Why Information Risk is a Board-level Issue

- **Every organisation, whether public or private sector, handles information. This information must be appropriately controlled and protected against the threats, non-technical as well as technical, that can affect it.**
- **Compromised information can cause enormous damage to an organisation's operations and reputation. Information not appropriately protected can lead to serious compliance and legal failures.**
- **Good Information Risk Management helps an organisation get the best out of its information and to move forward and develop, confident that its risks are under control.**

What is Information Risk?

Information, in whatever form, is a valuable asset to any organisation. It is the basis on which strategic decisions are made and daily tasks are performed. Executives, staff, customers and stakeholders all rely on that information being accurate and complete.

There are many ways in which good information can be undermined. Corrupted or compromised information can cause a wide range of problems, from those which are simply annoying to those which could have a major impact on an organisation's future.

Information Risk encompasses all the challenges that result from an organisation's need to control and protect its information.

Why Information Risk is an Important Issue

The value of information as an asset extends beyond its volume. Where it is the basis on which executives, customers and investors make critical decisions, it is essential for that information to be accurate and complete. An organisation's success depends on the trust and goodwill of staff, suppliers, customers, and the public at large, so it is essential that all its information is properly managed, controlled and protected.

Why it is a Board-level Issue

Because of the magnitude of the damage that can be caused. Poorly managed information can lead to a material impact on an organisation's future.

Because information risks can affect an organisation in every way: financially, operationally, they can damage reputation, they can lead to regulatory sanctions.

Because how an organisation addresses information risk will need to reflect ever changing demands and the complex dynamics of the business environment. Strategic direction is required.

And finally because directors have accountability in law for how their organisation protects its information.

Only the directors collectively have the necessary vision, organisational understanding, and authority required to address this issue.

Should All Information Risks be Mitigated?

Information risk has potentially critical consequences and it should be approached in much the same way as other critical areas of risk.

The key is to determine the level of risk faced by your organisation, and the level of risk the Board is prepared to tolerate.

Gauging the impact if a significant risk were realised is essential. How harmful would it be if, somewhere within your organisation, critical information were:

- Used improperly by staff to facilitate fraud?
- Not available to those who need it when they need it, or not known to be available by those intended to benefit from it?
- Inaccurate or incorrect?
- Lost or disclosed to competitors or the media?

Understanding your organisation's ability to tolerate risk is also important. How much would progress be impaired, interrupted or blown off course if:

- A member of staff was found to have abused the private information of a customer?
- A product release was badly designed and a customer suffered a major fraud?
- Data and analysis you had been building up over the past ten months was stolen, by person or persons unknown?
- Your organisation developed a reputation, unfairly or otherwise, for losing information?
- Current information in a database used every day got overwritten by a month-old back-up?

If you allow your organisation to carry too much information risk:

- You could be forced to apply expensive tactical solutions to a problem which could have been addressed more efficiently with foresight.
- You could be forced to apologise to your customer base or to provide undertakings to the ICO.
- Your organisation could become the example everyone else uses to justify their internal risk management investments.

If the consequences of information risks materialising would be more than the Board is prepared to accept, then you need to take steps to mitigate the risks. The purpose of information risk management is to reduce your organisation's information risks to a tolerable level and to keep them under control in a manageable way, rather than try to eliminate them entirely.

Realising the Benefits

- **An organisation's mission and goals are more likely to be achieved if information risks are properly managed. Good Information Risk Management underpins a wide range of organisational goals and can provide benefits everywhere.**
- **Good Information Risk Management is an enabler. It does not exist to stifle initiative or restrict operational freedom.**
- **Organisations need to find a balance between risk mitigation and enabling the organisation to release the benefits its information can deliver.**

What Benefits?

Good information risk management enhances stakeholder value. The benefits will vary between organisations, but can be expected to include:

Operational efficiency	Accurate, up to date information reduces wasted effort and costs.
Greater agility	Dependable information allows for faster decision making.
Improved manageability	Risk mitigation makes the organisation more manageable.
Exploitation of new opportunities	Information risk mitigation supports expansion into new areas of business with more confidence.
Customer retention	Customer experience is improved in a measurable way.
Strengthen the brand	Help your organisation be seen as a safe partner, contributing to success rather than introducing another source of risk.
Cost-efficient compliance	Satisfy multiple compliance needs within a single framework.
Maximise return on capital	Reduce the capital required to deal with unplanned turns of events so that it can be used for more productive purposes.

Why Impose any Restrictions?

Uncontrolled or unconstrained exploitation of information can introduce dangers of its own. To realise the benefits from information whilst avoiding the dangers, organisations must understand and control their information risks.

- Exploitation of information for particular business initiatives needs to take account of the organisation's wider interests or responsibilities.
- There might be applicable external constraints on the purposes for which information can be used, and an organisation might be the custodian and not the owner of the information it wants to exploit.
- Short-term benefits need to be weighed appropriately against possible long term effects on the organisation and its customers.
- Specialist attention might be needed to ensure non-contravention of legislation or regulatory regimes, often differing country-by-country (see *Regulation and Legislation*).

Control Need Not be a Straightjacket

Good information risk mitigation supports organisational strategies and tactical agility rather than limiting them.

- Understanding its information risks can help ensure an organisation takes the right path towards its goals and objectives and avoids taking dead-end paths or hitting major bumps in the road.
- Monitoring and mitigating its information risks helps an organisation to anticipate what might happen and increases the ability of the organisation to react and respond well to what does happen.

