



“In theory, there is no difference between theory and practice; In practice, there is.”

Chuck Reid

Information Security Governance Implementation

Information Security Governance provides a framework to protect information within the organisation or enterprise. However, the definition and design of this framework alone is far from sufficient to deliver effective information security. The framework provides a high level approach to information security, but these principles need to be put into practice. The implementation of information security governance will translate the theoretical framework on operational level.

The main target is to establish processes and security practices within the organisation. These processes and practices can be supported by:

- *Procedures: clear and detailed descriptions of actions that have to be performed;*
- *Directives: Communicate the principles and derived procedures to (a specific) operational level;*
- *Acceptable use policies / Code of conduct: address the human factor and behaviour in information security;*
- *Align complementary security measures to achieve desired level of Security.*

The Theory

Before implementing information security governance, it is necessary to have the framework in place. This does not imply that the full context of the framework has to be defined before one can start to implement. However, it is highly recommended that after the definition of a security policy or principle, the translation of the very same element of the framework is presented to the organisation in a format that is immediately effective and applicable. Only by putting the theory as defined within the information security governance framework into practice, one can be assured that the governance efforts will yield effective results.

The Practice

Implementing the information security framework will result in security measures that are taken within the organisation. Security measures will support the phases of the PDCA cycle, except the planning phase (covered by governance framework definition):

- **Do:** Preventive measures will reduce the probability that information risks materialise;
- **Check:** Detection measures will assure that compromises are detected;
- **Act:** As such, reactive measures can be taken to reduce the impact of the materialised residual risk.

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 Implementation

Multidimensional approach

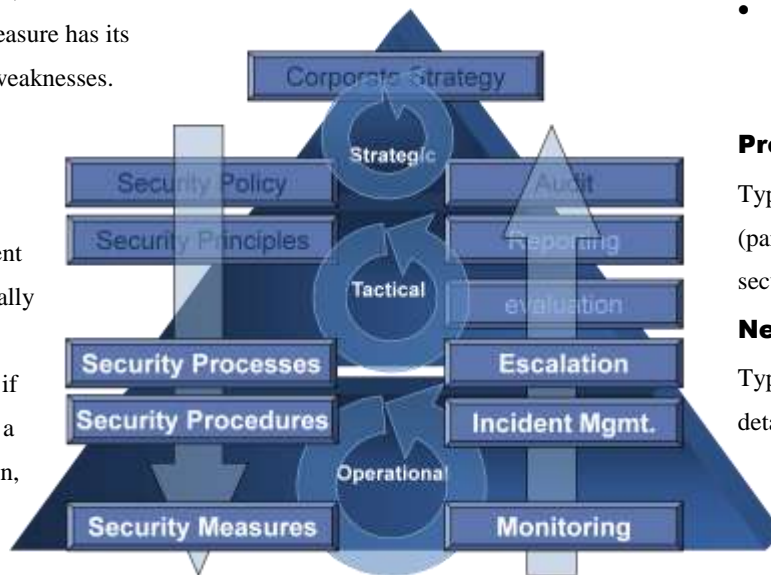
There are literally thousands of ways to protect information. How to make sense of all these methods? A first clear structure that emerges is the definition of the framework. One can compare the governance framework as being the skeleton for your information security body. However, it won't do much if muscles (Do), Senses (Check) and neural system (Act - Plan) aren't available. Putting meat to the bone is usually done by implementing security measures within your organisation. After structuring the approach, one should be aware that:

- It is rare to find one single solution to security problems;
- Each security measure has its limitations and weaknesses.

In order to achieve an optimal solution to security problems, a combination of different security measures usually is the best choice. This is especially true if the measures work in a complementary fashion, where weaknesses

Of one security measure are leveraged by other measures. As such three dimensions to security measures and solutions have to be addressed:

- **Technology:** automated solutions are reliable and transparent to users of the protected information technology, but tend to have some (hard) limitations;
- **People:** The best firewall is usually between the ears, and is by far the most flexible and intelligent one, but is less consistent and hard to implement (usually requires behavioral change);
- **Processes:** Effective security measures rely on correct / desired behavior combined with the right technology in a specific sequence of actions.



Deliverables

Aszure typically can provide the following implementation deliverables:

- Conceptual Security Architectures integrating complementary *technologies*;
- Directives and Codes of Conduct to steer the behaviour of *people*;
- Adaptation of existing processes or definition of specific security *processes*.

Aszure Benefits

- Broad experience from large variety of organisations (public and private);
- Result driven towards effective implementation (no theory);
- Aszure has the necessary knowledge to perform any further detailing of security measures.

Precursors:

Typically this activity is preceded by a (partial) definition of the information security governance framework.

Next step:

Typically this activity is followed by detailing the implementation of each dimension of the complementary security measures.

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