



Security management
Protecting your
information and systems

It's no secret. There's an ever-increasing demand for greater access to your information and systems and from virtually anywhere in the world. The reality is that more points of entry could well mean increased threats to your operations and information assets.

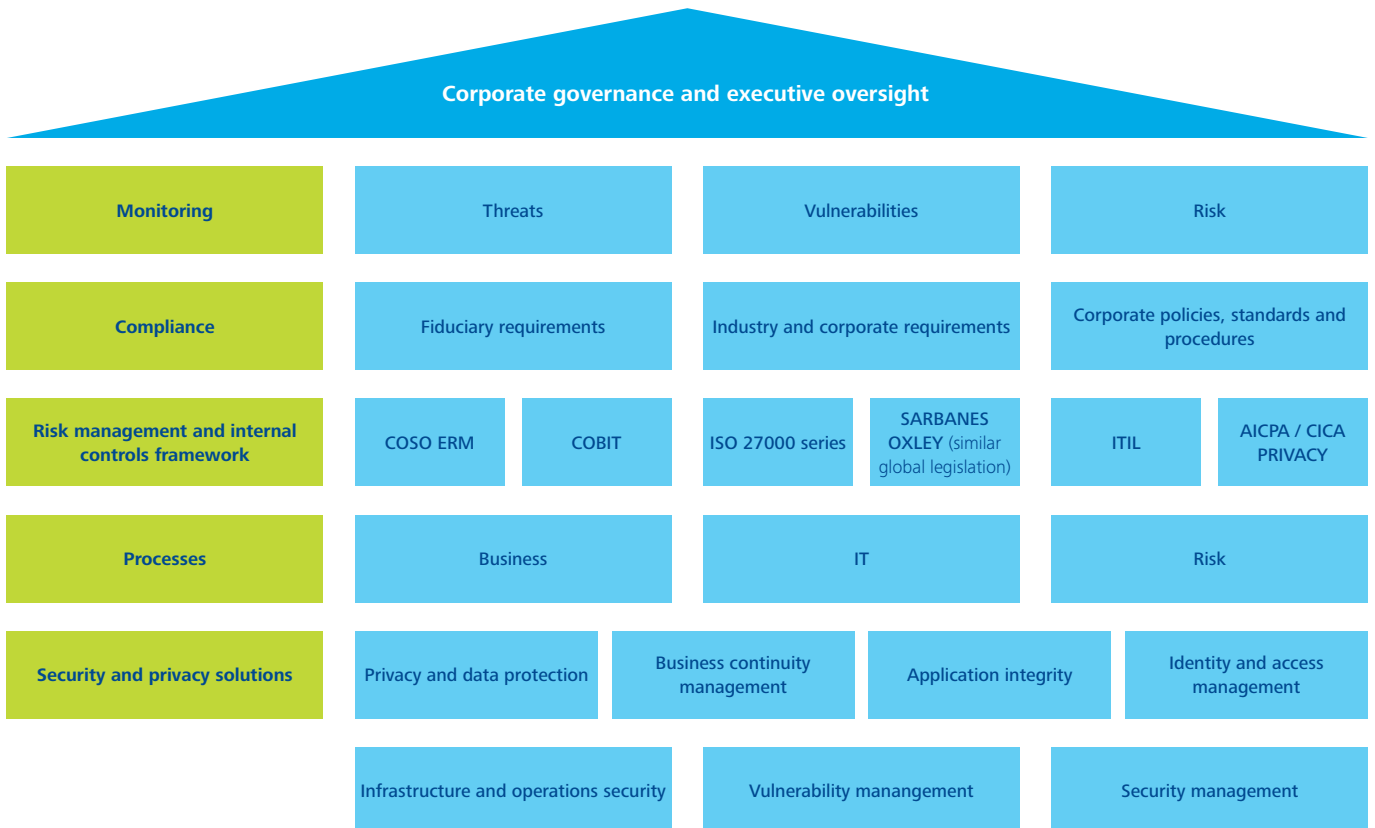
Factors that contribute to this reality include:

- New interfaces between distributed and legacy systems present new access and authorisation challenges.
- The growing popularity of IT operational models and the need to adopt risk and compliance management frameworks are forcing those responsible for information security to rethink their strategies for implementing effective and efficient security controls.

- Security and privacy system costs continue to grow.
- Increased regulation and oversight mean that executive officers carry ever-greater fiduciary responsibility to protect supplier, partner and customer information while, at the same time, meeting regulatory and compliance requirements

An end-to-end solution

Before you can effectively mitigate risk, you need to understand what it is and where it's coming from. A truly effective solution has to be end-to-end. Deloitte can help you develop a framework that successfully integrates security controls into your operations.