Find the Right Path

Each organisation needs to find the path which is right for them and to understand their particular reasons for wanting to manage their information risks. These reasons will be a mixture of risk mitigation, the expected benefits, and the need for compliance, the themes developed in the three ORGANISATION guides. Like the legs of a tripod, all of these themes need to be in balance.

All decision makers within the organisation, and that includes everyone from executive management to the shop floor, need to know what is expected of them. They need to know where they fit within the larger governance picture (see *Governance and Structures*) and the effects their decisions have on the organisation's exposure to information risks (see *Creating a Strong information Handling Culture*).

On behalf of your organisation, you will want to find the optimum level of effort which maximises net value and builds success. The level of effort and resource your organisation puts to information risk mitigation should reflect the degree to which success in achieving organisational goals and objectives depends on reducing information risks (see *Information Risk Management Approach*), plus on the nature and level of the actual risks your organisation faces at any time (see *Information Risk Mitigation*). Decide on your priorities and set your programmes, methodologies and standards to ensure you achieve your risk management milestones (see *Programmes, Methodologies and Standards*).

Regulation and Legislation

- **Directors must ensure that they know and understand all legislation and sector regulation relating to information risk, and that their knowledge remains up to date.**
- **Directors are personally accountable, and can be held personally liable, for non-compliance.**
- **The tide is running towards an ever greater focus on the control of information.**

This Guide is intended to serve as a general guide to directors and is not intended to serve as legal advice. Legal opinion should be sought on a case-by-case basis as required.

Directors' Accountability and Liability

Information risk is one of the many risks for which the Board is accountable, and hence the normal requirements, regulations and penalties apply. However, regulators, legislators and the public in general have become increasingly concerned to ensure the proper protection of information and the accountability of the individuals who direct organisational behaviour. Directors need to understand the nature of their obligations, which may vary from country to country, and to take care that they are discharging those obligations fully.

The consequences, both for the organisation and for directors personally, can be severe. For the organisation, disregarding relevant provisions can result in:

Regulatory penalties	Regulators can impose fines, sanctions, or additional monitoring, and in extreme cases withdraw a licence to operate within the sector.
Claims for compensation	Perhaps for breach of confidentiality or for not being able to resist claims due to a failure of records management.
Reputational damage	Publicity relating to a breach of key legislation or an irregularity in fundamental controls can damage the brand and lead to a crippling loss of confidence.

Under, for example, section 1121 of the Companies Act 2006 or section 400 of the Financial Services and Markets Act 2000, individual directors can be held liable for offences committed by their organisation. For the director, disregarding relevant provisions can result in:

Fines	In some circumstances, unlimited fines can be imposed.
Civil claims	For example, for negligence, a breach of duty or a breach of trust.
Criminal penalties	In serious cases, a culpable director can be charged with a criminal offence (which might entail extradition) and possibly sentenced to imprisonment.

There has been a significant growth in the UK of litigation against directors. Directors cannot rely on corporate D&O indemnities to provide them with complete protection from such penalties. And, even if charges against a director are unsuccessful, defending claims can still be highly disruptive and very costly.

Directors' Responsibilities

A director's responsibilities fall into two classes. The first is to ensure the organisation retains and protects all the records it might need to meet its obligations. These can include legal and regulatory obligations (e.g. under money laundering regulations, the Companies Act, Health and Safety, tax regulations), the obligation to manage operational risk (e.g. ensuring that copies of contracts are retained for the duration of the contract) and to fulfil business needs.

The second class is to ensure that confidential information is not disclosed without appropriate authority. This can be driven by legal, regulatory or sectoral requirements (e.g. the Data Protection Act 1998, the Financial Services and Markets Act 2000, the Official Secrets Act), by common law duties of confidentiality (e.g., in banking, health services) or by contractual terms (e.g., confidentiality provisions within contracts).

Directors should ensure, at a minimum, that their organisation implements a records management programme which provides for the identification, capture, protection and proper disposal of relevant documents. Directors should also ensure they seek competent legal advice whenever appropriate. The standard of care required by directors is an objective and retrospective test. Directors cannot hide behind incompetent advice if they knew, or should have known or suspected, that such advice was wrong or incomplete.

Legislation

There is a vast range of relevant statutes and laws. These include:

- The **Companies Act 2006, and where relevant, the retained provisions of the earlier Companies Acts**. Relevant sections cover, for example, culpability for destroying company documents and providing false information. Documents are defined as information recorded in any form.
- The **Data Protection Act 1998** (DPA). In particular, the DPA lays out eight principles regarding the way in which data should be retained and handled.
- The **Computer Misuse Act 1990** (CMA) and revisions.
- The **Regulation of Investigatory Powers Act 2000** (RIPA).

There are also many other acts and sector-specific legislation which, though they might not mention record keeping *per se*, do imply it. Defences under such acts might not be available unless the organisation can provide evidence, in the form of reliable protected records, to show that senior management conformed to legal and regulatory duties.

Organisations operating or trading outside the UK or having dealings with foreign organisations will also need to pay attention to EU and foreign laws. Many other countries, both within the EU and beyond, have equivalents to the UK's DPA. America (e.g. Sarbanes Oxley Act 2002; individual state legislation dealing with data loss disclosure) is recognised as a more litigious country than the UK and directors need to take extra care. Other countries with relevant legislation include Australia, Canada, Hong Kong, Singapore, Dubai, UAE, France, Germany, Switzerland, South Africa, Gibraltar, Jersey, and many more.

Certain regulators, for example the FSA, follow a "principles-based" approach. This requires compliance not only with the letter but also the spirit of relevant regulation. Even if an issue does not result in a breach of a specific rule, the regulator may still censure the organisation, and, *in extremis*, its directors, for failing to apply the spirit of the rule.