

Information Risk Mitigation

PROCESS

- Risk mitigation should be commensurate with the level of the risk – it will not necessarily need to remove all the risk.
- Keep risk mitigation simple so it is manageable and can be communicated readily to all staff.
- Plan and Do, but also make sure you Check and Act.
- Monitor and report on the on-going level of information failures and security breaches so the effectiveness of the protection being achieved can be assessed.

What is Information Risk Mitigation?

Information Risk Mitigation is the collection of processes that together ensures information risks are adequately reduced to an acceptable level. It includes the methods for identifying and assessing risks plus the methods for determining which controls need to be applied, for checking that those controls have been applied, and then for tracking the actual level of protection being achieved.

Risk-Based Approach

Every organisation has the dual objective of ensuring it applies an adequate level of risk mitigation in those situations where the risks are highest and ensuring it does not over-engineer solutions where the risks are minimal. For this reason, it is necessary to take a risk-based approach so that mitigation efforts are applied in proportion to the level of risk being addressed.

Defence in Depth

Risk is driven by uncertainty and risk mitigation is an inexact science. In addition, risk can arise from any of a countless number of sources and in any of a countless number of ways. Organisations should not expect to identify all their specific risks in detail, or assess their risks with precision.

Risks should be assessed in terms of the general level of harm that could reasonably be caused if information were to fail or be compromised. Mitigation should take the form of a wide range of overlapping controls, some of which work to reduce the likelihood of an information failure and some of which work to reduce the amount of harm a failure can cause. A range of controls covering both aspects helps to ensure that, whatever the form in which a threat materialises, there is a good chance one or more controls will be in place to mitigate the risk.

Good Practice Standards

Experience has shown that some controls are effective across a broad range of common risks. These are codified in what are known as Good Practices. Applying Good Practices across the organisation provides a pragmatic approach to risk mitigation that everyone within the organisation can understand and apply. Organisations will still need the flexibility to recognise and respond to situations where the risks are particularly significant or unusual. Good Practice control baselines need to be supplemented by customised controls applied in specific higher-risk circumstances.

Plan, Do, Check, Act

The adoption of a risk-based approach implies there will always be some level of risk that senior management would rather accept and tolerate than reduce further. In addition, controls are often applied under constraints of expertise, cost, effort and practicability, with controls sometimes being deployed in phases or as opportunity allows. Hence, the Plan aspects of risk assessment and the Do aspects of controls selection need to be supported by Check and Act aspects that check that required controls have been implemented adequately and action plans are in place to address control shortfalls. Escalation paths need to be defined for situations where the information risk owner and internal subject matter experts cannot agree on the protections required or on the timescales on which protections should be implemented.

Monitor and Review Protection Failures

No matter how diligently an organisation strives to ensure it has all appropriate controls in place, protection failures will arise from time to time. Organisations need to monitor for protection failures so they can deal with incidents as they

arise and contain the harm those incidents cause. Organisations also need to keep the number and nature of their incidents under review so they can learn the available lessons. Incidents provide a rare objective indicator of the real level of risk being experienced, and should be used to benchmark and adjust the risk mitigation controls in place.

Review and Report on Aggregate Provision

The organisation's objectives, its internal structures and systems, and the environment in which it operates, are evolving continually. As a result, the risks the organisation faces will be changing continually. A sound system of information risk mitigation will include the regular re-evaluation of the nature and extent of the risks to which the organisation is exposed, plus periodic adjustment to ensure the organisation continues to steer the line between allowing risks to grow out of hand and constraining operational effectiveness.

Information risk mitigation processes normally deal with each risk situation in isolation. The regular review of risks should include a reckoning to ensure the aggregate risk position does not grow out of proportion to expectations or to the organisation's risk tolerance.

The aggregate risk position is part of the regular reports to the Board under the Information Risk Governance framework. The Board will need to understand and accept the organisation's aggregate information risk position as part of satisfying itself that the organisation's information protection obligations are being adequately fulfilled.

