

Programmes, Methodologies and Standards

- Information risk mitigation programmes plus their supporting documentation must be clear and comprehensible to all users. They should be “user friendly” rather than “written for lawyers”.
- All material must be consistent across the organisation. This gives confidence that effort expended in one place is not being undermined by weaknesses introduced elsewhere.
- Recognised national and international standards are valuable reference sources. Even if formal certification against a standard is not a requirement, good value can still be obtained by adopting the standard’s ideas or practices.

Risk Mitigation Programmes

Each organisation will establish its own programmes for how it wishes to implement and maintain its information risk plan. These programmes will reflect the organisation’s risk tolerance, and should be aligned with corporate governance needs and the operational needs of users. They focus attention on those aspects of risk mitigation the organisation considers most important to its success, and enable the development of coherent structured risk mitigation approaches all staff can understand and support.

It is important that risk mitigation programmes, plus the policies, processes, guidance and standards supporting them, are communicated to all users and are clear and comprehensible to all users. For these to be effective, users need to be able to interpret these documents correctly and reliably. They should be designed to be “user friendly” rather than “written for lawyers”.

Risk Mitigation Methodologies and Standards

Methodologies set out how the organisation assesses its information risks, addresses its control and protection needs, and measures the results. For all but the smallest organisations, following a risk-based approach implies there will be different people assessing and addressing risk at different times in different locations. All parts of the organisation are interconnected so a weakness in the risk mitigation arrangements in one part of the organisation can put the whole organisation at risk. Methodologies and standards should be consistent throughout the organisation to provide confidence that risk mitigation efforts expended in one place are not being undermined by weaknesses allowed elsewhere. Consistent methodologies help to ensure consistent practice across the organisation and enhance interoperability and versatility.

Key Methodologies

Though each organisation will develop its own methodologies, some methodologies are key to the success of an effective information risk mitigation programme and each organisation should consider employing them.

- **Information Classification.** Information assets (technical and non-technical) are classified according to the magnitude of the impact a failure or compromise could have on the organisation. This enables critical assets to be identified as such so they can receive priority risk mitigation attention.
- **Risk Ownership.** Each information asset assigned a significant classification should be assigned a Risk Owner, a named individual or role within the organisation who is accountable for safeguarding that information asset and who has the authority to make decisions that affect the protection of that asset.
- **Risk Assessment.** The methodology should set out to identify reliably and with only a small amount of effort those situations in which risks have the potential to become significant, so the bulk of the risk assessment effort can then be applied where it is most needed.
- **Control Baselines.** Baselines ensure all assets receive consistent protection, providing cover for any situations in which a risk assessment might have underestimated a source of risk. Baselines are supplemented by customised risk mitigation designs for those information assets that are considered to be high risk, allowing high risk assets to be protected adequately without having to raise the baseline for all assets.
- **Checking and Testing.** Check independently that all information assets are protected in line with their risk assessment. For baseline protected assets, this can take the form of a periodic audit to check that the correct baseline is being applied in full. For higher risk assets, this might also include periodic testing to ensure the on-going effectiveness of key controls.
- **Monitoring.** Monitoring turns the lights on. Without it, the organisation would be in the dark with respect to whether it is exposed to a high or low level of threats and whether it is

experiencing information failures and breaches continually or hardly ever. Monitoring includes technical monitoring (of threats, weakness, and actions performed) and reporting by staff (of any threats or inappropriate actions they notice as they go about their daily tasks).

- **Incident Management.** Information failures and security breaches will occur from time to time. Organisations need to be able to detect incidents reliably and invoke an appropriate response promptly to minimise the harm that can result.

Developing Standards

An organisation can take guidance from recognised external standards but must expect to develop its own standards according to its own particular needs. In some instances, formal compliance with external standards might be required by an external regulator or might add specific value, for example as a way to meet customer or client concerns. In most other situations, worthwhile benefits can be obtained by adopting the standard without necessarily progressing to formal certification.

The main national and international standards relevant to Information Risk Mitigation include:

- ISO 9000 series – the ISO standard for quality management systems;
- ISO 27000 series (formerly BS 7799 and ISO 17799) – best practice recommendations for information security management systems;
- BSI DISC PD0008 – the British standard relating to the legal admissibility and evidential weight of information stored electronically;
- BS 25999 – the British standard for Business Continuity Planning;
- BS 25777 (formerly PAS 77) – a code of practice for IT Service Continuity Management;
- COBIT – internationally recognised guidance for IT Governance and Control.

