

Governance and Structures

- Directors are accountable to stakeholders for safeguarding the organisation's information. They must establish effective arrangements so they can ensure information risk obligations are being adequately fulfilled.
- All levels of management need to have a clear understanding of the part that they play in information risk management. The information risk governance framework and information risk policy must be documented.
- Governance is a continual active part of a director's role. The governance framework is not something that can be documented and then put to one side.

The Purpose of an Information Risk Governance Framework

Though directors are ultimately accountable for the protection of the organisation's information, the entire organisation needs to work together to ensure protection obligations are fulfilled. Directors need to put in place the arrangements and processes by which responsibilities are distributed and significant information risk decisions are to be made and reviewed. All officers and managers of an organisation need to understand these processes and to be clear as to the part they play in fulfilling the organisation's information protection obligations. The governance framework describes the way these arrangements and processes work and needs to be documented.

Objectives for an Information Risk Governance Framework

The organisation's information risk governance framework should:

- Provide balance: enable the organisation to move forward and achieve its goals whilst ensuring that information risk issues receive appropriate attention;
- Set the direction: provide the vehicle by which the directors articulate the organisation's information risk objectives and set the risk management principles and policies to be followed by all staff;
- Maintain the course: enable the directors, through effective reporting arrangements, to verify that directives are being followed and information risks are being appropriately mitigated.

What Should be Included in an Information Risk Governance Framework

Good governance is based on clarity about the organisation's information obligations and on having the right arrangements in place to ensure those obligations are fulfilled. Each organisation will develop its own model and structures but some aspects should be common to all. The following are essential requirements for a governance framework.

- **Scope.** Identify the nature of the organisation's information assets and the stakeholders (specific and general) who have an interest in how the organisation uses and safeguards those assets.
- **Ownership.** Identify who owns the different types of information the organisation uses.

Some information will be owned by customers, or by the person about whom the information relates, or by third parties providing the information as part of fulfilling a service. The organisation is then the custodian of that information, not the owner, and custodianship implies its own obligations, accountabilities and responsibilities.

- **Risk tolerance.** Document the organisation's information risk objectives, and its tolerance for information risk. This will dictate the priority afforded to information risk mitigation in comparison with other types of risk.
- **Setting direction.** Describe the means by which the directors set the information risk principles and policy to be followed by all staff.

- **Allocation of accountability.** Specify how accountability for the use and protection of information is allocated. Usually, risk management accountability will follow operational accountability, i.e. those in control of the organisation's operations are accountable both for the uses made of information within those operations and for the safeguarding of that information whilst it is in their care.

Each person, once they have received appropriate training, should be held accountable for the actions they as individuals perform on information, and for not using information illegally.

- **Delegation of authority.** Describe the processes by which decisions affecting the use and protection of information are to be made, and are to be monitored and reviewed. For large organisations, these arrangements may include the setting up of an Information Risk Management Committee reporting to the Board, or regional or function-specific IRM committees with more limited authority.
- **Allocation of responsibility.** Define the responsibilities needed to ensure information is properly safeguarded. Lack of clarity regarding the allocation of responsibilities is one of the most common causes of governance failures.

Organisations that establish internal functions to discharge key responsibilities must ensure those functions have appropriate levels of skill and expertise, and that they maintain the interests of all stakeholders in balance.

- **Reporting and assurance.** Define the reporting and assurance arrangements by which the directors ensure that their mandates and policies are being followed correctly and information control and protection obligations are being fulfilled.

