**Information security risk management**

**Importance of risk management**

Organizations, governments, society and citizens face many threats and risks. No one in these four broad groups is excluded from the situation. In addition we, as individuals, are both risk takers and risk averse depending on the particular circumstances we are in. We may take risks in one area of our lives and be risk averse in another area.

Modern society is highly dependent on the use of IT for commercial and private use. IT presents us with a variety of risks. As individuals we take risks and we are at risk: what we do, how we do things, and how we interact with the IT we use and the environment in which we live and work. There are also specific categories of risk - for example, physical and environmental risks, safety risks, health risks, financial risks, operational risks and, of course, information security risks.

Information is a business asset with varying levels of commercial value and sensitivity. In addition, some of this information is personal data. This means that information needs to be protected from the risk of being stolen, misused, modified, destroyed, or not being available to those authorized to have use of such information.

Information security is now a mainstream political, economic, societal and business issue. It is no longer the province of technologists alone; it is a far broader issue affecting all from the CEO, the company board, shareholders, senior and middle management through to every user and member of staff in the organization, irrespective of rank or job role.

**Risk focused strategy**

To be meaningful to the organization, a strategy for dealing with information security risks must be considered in a business context, and the interrelationships with other business functions - such as human resources, research and development, production and operations, administration, IT, finance and customers - need to be identified, to achieve a holistic and complete picture of these risks. This should include taking account of the organizational risks, and applying the concepts and ideas of corporate governance. This, together with the organization’s business, effectiveness and the legal and regulatory environment, all serve as drivers and motivators for a successful risk management process.

**Nature of the Information Security Risk Landscape**

***Risk - what is it?***

Giving a definition of risk is difficult given the wide variety of ways in which the term is used and applied to different fields and applications. What is generally common to these different uses is that the context usually considers:

* uncertainty
* undesirable consequences.

For the purposes of interpreting the term ‘information security risk’ we shall use the following definition:

***Risk*** *= combination of the risk of exposure and the impact = combination of (likelihood of the threat being able to expose an element(s) of the system) and impact*

***Risk of exposure*** *is the likelihood that an element of the system lacks enough protection to be able to counter the effects of a threat. In other words, there is a likelihood that the system element is exposed to being at risk.*

The *uncertainty* is that the organization can only estimate how likely it is to experience the risk of exposure; it cannot work on a basis of certainty. The *undesirable consequence* is the impact to which the organization may be subjected if its assets are exposed to risks. Here we have an important link between the impact and the value of the assets at risk.

The ‘likelihood’ is used to obtain estimates based on unknown parameters and on known outcomes. Therefore, in the risk definition above it is the ‘likelihood’ that the threats (unknown parameters) might be able to exploit weaknesses in the organization, to cause a risk of exposure. Sometimes the word ‘probability’ is used as a synonym for ‘likelihood’, particularly in non-technical everyday speech. However, there are technical and mathematical differences between ‘likelihood’ and ‘probability’: ‘probability’ allows us to predict unknown outcomes based on known parameters whereas ‘likelihood’ is based on unknown parameters and on known outcomes.

***Information security governance***

Information security governance is an essential component of corporate governance. It is a requirement of company directors to demonstrate due diligence in handling information assets on behalf of stakeholders. Information security governance includes all the processes and management decisions that affect company assets in terms of their confidentiality, integrity and availability for business. Without information security governance corporate governance policy cannot be met since there can be little or no assurance and confidence in the internal control system.

(information security

governance)

Information security governance encompasses all business assets, as well as their risks and threats, including information, processes, people, services, IT and reputation. Thus information security governance involves a risk management process, which includes IT risks, human resource risks, service risks, and so on. So, from the point of risk, information security governance has a greater scope than IT governance and its line of reporting is directly to the company board of directors and stakeholders.

The organization’s policy regarding information security governance should recognize:

1. Information risks are an issue for the board of directors.
2. The accountability for information security risk management lies ultimately with the board of directors.
3. Information security risk management should support and achieve the organization’s risk appetite and the approach to integrating risk in management decision-making, providing achievable goals for risk management. The approach taken should meet the needs of the core business activities.
4. Ownership and accountability for managing and reporting information security risks.
5. Roles and responsibilities for managing risk cover:
6. direct responsibility for the management of risk - e.g. management and staff working within each organizational unit;
7. responsibility for the development, implementation, maintenance and oversight of the effectiveness of the risk management framework - e.g. a risk committee;
8. responsibility for providing independent assurance - e.g. internal audit;
9. ultimate responsibility for obtaining assurance and thereafter driving improvement. There is a need to take into account how people (e.g. staff) behave or are likely to behave within risk management processes.
10. A well defined and understood policy which sets out the requirements for managing risk and which is effectively communicated across the organization.
11. Well defined processes and procedures for information security risk management.
12. An effective method of assessing and monitoring the organization’s information security risk management culture.
13. Clearly defined parameters around the level of information security risk that is acceptable to the organization, and thresholds which trigger escalation, review and approval by an authorized person or body.
14. A well defined approach to recognizing information security risk in management decision-making. Information security risks should be considered in decision-making when any significant business change is planned, be it acquisition of new IT applications, entering into a new area of business, or changing business processes.
15. Specific, timely, accurate and reliable methods of reporting, and an appropriate flow of risk information around the organization.
16. A commonly defined and agreed terminology for key information security risk management principles and practices.

*Information Security Risk Management* ***Handbook***

**1. Say if the following statements are true or false. Give reasons for your answers.**

1. Every person, organization or society is both risky and cautious.
2. Nowadays information is a valuable asset of a business.
3. Information security today is the only priority of optical, economic, societal and business circles.
4. Information security strategy is one of the functional strategies.
5. The concept of risk encompasses two ideas: danger and consequences.
6. In terms of information security the ideas of uncertainty and undesirability are not interrelated.
7. Information security governance is part and parcel of corporate governance.
8. A risk management process includes all kinds of risks a company may face.
9. The board of directors is responsible for meeting the needs of the core business activities.
10. Information security strategy is the priority of the IT department .
11. It is impossible assess any corporate risks in advance, so the risk manager is to square all the problems occur when they arise.
12. The key information security risk concepts must be understandable and executable by anyone in the company.

 **2**. **Make a gist of the text (1-2 sentences).**

**3. Make an outline of the text.**

**4. Make a summary of the text (10-15 sentences)**