The Institute of Internal Auditors Australia

Compliance Program

Updated 2022

What is compliance?

Compliance – Fulfillment of an obligation, while non-compliance is non-fulfilment of an obligation. Obligations may be externally imposed or may be a voluntary undertaking.

Compliance program – A formal structured approach to assuring obligations are met.

Organisations that aim to be successful in the long-term need to maintain a culture of integrity and compliance and to consider the needs and expectations of stakeholders. Integrity and compliance are the basis for a successful and sustainable organisation.

In response to increasing regulatory pressures, well-publicised compliance breaches and a trend toward greater transparency, compliance and ethics programs have grown exponentially.

Effective, organisation-wide compliance management enables an organisation to demonstrate its commitment to complying with laws and regulations, together with standards of good governance, ethics and community expectations.
Source: ISO 37301:2021 'Compliance management systems – Requirements with guidance for use'

An organisation's approach to compliance is usually shaped by the leadership applying ethical and community standards.

Embedding compliance depends on leadership and clear values, as well as measures to promote compliant behaviour. Otherwise, there is risk of non-compliance which may impair business activities, attract penalties and damage an organisation's reputation.

Integrity is part of culture and compliance builds upon that cultural value. Organisations are increasingly convinced that by embedding compliance activities they can safeguard integrity and minimise non-compliance with obligations.

Integrity and effective compliance are key elements of good, diligent management. Compliance also contributes to socially responsible behaviour of organisations.

How is compliance used?

Compliance is a key component of an organisation's overall governance framework.

Compliance can vary according to the type of industry or business activity.

Every organisation should be seeking:

- Legal compliance – with laws, regulations, statutory obligations and contracts. This is a mandatory obligation that is imposed.
- Policy compliance – with organisation policies. This is a voluntary obligation that is self-imposed.

Compliance is actively used in high-value, high-transaction environments such as financial services where a compliance unit reporting to top management is mandated in many jurisdictions. This philosophy extends to other high-value, high-transaction environments in government where there may be fiduciary risk, but also reputational risk from political and community expectations where government programs may run ineffectively or be subject to fraud risk.

Getting started

Most compliance obligations will be built into the day-to-day organisation procedures so everyday operation of the organisation will be compliant.

A 'getting started checklist' would include:

- Identify compliance obligations.
- Build or check systems, policies and procedures for consistency with obligations.
- Assure systems, policies and procedures are being followed.
- Undertake regular checks and reviews to assess compliance with systems, policies and procedures.
- Ensure early detection of process weaknesses and timely corrective action is taken.
- Identify, analyse and address any instances of non-fulfilment of obligations (non-compliance).
- Continuously strengthen systems, policies and procedures.
- Ensure policies and procedures are reviewed and updated periodically in line with pre-determined review periods.

What happens with compliance now?

While some organisations have a strong compliance approach, especially in jurisdictions where there are mandatory compliance requirements, many organisations

seem to take a fairly laid-back approach to compliance and do not have a formal compliance program.

When a chief executive officer is asked:

- 'How do we know our organisation is complying with all relevant laws, regulations, statutory obligations and contracts?'
- 'How do we know our organisation is complying with its policies?'

the answer is likely to be that management look after this. But when pressed on such things as:

- Evidence to support compliance assumptions.
- Independent validation of management compliance assertions.

the result will often be there is nothing substantive or evidence-based the chief executive officer can hold up as evidence or validation there is in fact compliance.

What are compliance benefits?

A targeted compliance program has the following benefits:

- Provides greater insight into compliance issues.
- Focuses on the most critical and complex processes.
- Ensure consistency in approach and adherence to legal obligations, policies and procedures.
- Identifies short-term and long-term needs to improve compliance capabilities.
- Manages risks more cost-effectively and efficiently.
- Operates consistently across international, national and regional levels.
- Establishes regular checks and reviews to validate compliance.
- Takes the lead on compliance management.
- Establishes a process for continuous strengthening of systems and processes.
- Provides early detection of weaknesses and timely corrective action to be taken.
- Provides integrated compliance analysis and reporting to senior management and the audit committee.
- Gives confidence to stakeholders the organisation is serious about complying with its obligations.

Is there a compliance standard?

ISO 37301:2021 'Compliance management systems – Requirements with guidance for use'. It replaced the previous compliance standard ISO 19600:2015 'Compliance management systems – Guidelines'.

Steps to compliance

Legal compliance

Definition – Fulfillment of obligations to comply with laws, regulations, statutory obligations and contracts.

Objectives

- Meet legal compliance obligations.
- Comply with requirements of laws, regulations, statutory obligations and contracts.
- Assure no instances of non-fulfilment of legal obligations (non-compliance).

Steps to establish

- Develop legal compliance policy and methodology.
- Assign resources for legal compliance.
- Research legal compliance obligations and compliance risks.
- Develop legal compliance register.
- Prepare legal compliance work plan.
- Build legal compliance program awareness.
- Roll-out legal compliance activities.
- Implement legal compliance monitoring and reporting.
- Commission periodic independent reviews on the legal compliance program.

Policy compliance

Definition – Fulfillment of obligations to comply with mandated policies, procedures, systems and methods.

Objectives

- Assure policies, procedures, systems and methods are followed.
- Undertake regular checks and reviews to assess compliance with systems, policies and procedures.
- Continuously strengthen systems, policies and procedures.
- Early detection of weaknesses and timely corrective action taken.

Steps to establish

- Develop policy compliance model and methodology.
- Assign resources for policy and system compliance.
- Develop targeted policy and system compliance strategies.
- Prepare policy compliance work plan, including check and review schedule.
- Develop policy compliance activities and reporting.
- Build policy compliance program awareness.
- Roll-out policy compliance activities and reporting.
- Commence regular checks and reviews to assess policy compliance.
- Implement policy compliance monitoring and reporting.
- Commission periodic independent reviews of the policy compliance program.

Conclusion

If you cannot answer the following questions by producing evidence-based and validated data:

- *'How do we know our organisation is complying with all relevant laws, regulations, statutory obligations and contracts?'*
- *'How do we know our organisation is complying with its policies?'*

then you really do not know whether you are complying with your obligations.

Acknowledgement

This factsheet has drawn upon information contained in ISO 37301:2021 'Compliance management systems – Requirements with guidance for use'

Useful references

ISO 37301:2021 'Compliance management systems – Requirements with guidance for use'

The 20 Critical Questions Series 'What Directors should ask about Compliance', IIA-Australia

White Paper 'Auditing Your Entity's Compliance Frameworks', IIA-Australia

White Paper 'GORC – New and Improved GRC with Added O, IIA-Australia

White Paper 'The Obligation Hierarchy, IIA-Australia

White Paper 'The ORC Model for Compliance Management', IIA-Australia

White Paper 'The Obligations Register and the Rumsfeld Matrix', IIA-Australia