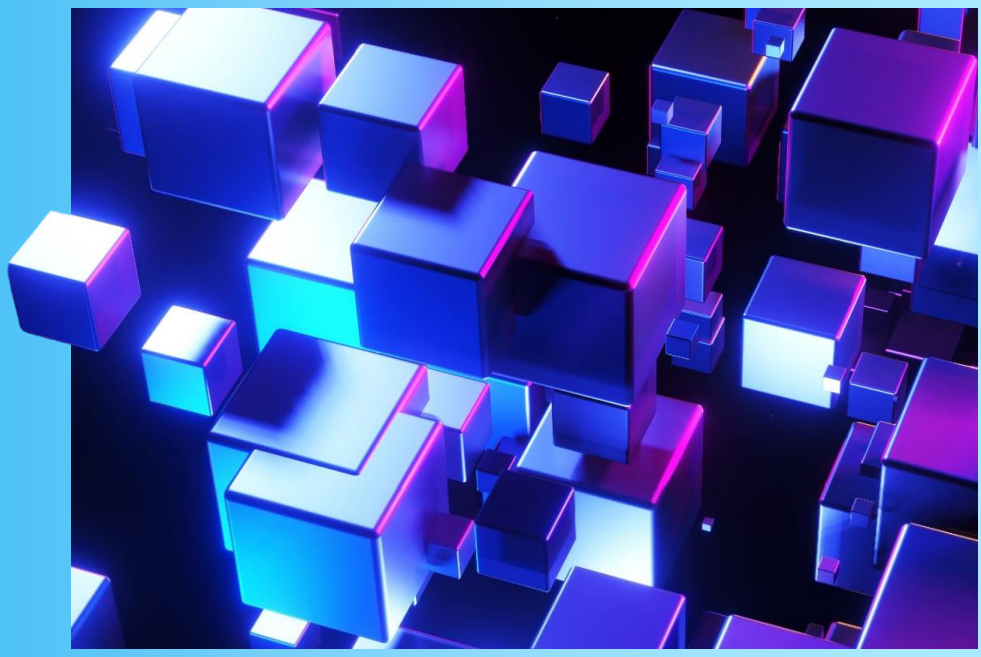
Malta & Cybersecurity - Inspiring Trust beyond Regulation



August 2022

kpmg.com.mt

Is your business data safe? Do you trust your information security measures? Can you prove to external parties and authorities that you take care of their data? Can you recover from a cyber attack?

Introduction

- It is a misconception to think that only regulated entities see value in aligning their organisation to the comprehensive characteristics of internationally recognised information security standards such as ISO/IEC 27001 or NIST.
- Avoiding data breaches (and their associated penalties), safeguarding sensitive data, and improving the ability to tender for contracts where an Information Security Management System (ISMS) certification is a requirement are not issues confined to the Financial Services industry.
- The truth is that protecting one's reputation and information is of paramount importance for all companies, as being trusted is a key element of business success.
- ISMS (Information Security Management System) compliance generates trust in the market; it proves that your organisation and its employees take data security seriously.

Why do we have frameworks?

What is ISMS?

An ISMS (Information Security Management System) is a framework which supports and demonstrates that security is appropriately managed across numerous areas, including operations, financial information, intellectual property, employee details, or information entrusted from third parties.

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.

What is ISO/IEC 27001?

ISO/IEC 27001 is a standard published by International Organisation for Standards (ISO). ISO/IEC 27001 may be used as the basis for ISMS implementation. It specifies the requirements for the design, implementation, operation, monitoring, analysis, maintenance and improvement of documented ISMS in the course of an organisation's general business processes.

ISO/IEC 27001 may also be applied, as it contains a set of practical guidelines for ISMS building based on best practices and experience in this area. In addition, the requirements of these standards can also serve as a basis for ISMS assessment.

Industry Frameworks

Experience

Allows organisations to build on decades of research, thinking and real world experience to provide leading practices and responses to threats.

Recognition

Adopting a recognised framework provides others with a way of understanding how an organisation performs security, and to what level.

Stability

Frameworks provide a consistent target for long-term programmes, with predictable change to address emerging threats. This helps with budget and investment cycles, as well as assurance practices.

Structure

Understanding the completeness, risk position, and being able to have a structured approach to security is vital for a robust and successful security implementation.

