KPMG

ISO/IEC 27001

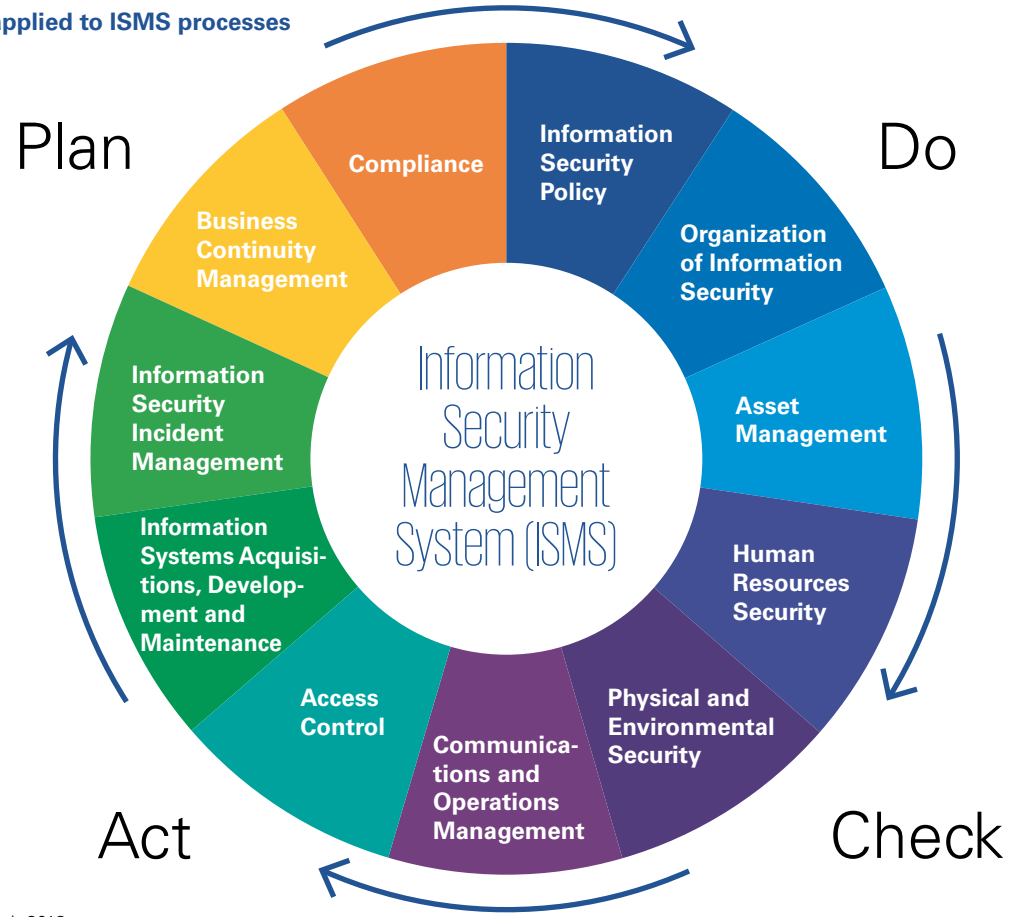
Information Security Management Systems (ISMS) Certification

Are your business data safe? Do you trust your information security measures? Can you prove to external parties that you take care on their data?

The protection of business data is one of the most important success factors in today's world. All companies are potential victims of cyber attacks: increasingly, we hear that companies became victims of hackers and suffered massive reputational damage. As a result, many customers decide not to use some services because they do not trust the company. In addition, the new EU General Data Protection Regulation (GDPR) implies administrative fines for data security breaches (also in Switzerland).

Complying with different regulations and maintaining reputational integrity is a complex task that can most effectively be achieved by means of an Information Security Management System. The ISO/IEC 27001 standard is an international comprehensive framework for developing, implementing and maintaining an independently auditable Information Security Management System (ISMS) aligned with the business strategy and the company's context.

PDCA model applied to ISMS processes



What are the challenges?

- Information security is front page news across the globe, with a constant flow of **new breaches, hacks and incidents** undermining public confidence in the ability of organizations to keep their data safe.
- **Industry regulators** are focusing their energies on ensuring that organizations take the emerging threats seriously and that information security is scrutinized at the highest level in an organization.
- Your **clients are becoming increasingly sensitive** to the measures taken to protect their confidential information and to ensure availability of their systems.
- **Deficiencies in your security** may result in the release of client information and lead to reputational damage both to you and your clients.
- Real or perceived **security breaches** may cause your clients to believe that your organization is unable to conduct business securely and responsibly.
- Security breaches may cause high administrative fines according to the new **EU General Data Protection Regulation.**
- You are **confronted with multiple visits of clients' auditors** and requests to complete security questionnaires or checklists about your controls environment.
- You must demonstrate your capability to meet your **clients' compliance** needs and strengthen their confidence in your ability.

Your Benefits

An ISO/IEC 27001 certification is **proof of your capability** of maintaining an effective Information Security Management System to a broad public, including Industry Regulators and your current and future clients.

Competitive Advantage / Increased Necessity

Reduced Effort for Client-Specific Security Questionnaires / Audits

Proactive Response to Customer Oversight of Security, Privacy, and Data Risks

Internal Assurance Regarding Security and Related Controls

Why KPMG?

KPMG has a team of trained ISO/IEC 27001 lead auditors with extensive experience of performing certifications across all industry sectors. Thanks to our proven methodologies, we can identify and demonstrate improvement and are able to generate valuable benefits for our customers.

Approach Certification Audit

Identify Risks / Gaps (Pre-Audit)

- Health Check Gap Analysis
- Risk Assessment
- Review of Policies and Guidelines
- Review of pre-selected control objectives based on ISO/IEC 27001

Certification Audit
Stage I: Documentation Audit
Stage II: Implementation Audit

- Conduct on-site audits and planning
- Involve subject matter specialists
- Documentation audit
- Take and assess samples in the IT environment
- Perform walkthrough audits and site inspections
- Conduct technical console testing
- Create a draft audit report

Audit Report and ISO/IEC 27001 certificate issuance

- Discuss the draft report with the client
- Finalize the reporting using client input
- Release the final report
- Plan countermeasure for non- conformities, observations, and recommendations
- Issue the ISO/IEC 27001 certificate if the organization is mature enough
- Plan the surveillance audit

Contact

KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich

kpmg.ch/ipbr

Matthias Bossardt
Partner
Head of Cyber Security

+41 58 249 36 98
mbossardt @kpmg.com

Reto Grubenmann
Director, Consulting
Head of Certification Services

+41 58 249 42 46
retogrubenmann@kpmg.com

Reto Mathys
Manager
Certification Services

+41 58 249 26 27
rmathys@kpmg.com

ISO/IEC 27001 March 2018