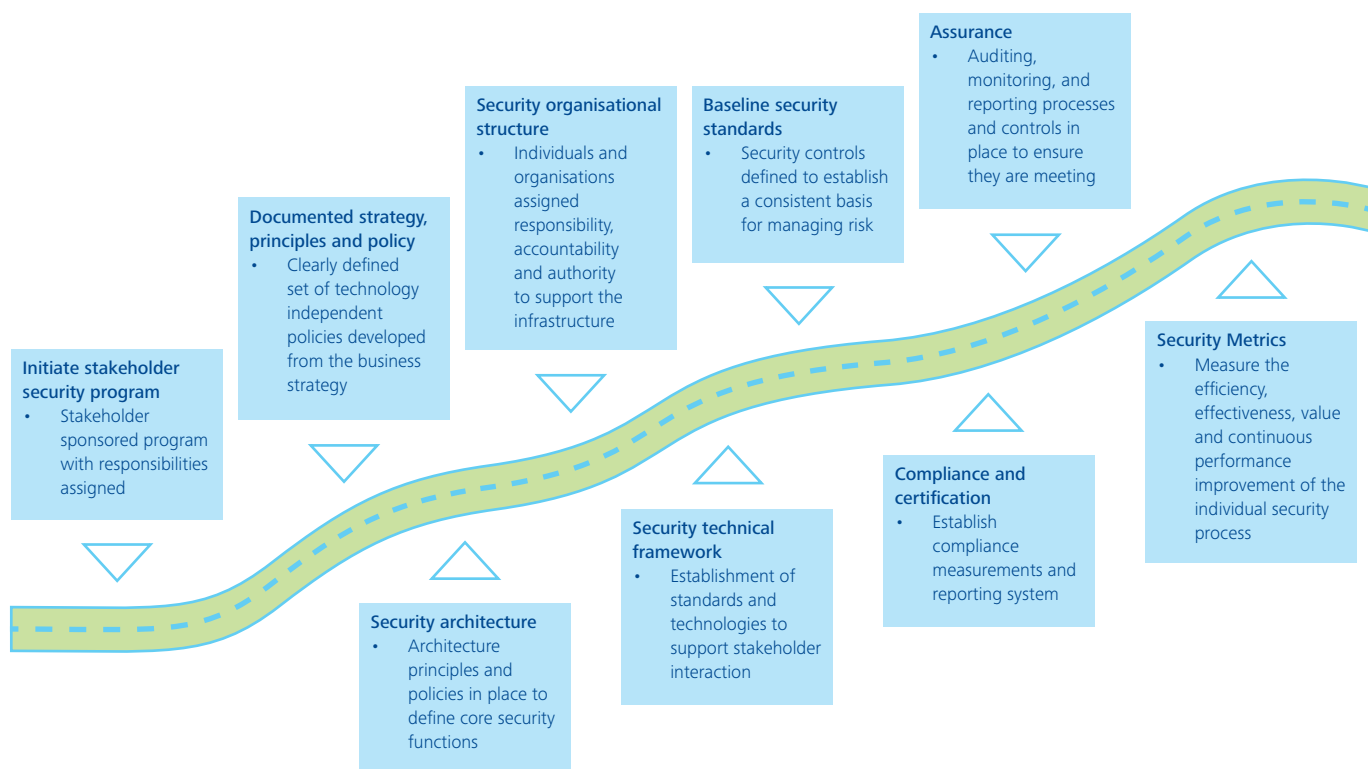
By employing an end-to-end approach, you will increase awareness and understanding of security accountability throughout the organisation, from the governance roles of executive leaders and stakeholders to the responsibilities of people handling day-to-day operations.

As part of an end-to-end solution, Deloitte helps clients to:

- Establish a common risk “language” for all stakeholders.
- Determine the business perspective of what security means to the organisation.
- Align security policy management with business and risk management requirements.
- Establish the elements of the required security program.
- Develop long-term and tactical strategies for addressing multiple industry and regulatory compliance requirements.
- Implement risk management solutions to address business requirements, including risk and control self-assessments, key risk performance indicators and reporting.
- Architect the underlying security and privacy organisation, technology, processes, policy and standards.
- Devise realistic roadmaps for implementing a security program.
- Define the key metrics and reporting mechanisms for ongoing security management effectiveness.
- Reap the benefits from security training and self-assessment offered by Deloitte directly or in conjunction with leading institutes.
- Increase the effectiveness, repeatability and sustainability of the security management operation through automated process workflow and optimised business activities.

By helping you align your security and privacy strategies with your business objectives and structure, Deloitte can help you increase system, process and data security while still controlling costs throughout the entire risk management evolution (see diagram overleaf).





A tailored solution

Security and privacy needs vary from business to business, based on a number of factors, including existing governance, technologies, processes, responsibilities and the degree of collaboration among business partners.

For example, your unique situation may require:

- An integrated information repository that provides a common view of risks to your organisation
- Security plans for core systems, processes and functions
- Other overarching requirements, such as a security and privacy self-assessment program

A multi-dimensional approach

Deloitte's security framework is based on the ISO 27000 series of information security management system standards and is augmented by other control-related frameworks, including COSO ERM, COBIT, ITIL and AICPA/CICA Privacy.

