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 which 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 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 policy 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 should be held accountable for the actions they as individuals perform on information, and for not using information illegally.
- **Delegated 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 reasons for governance failures.

  Organisations which establish internal functions to discharge key responsibilities must ensure those functions have appropriate levels of skill and expertise, and 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.

Creating a Strong Information Handling Culture

- **Having a strong information handling culture is critical to the success of Information Risk Management. Without it, policies will fail and much effort will be wasted.**
- **The culture must permeate throughout the organisation and must inform every person's approach to how they perform their daily tasks, regardless of seniority.**
- **Culture is set by the leaders at the top of the organisation. If they do not demonstrate the necessity of good information handling, the staff beneath them will not believe in it.**
- **The goal is to develop in all staff a good level of Information Risk common sense so staff can, in their day-to-day work, make sensible information risk decisions themselves.**

Why Culture is Important

Information is used throughout the organisation and by every person in one way or another according to their responsibilities and daily tasks. It is through these daily tasks that information is put at risk by poor decisions or poor practices. The damage which can be caused by poor staff behaviours can be serious. Inaccurate recording of data, careless talk, excessive distribution of documents, failing to apply security procedures, can all create dangers for an organisation, blight reputation, reduce customer loyalty, and expose a company to litigation.

A sound appreciation of information risk, the forms it takes and the ways it should be mitigated, must permeate throughout the organisation and must form a part of every person's approach to how they perform their daily tasks. This is achieved by developing a good information handling culture which makes the control and protection of information a routine part of every activity. Without a strong culture, Information Risk policies will be more likely to fail and much risk mitigation effort will be wasted.

What Does Having a Strong Culture Mean?

Having a strong culture means each and every person, at whatever level they serve within the organisation, having a clear shared sense of "how we do things within this organisation". It means everyone understanding the importance information plays in the success of the organisation, the need for information to be safeguarded and assured throughout its lifecycle, plus having a clear sense of what this means for how they personally perform their day-to-day tasks.

How Culture is Set

The culture is set by the organisation's leaders (directors, executives, senior management) and the messages they project to staff. If the leaders project an image of having no particular concern for the value of information and no particularly concern for how information is used or safeguarded, then staff throughout the organisation will follow suit.

It is not sufficient for the leaders of the organisation just to acknowledge in words that information is valuable and that risks must be mitigated. They must portray it through their decisions and actions. Staff develop their understanding of the organisation's culture more by what they see than by what they hear. Consider, for example:

- How often do staff see information stewardship discussed at Board meetings?
- How often and in what light do they see information handling being the subject of internal communications?
- Do they see information failures and breaches being dealt with transparently and openly?

How to Assess the Culture's Strength

Key signs which indicate the strength of an organisation's information handling culture include:

- Everyone, from the top of the organisation to the bottom, will know that good information handling is a part of everyone's job – including theirs.
- Senior staff will understand they are bound by the same rules and requirements that they would expect junior staff to be bound by. They will not override Information Risk decisions for reasons of convenience, or allow senior colleagues to do so.
- All staff will be able to answer general questions about their information protection responsibilities. Staff with specific risk management responsibilities will have received the training and information they need to enable them to fulfil those responsibilities.
- Everyone within the organisation will be able to make sensible information risk decisions for themselves. This will include knowing the limits of their subject matter competence and when to defer to others or refer to policies or standards for specific guidance.

How to Strengthen the Culture

A good culture and good information risk common sense starts with an effective programme of information risk awareness and education for all staff, plus tailored training for those with specific risk mitigation responsibilities.

This should be supported by feedback mechanisms to help guide staff towards better behaviour. Staff should be shown both good and bad examples of information handling in practice so they learn to recognise bad practice when they see it and build up their knowledge of what constitutes good practice.

Feedback also demonstrates that senior management attaches importance to its information protection principles and takes care to ensure they are applied effectively.

It should be made easy for staff to take personal responsibility for ensuring the effectiveness of information handling practices. They should be encouraged to question any instruction they have been given if it seems inappropriate on information risk grounds. They should know they are expected to intervene in or, if serious, report, any instances they see of inappropriate behaviour, and should be confident they will be supported no matter how the issue is resolved.