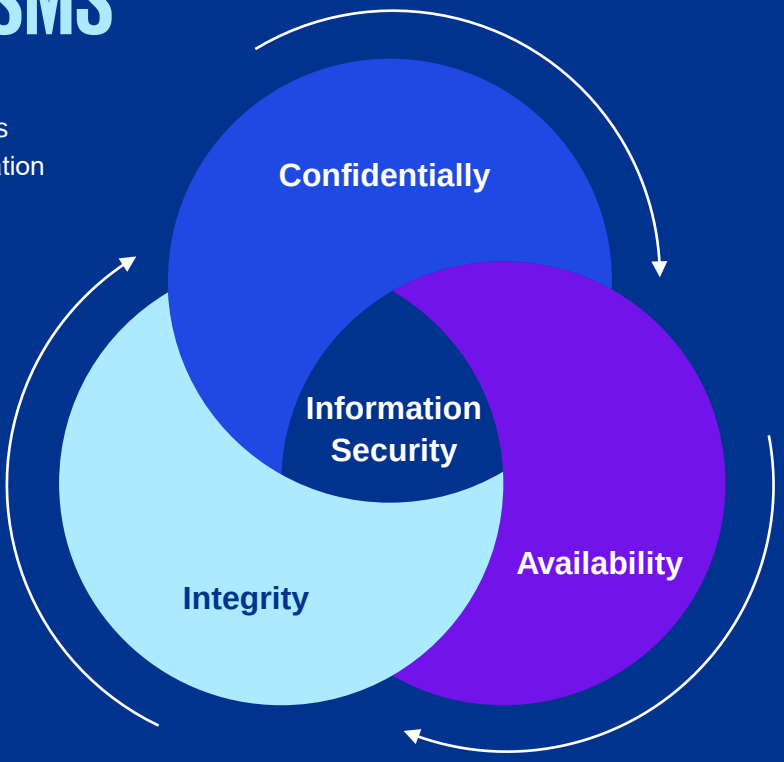
Drivers to follow ISO/IEC 27001 ISMS framework

An **Information Security Management System (ISMS)** consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information assets.

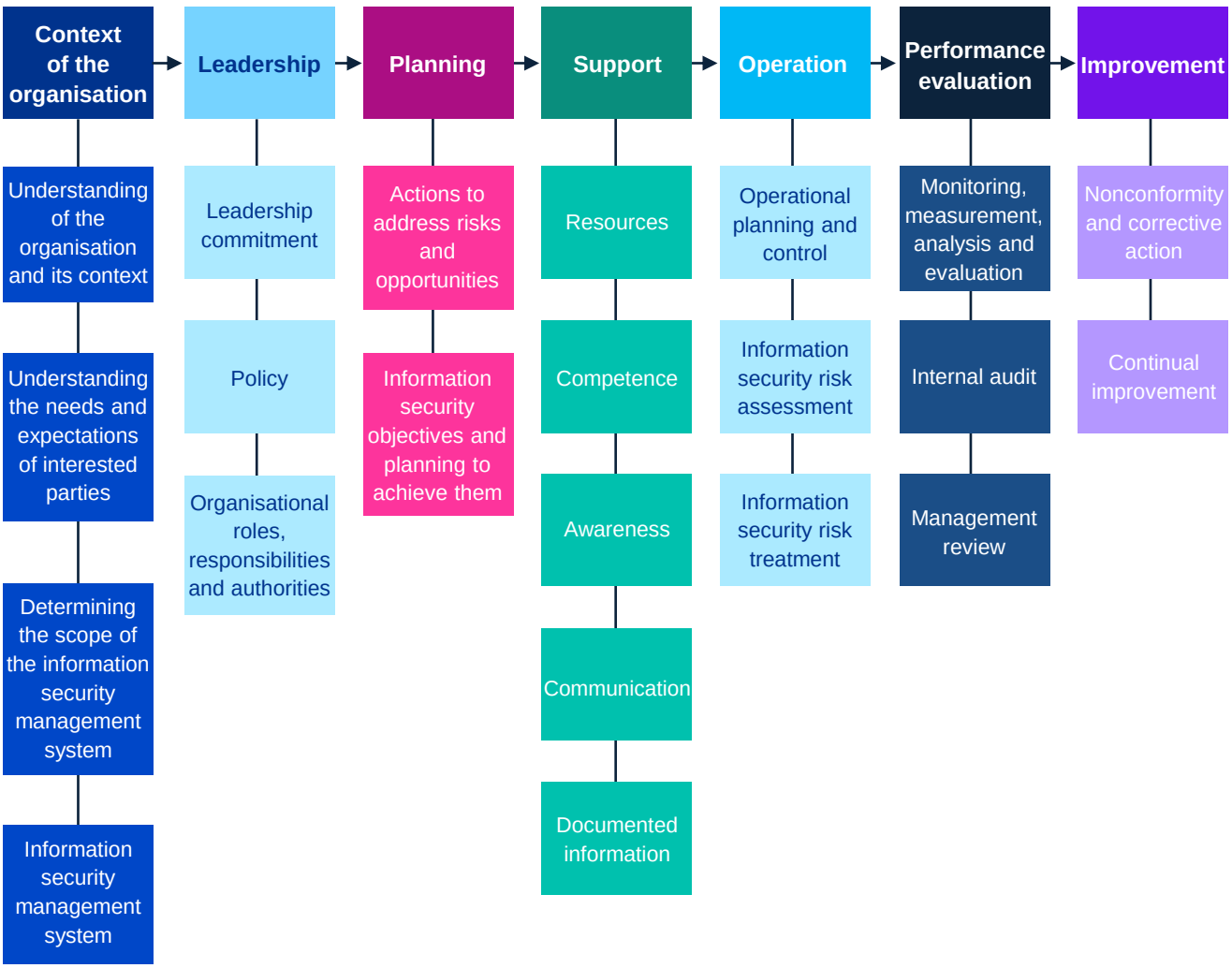
- To **manage risk** and security investment more effectively.
- To drive information security and **maturity** across the organisation.
- Raising **security awareness**, and reducing the risks.
- **Reduce impact** from cyber attacks and other attack vectors including insider threats.
- To establish a **minimum level** of security across global operations.
- **Build Trust** with clients, partners, industry and/or market.
- **Win new business opportunities** where a compliant ISMS is a requirement.
- **Strategic approach** to emerging threats.

