# Information Risk Management Approach

- **The organisation's Information Risk Management approach must be aligned with organisational goals.**
- **It must be understood and supported across the senior management of the organisation.**
- **Regular reporting to management is essential to demonstrate the value provided by effective Information Risk Management practices.**

## Positioning Information Risk Management within the Organisation

Effective information risk management programmes contribute directly to successful organisational outcomes and sustainability. These programmes must be provided with sufficient top management support and resources to ensure they are effective and provide value for money.

This goal is achieved by ensuring information risk management programmes are seen by executive and operational management as positive contributors to the success of the organisation and not just as another cost of doing business. Senior management should be shown that the approved programmes are providing them with enhanced organisational outcomes as well as cost-efficient risk management. Reporting can demonstrate this using a combination of metrics, benchmarks, scorecards and dashboards.

## Key Objectives

Information Risk Management programmes will need to be tailored to suit the individual organisation and designed explicitly to help it achieve its particular goals and objectives. They should be designed to:

- Directly and demonstrably support each of the organisation's stated strategic objectives (e.g. breed client confidence especially amongst the organisation's target client sectors), not just to reduce the aggregate impact of information failures and security breaches.
- Support senior management in fulfilling each of their risk management responsibilities.
- Support and assist executive management in making key information risk-affecting decisions.
- Provide feedback mechanisms by which management can measure the success of the decisions they and others make.

**PROCESS >** Establish and oversee information risk management practices which will help to make the organisation successful.

## Information Risk Management Reporting

Those responsible for leading the Information Risk Management programme should demonstrate that, in return for the support and funding provided, their programmes are providing effective information risk management which meets strategic needs. Risk Management reporting should enable the Board to verify that the Information Risk Governance arrangements are being applied diligently and that the end results are positive for the organisation as intended.

Regular reporting to the Board should cover:

- The balance between the level of risk the organisation faces, its tolerance of risk, and the level of effort being expended providing risk management, plus the gap between its current and target risk positions.
- How well key information risk management arrangements are functioning (measured in a way that the Board finds helpful).
- The progress being made against agreed information risk priorities. These will be the key priorities proposed by the programme leaders and agreed by the Board.
- The effectiveness of the risk management arrangements at achieving the desired ends, i.e. the successes being achieved and failures being experienced.

There can be situations where reporting to external stakeholders is either a requirement or is advantageous. In some situations, e.g. regulators, the reporting requirements will be set by the stakeholder. In other situations, e.g. customers, external communities, the reporting requirements should be determined by the Board according to how such reporting helps to strengthen the reputation of the organisation, enhance goodwill, encourage customer loyalty or support social responsibility.

## Assess the Strength of the Organisation's Approach

Identifying gaps in the way information risk is managed will show the strengths and weaknesses of the organisation's Information Risk Management approach. For example:

- Is responsibility for Information Risk Management clearly owned at Board level?
- Do senior management afford information risk the priority it deserves given the organisation's sensitivity to information risk?
- Are there documented Information Risk Management programmes which have been signed off by the Board?
- Are key Information Risk Management milestones normally achieved or is the programme continually struggling against a lack of support and funding?
- Is on-going awareness, education and training in place for all staff?

# Information Risk Mitigation

- **Risk mitigation should be commensurate with the level of the risk – it does not need to remove 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 a tolerable 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 which 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 which 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 continually evolving. As a result, the risks the organisation faces are continually changing. 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 reporting 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.

# 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 significantly classified information asset 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 little 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, covering 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 assessed as high risk, allowing high risk assets to be protected adequately without having to raise the baseline for all assets.

- **Checking and Testing.** Independently check that all information assets are protected in line with their risk assessment. For baseline-protected assets, this can be in the style 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 serves as the means to switch on the light. Without it, the organisation will 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, good value 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

Business Relationship