the share price. For external laws and regulations compliance, not following the rules can have consequences as serious as injury and death.

The UK Corporate Governance Code 2018 talks about ‘long-term sustainable success’ and establishing ‘a framework of prudent and effective controls, which enable risk to be assessed and managed’. Establishing suitable compliance frameworks within an organisation is one of the building blocks to help ensure this can be achieved.

Whose responsibility is it?

All employees within an organisation are responsible for compliance, however, senior management of the organisation are ultimately responsible for ensuring employees know what they need to comply with, and this can be, and usually is, delegated.

A sustainable organisation will assign roles and responsibilities for compliance to fit with the size and appetite of the organisation. Examples of such roles might be a head of health and safety, a data protection officer, a regulatory risk team or a property compliance officer. In a smaller organisation, compliance responsibilities might be managed alongside a ‘day job’, for example there might be a director of corporate services who manages several operational workstreams, compliance being one.

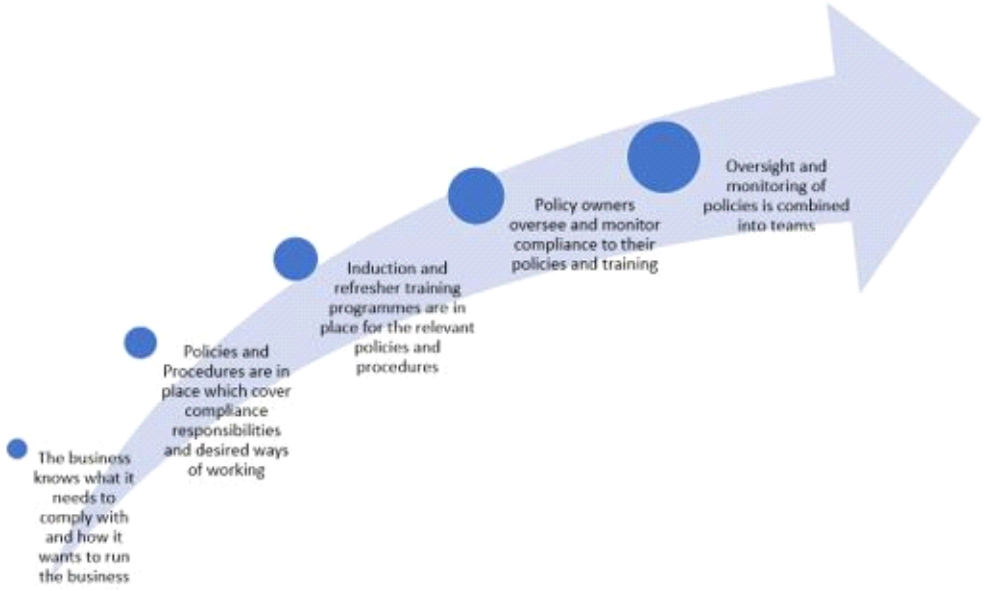
What is our role as internal auditors?

Compliance risks should form part of the audit universe and should be included as part of the risk assessment process feeding into the audit planning cycle.

Internal audit teams may have cyclical compliance audits as well as risk-based audits. Some compliance audits are mandatory as per external regulations, for example in the aviation industry, financial services and healthcare.

The approach to providing assurance over compliance risk will depend on the organisation’s maturity. For the most mature organisations, internal audit’s role is to provide assurance over the effectiveness and reliability of the work of compliance functions, in accordance with the three lines of defence model below, and for the least mature it will be to help ensure the organisation knows what it needs to comply with.

Our role is to remember that one size does not fit all and look to provide assurance to the board that the desired outcomes are being achieved and compliance risk is being managed effectively.



The path of compliance maturity

Our recommendations must take the maturity and appetite of the organisation into account and guide the organisation on its compliance journey.

A compliance framework model

Strategy

The board has appointed a compliance risk owner, set the risk appetite and has defined the desired culture.

Structure/roles and responsibilities

Roles and responsibilities for compliance have been assigned and aligned to the desired organisation structure eg that reports into the executive team and has direct access to the board.

Staff in specialist roles have the desired skills and experience and/or access to external resources with sufficient knowledge and experience of regulatory compliance.

Horizon scanning takes place to identify any external changes and the impact on the organisation.

Policies and procedures

The required policies and procedures are in place, communicated and accessible, regularly reviewed, aligned with regulations and legislation and authorised by senior executives.

You should expect policies and procedures to cover the compliance risks relevant to the organisation. Examples of policies and procedures you might expect in any organisation are:

- health and safety, including the procedures to comply with the policy such as risk assessments, and
- data protection and all associated policies to comply with GDPR, including operational procedures for elements such as data privacy impact assessments, subject access requests and rights to erasure.

There is a whistleblowing/speak up procedure that is publicised to enable confidential reporting of potential issues/incidents such as regulatory breaches.

Training

Staff and other company representatives receive induction and refresher training on the elements of compliance relevant to their job.

Oversight/monitoring

Compliance checking procedures are in place, and appropriate governance committees/meetings are in place to provide oversight.

Enforcement of compliance standards, policies and procedures is through appropriate consistent disciplinary procedures.

Management information/reporting

Compliance reporting highlights trends and areas of concern, with continuous improvement actions captured and tracked.

Where breaches are identified, lessons are learnt and all reasonable steps are taken to prevent future similar occurrences, including a review of controls and making any appropriate changes to the compliance programme.

Auditing compliance functions

The most mature organisations will have compliance functions, usually in the second line of defence although they can also be in the first line or both, particularly in financial services where there are more rigorous regulatory demands.

When auditing compliance functions, the desired outcome is to be able to confirm to the board and the audit committee that the work of the compliance function(s) can be relied upon as a source of assurance.

Internal audit should expect the compliance function itself to have the same sorts of controls as described in the compliance framework model above.

Whilst not bound by the same standards (the International Professional Practices Framework) as internal audit, the internal auditor should expect a methodology to be in place to drive consistency and quality within the compliance team's work. Many of the controls you would find in an internal audit function such as an annual planning and action tracking process should also be in place.

In order to be able to rely on the work of the compliance function, the internal audit team should be able to re-perform any compliance reviews and reach the same conclusion. To do this, the internal auditor should expect compliance review work to be properly documented, with clear evidence of sample checking results.

Integrated assurance

As first, second and third lines of defence mature together, the goal should be to move towards integrated assurance whereby the work of other assurance functions has been validated and can be relied upon, which allows internal audit to mature the internal audit plan to move away from compliance reviews and focus on other strategic risks to the organisation. Internal audit's role becomes more focussed on providing periodic assurance over the 1st and 2nd line management of compliance risk.

The work of the three lines of defence should become co-ordinated, and an assurance map can be implemented to provide clarity over where all the sources of assurance are within an organisation and whether they can be relied upon.

Further reading

Standards

2050 Coordination and reliance

Implementation guidance

2050 Coordination and reliance

Supplemental guidance

Coordination and reliance - developing an assurance map
Reliance by internal audit on other assurance providers

Guidance

Coordination of assurance services
Working with stakeholders