Scope of the ISMS

The scope of an Information Security Management System (ISMS) requires the organisation to “apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the organisation. This is carried out by building synergy between people, processes and technology to fortify and protect critical information and assets.



ISO/IEC 27001 Management System Clauses 4-10



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 organisations to keep their data safe.

Industry regulators are focusing their energies on ensuring that organisations take the emerging threats seriously and that information security is scrutinised at the highest level in an organisation.

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 organisation 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.

PDCA Model for continuous improvement

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

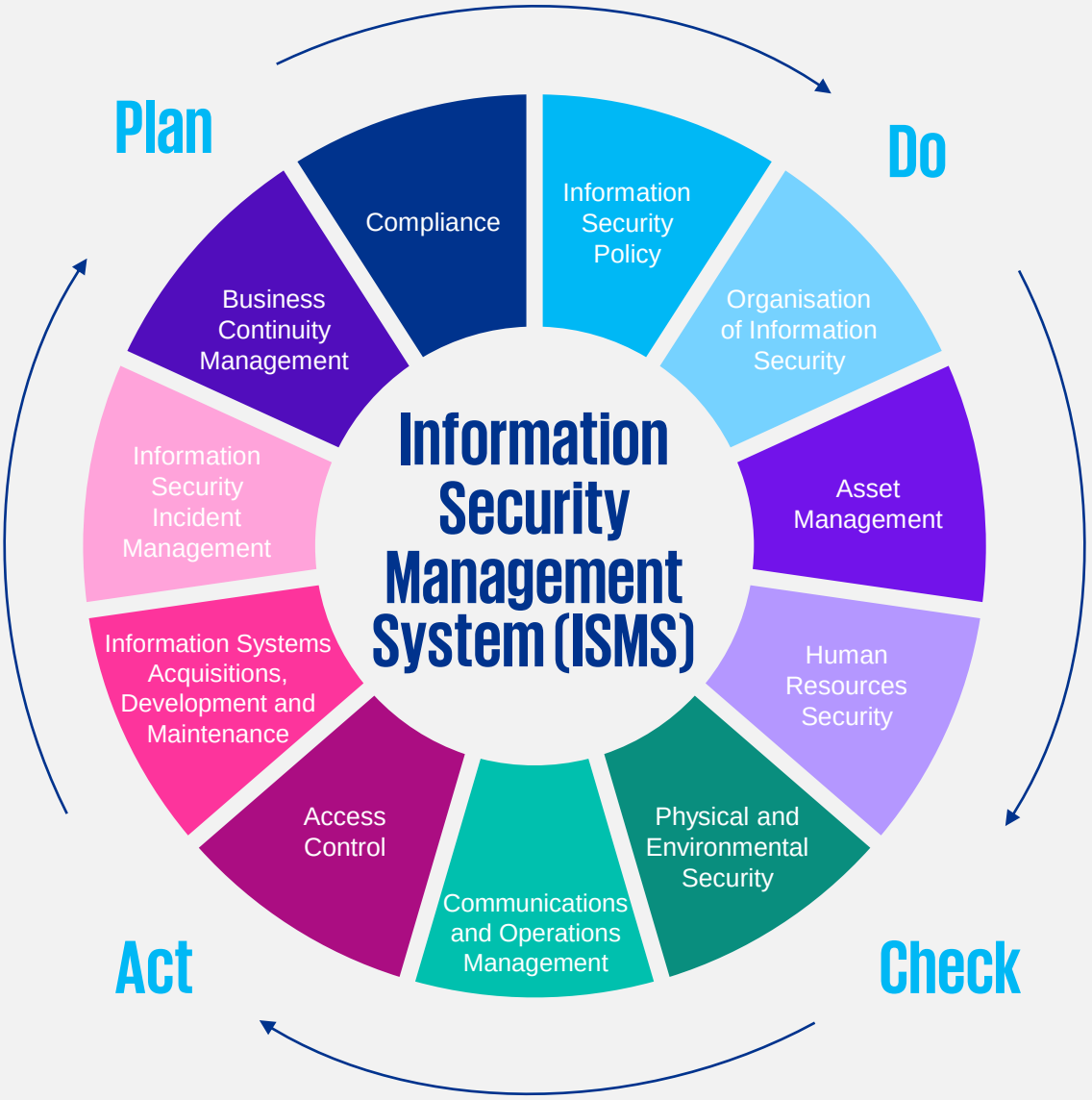
How can KPMG help?

We can help you assess the maturity of your organisation's information security and the divergence from best practice by performing information security management system framework Gap Analysis and Implementation Assessment.

Our level of involvement in your ISMS journey can be adapted to your specific needs, be it:

- Performing a gap analysis against a standard to identify the areas that require attention prior to or during the implementation of your ISMS (such as ISO/IEC 27001 certification).
- Helping with the initial scoping, assisting you in addressing gaps, right through to full implementation, to allow you to become fully compliant, or aligned to an ISMS. This can include planning the project, scoping the company assets, assessing risks, provide training, designing effective processes, practices, policies and standards.
