Information Security Management System (ISMS)

ACTAGIS Consulting services deploying ISMS in your organization in order to protect your business in a coordinated and sustainable way

Why deploying an ISMS ?

Information is a vital asset for your organization and any attempt to undermine its integrity, confidentiality or availability can cause major impacts at the financial, legal, operational and reputational levels.

In this context, and knowing that the threats to your information systems are continuously evolving, the expectations of stakeholders to secure organizations are increasing. To meet these needs, ACTAGIS offers to implement an ISMS that will allow you to:

- secure your information effectively and efficiently
- reduce costs through optimal application of security measures based on risk management
- establish a framework for compliance with contractual, legal and regulatory requirements
- fulfill easily your contractual obligations towards your customers and partners
- strengthen your image in the market and therefore help you gain a competitive advantage

ACTAGIS consulting services

Through the experience acquired during multiple successful ISMS deployment projects in large companies and government agencies and strengthened with the corresponding professional certifications, ACTAGIS consultants can help you deploy an information security management system adapted to your context, while providing the methodological and practical skills needed.

Why ACTAGIS ?

ACTAGIS consultants have comprehensive expertise and the experience required to implement an ISMS with experts and specialists mastering the pragmatic sequencing of the actions to undertake to reach the success of the project.

ACTAGIS also offers a methodology from which its customers can benefit in order to reduce the complexity and duration of such projects, which will fit all sizes and types of organizations.

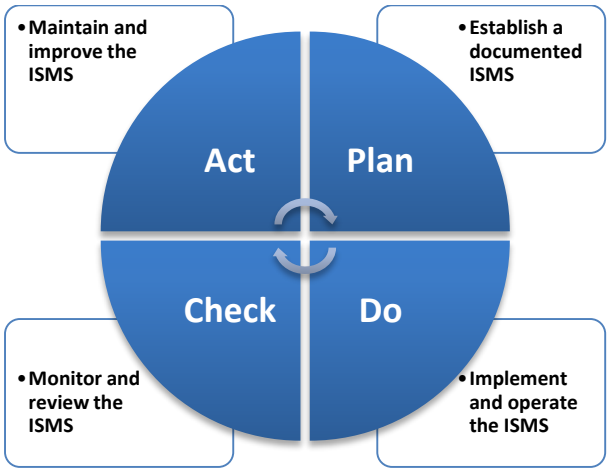
The ISMS

An ISMS deployment project is inherently complex by the fact that it concerns not only the IT department, but also many other services, such as human resources, general resources, and all business services involved. In addition, this project aims to involve people at all levels of the hierarchy.

This high level of complexity results in the need to organize the process in many major phases and then in sub-projects, which are often supported by different people.

One possible approach to the implementation of an ISMS - and one of the first that comes to mind - is the so-called sequential approach, which consists in following sequentially the requirements of ISO 27001 (ISO 27001 standard sections 4-8).

The diagram below shows the general steps for the establishment and management of an ISMS (according to the section 4 of the ISO 27001 standard).



The "Plan" phase

This phase covers planning and preparation activities before the actual implementation, and includes the following key elements:

- validation of the management and authorization to implement the ISMS
- definition of the scope
- risk assessment and planning of the risks treatment
- choice of security controls to implement (statement of applicability)
- design and planning of the implementation project

The "Do" phase

During this phase, the organization implements the security objectives that have been defined previously.

These activities are:

- deployment of security controls
- establishment of performance and compliance indicators
- staff training and awareness

The "Check" phase

To manage the ISMS on daily basis and to detect the incidents in order to act accordingly.

These activities include:

- internal audits to verify compliance and effectiveness of the ISMS
- internal control to ensure that the processes are working as expected
- reviews that ensure the adequacy of the ISMS in its ecosystem

The "Act" phase

This last step of the cycle covers the ISMS maintenance and continuous improvement.

The corresponding actions can:

- preventive actions to address the causes before the incident occurs
- corrective actions addressing the effects to correct discrepancies and the causes to prevent incidents from reoccurring
- improvement actions, to enhance the performance of the ISMS processes

About ACTAGIS

Active since over 25 years in the areas of IT governance and security, ACTAGIS's trainers and consultants offer their services to businesses to help them create value while reducing risk.

During their professional life, the ACTAGIS's consultants have held senior management positions within large companies or IT departments. They are graduated engineers of the Swiss Institute of Technologies of Lausanne in Switzerland and own a MBA. They have the following certifications: CISSP, CISA, CGEIT, CRISC, ISO 27001, ISO 20000, ISO 27005 RM, CBCI and SABSA SCF.

ACTAGIS Sàrl, which is vendor-independent, is active in international and government organizations and large Swiss companies, offering services and high-level expertise in the areas of value creation, risk reduction and audit.