



“Think, then act - There is nothing so useless as doing efficiently what shouldn't be done at all.”

Peter F. Drucker

Information Security Governance Design

Information is the blood of every modern organisation. In order to allow the organisation to function properly, it is paramount to protect the flow of information throughout the organisation. Information Security Governance provides the framework wherein the information security policy, principles, responsibilities and practices are defined. It provides adequate security, ascertains that risks are managed and addressed appropriately, and verifies that the organization's resources are used responsibly.

The qualities of a well designed Information Security Governance framework can be recognized:

- *Alignment with the organization's security requirement;*
- *Integration with the corporate/organizational culture and processes;*
- *Effective risk management practices regarding information in all its aspects;*
- *Facilitating measurable protection of information.*

Information Security

The purpose of information Security is to protect information that is exchanged, processed and stored by the organisation, regardless the form, process or activity wherein this information is used. More specifically, the security properties of information that have to be protected are:

- **Confidentiality:** Information is available to the right people in the right form;
- **Integrity:** Information is correct and can only be changed as envisioned;
- **Availability:** Information is available to the organization to support the proper functioning.

Information Security Management

Information Security Management is a process that enables and establishes the protection of information. It is organized according to a typical management process, better known as the Deming Cycle.

According to this established model, information security management will have to pass through the following phases:

- **Plan:** Analyse the requirements and define/design your action or measures;
- **Do:** Execute the actions and/or implement the measures;
- **Check:** Verify and measure the results of the actions performed and monitor and control the implemented measures;
- **Act:** React on observed deviations from the preset objectives.

About Aszure

Aszure is specialized in operational risk management consultancy and staffing. Operational risk management, information security, business continuity and compliance to laws and regulations are major cornerstones of our services.

Aszure assists its customers with the incorporation of operational risk management at all levels and in all areas of their organization, including day-to-day operational decisions. No decision should be taken in any organization without applying proper operational risk management. It can be applied throughout the entire life cycle of any activity or project. In order to minimize risk, it is however preferable to apply operational risk management is applied at the beginning phase of a project or operational activity.

About Aszure Academy

Aszure offers, through the Aszure Academy, an extensive education and awareness program, covering several open classes, events and customized education experiences.

Contact

For further and additional information, please contact us on Tel. +32 (0)9 243 10 20 or info@aszure.com

On all Aszure services our general terms of delivery apply.

Information Security Governance Design

By closing this cycle (e.g. re-assessing security requirements and redesign security measures after observed shortcomings), effective and mature management practices are established.

Information Security Governance

By performing these management processes throughout the whole organisation, or in other words by demonstrating these information security management practices on a holistic level, the whole organisation and its objectives will benefit from the information security efforts.

This holistic approach implies that actions are taken on strategic, tactical and operational level.

Design the framework

The design of the framework will define the policy on strategic level, as well as the security principles and management roles, - responsibilities and –processes on the tactical level.

The global management process (across all three layers) is based ISO/IEC 27001:2005 ISMS requirements standard.

The framework that will be managed by the ISMS, is structured according to ISO/IEC 27002:2005. This allows for a holistic framework addressing the great variety of information security requirements that can and do exist, within an organisation on strategic and tactical level.

Deliverables

Aszure typically can provide the following design deliverables:

- Corporate Security Policy;
- Security Principles according to the security domains (from ISO 27002);
- Assigned (Security) Roles and Responsibilities;
- Security Process design (e.g. password management).

Aszure Benefits:

- Broad experience from large a variety of organisations (public and private);
- Result driven towards strategic objectives (no security for the sake of security);
- Holistic integration of the framework within the organisation to provide a large support base.

Precursors:

Typically this activity is preceded by an information security audit, assessment or GAP Analysis.

Next step:

Typically this activity is followed by implementing the information security governance framework on the operational level.



Interested in world-class education and training on information security governance, ISO standards and security policy: visit the website of the Aszure Academy (www.ascureacademy.eu).

For more information, please contact:

Tel.: +32 (0)9 243 10 20

E-mail: info@ascure.com www.ascure.com

Bijenstraat 16-17, B-9051 Ghent , Belgium