- Identifying and implementing the right tools or products required to meet the required level of controls.

PDCA model applied to ISMS processes



ISO/IEC 27001 March 2018

Why KPMG Digital Solutions

TRUSTED

We have worked with some of the largest companies in the world and delivered on complex global programs. You can trust in the quality of our approach and on receiving personal attention no matter what your size.

TRANSPARENT

We rely on transparent project execution, providing timely and adequate visibility to all the stakeholders and ensure the best output through our multi-tiered quality assurance model.

RELEVANT

We have deep experience and right skills having worked with leading financial institutions around the world.

AWARD WINNING

Our Cyber Security team is award winning. KPMG has been named as a Leader in the Forrester Research Inc. report for the Information Security Consulting Services, achieving the highest score for current offering and strategy

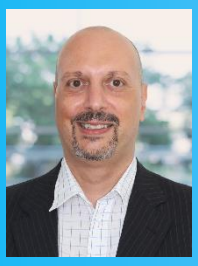
LOCAL PRESENCE, GLOBAL REACH

KPMG is global network of over 207,000 professionals in 153 countries. Through our global network and local pool of cyber professionals, we have the ability to orchestrate and deliver consistently high standards for clients worldwide

Contact us

If you would like to explore this further, understand the benefits and potential results, please feel free to get in touch and we can set up a quick introduction meeting.

Robert Gauci
IT Advisory Lead
Advisory - Digital Solutions
robertgauci@kpmg.com.mt



Dino Conti
Cyber Lead
Advisory - Digital Solutions
dinoconti@kpmg.com.mt

Sinem Demirel
IT Advisor
Advisory - Digital Solutions
sinemdemirel@kpmg.com.mt

kpmg.com.mt