This approach allows member firms to address all dimensions of security management, including:

- IT risk and compliance management
- Policy management
- Security program management
- Governance roles and responsibilities
- Identity and access management including Segregation of Duties (SoD)

- Information asset management
- Threat and vulnerability management
- Security awareness and training
- Business continuity management
- ISO 27000 series compliance and advice
- Gap analysis of organisations against leading information security standards

A responsive and adaptable solution

Deloitte’s framework is responsive to today’s industry trends, including integrated risk planning, compliance monitoring and operating models for managing security. The framework will help address the broader area of risk management planning and testing objectives.

One of the key requirements of any security solution is adaptability. For example, implementing a risk management solution that allows business units to develop and maintain risk and control profiles for each of their core business systems as well as satisfying multiple risk requirements is key.

A successful solution should deal with processes, applications and infrastructure across a diverse range of areas, including IT security, information risk management, business continuity management and data privacy.

Sustain

- Control Assessments and Certifications
- ISO 27000 series/COBIT/ITIL Compliance
- Business Continuity Planning
- Disaster Recovery Planning
- Security Awareness and Training
- Security Education and Certification

Implement

- Security Program
- Identity and Access Management
- Network Access Management
- Application Integrity (ERP/Web)
- Data Protection and Encryption
- Policy Management
- Incident Management
- Controls Automation



Assess

- Vulnerability Assessment (e.g. Penetration Testing, Ethical Hacking)
- Threat Risk Assessment
- Privacy Impact Assessment
- Application Security/Integrity Assessment
- PCI DSS
- Product Selection and Evaluation
- Health Checks
- Vendor Risk Management
- Security Benchmarking

Architect

- Security Architecture
- Security Design Patterns
- Platform Security Standards
- Secure Development Guidelines
- Governance, Policies and Standards

Deloitte services

The ongoing mission of the Security, Privacy and Resiliency team is to work with clients to achieve robust security through the delivery of end-to-end solutions, utilising proven methodologies and tools, in a consistent manner globally, by world class experienced professionals. By working together, Deloitte can assist you in improving enterprise security and value, bring new solutions to market and develop risk aware programs and processes.

Security, Privacy and Resiliency form part of the Enterprise Risk Services (ERS) practice. Deloitte has over 16,000 professionals helping clients manage risk and uncertainty, from the boardroom to the network. They provide a broad array of services that allow clients around the world to better measure, manage and control risks to enhance the reliability of systems and processes.

The Deloitte's Security, Privacy and Resiliency services include:

- Security Management
- Identity and Access Management
- Privacy and Data Protection
- Business Continuity Management
- Application Integrity
- Vulnerability Management
- Infrastructure and Operations Security

Deloitte offers broad, customisable solutions that can help clients enhance opportunities and master their most pressing and complex challenges. Deloitte value clients and commit themselves to their success.

Practice highlights

- Approximately 10,000 IT Risk Management and Security, Privacy and Resiliency professionals globally, including over 1,000 CISSPs (Certified Information Systems Security Professionals), more than any other professional services organisation
- Certified professionals in many other technologies and designations including CISA, CISM, CIPP, ISO 27000 series, GEAC, ITIL, CISCO, DR11, BCI, Novell, Tivoli, Checkpoint, Microsoft, Sun, Entrust, IBM, WebSphere, CA, Siemens, SAP, PeopleSoft and JD Edwards
- Industry association memberships with Information Security Forum (ISF), Information Systems Audit and Controls Association (ISACA), International Information Systems Security Certification Consortium (ISC)2, Information Systems Security Association (ISSA), CyLab, I-4, International Association of Privacy Professionals (IAPP), American Society for Industrial Security (ASIS), International Standards Organisation (ISO), Association of Contingency Planners (ACP) and Open Web Application Security Project (OWASP)

Here to meet your needs

Malta contacts:

Ashraf Fahmy

Leader Enterprise Risk Services
Tel + 356 23432000
asfahmy@deloitte.com.mt

Raphael Aloisio

Leader Financial Advisory
Tel + 356 23432000
raloisio@deloitte.com.mt

Ivan Spiteri

Manager Financial Advisory
Tel + 356 23432000
ispiteri@deloitte.com.mt



Deloitte Place, Mriehel Bypass, Mriehel BKR3000, Malta
Telephone: (+356) 2343 2000
Facsimile: (+356) 2134 4443
www.deloitte.com/mt

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte Malta refers to a civil partnership constituted between limited liability companies, and its affiliated operating entities; Deloitte Services Limited and Deloitte Audit Limited. The latter is authorised to provide audit services in Malta in terms of the Accountancy Profession Act.

A list of the corporate partners, as well as the principals authorised to sign reports on behalf of the firm, is available at www.deloitte.com/mt/about.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 140 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's approximately 169,000 professionals are committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.