



ISO/IEC 27001

**INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION –
INFORMATION SECURITY MANAGEMENT SYSTEMS – REQUIREMENTS**

SGS

Why ISO/IEC 27001?

ISO/IEC 27001 certification demonstrates the integrity of your data and systems, and commitment to information security, cybersecurity and privacy protection.

Implementing an information security management system (ISMS) demonstrates your dedication to protecting the integrity, availability and confidentiality of information under your organization's control.

What is ISO/IEC 27001?

Timely, accurate information, clear communications and confidentiality are essential in business. Information security is simultaneously about exploiting interconnectivity and risk management.

ISO/IEC 27001 specifies the requirements you need to establish, implement, maintain and continually improve an ISMS for safety and security. It also includes requirements for assessing and treating information security risks, tailored to your needs.

Key benefits

ISO/IEC 27001 can lead to:

- Enhanced credibility
- Reduced risk of fraud, information loss and disclosure
- Demonstration of integrity to your system
- Business culture transformation and greater awareness of the importance of keeping information secure
- New business opportunities with security-conscious customers
- A stronger notion of confidentiality throughout the workplace
- Better preparedness for the unavoidable – the next security event or incident

Vigilance is needed

The security of information systems and business-critical information needs constant managing to ensure operational continuity and data protection.

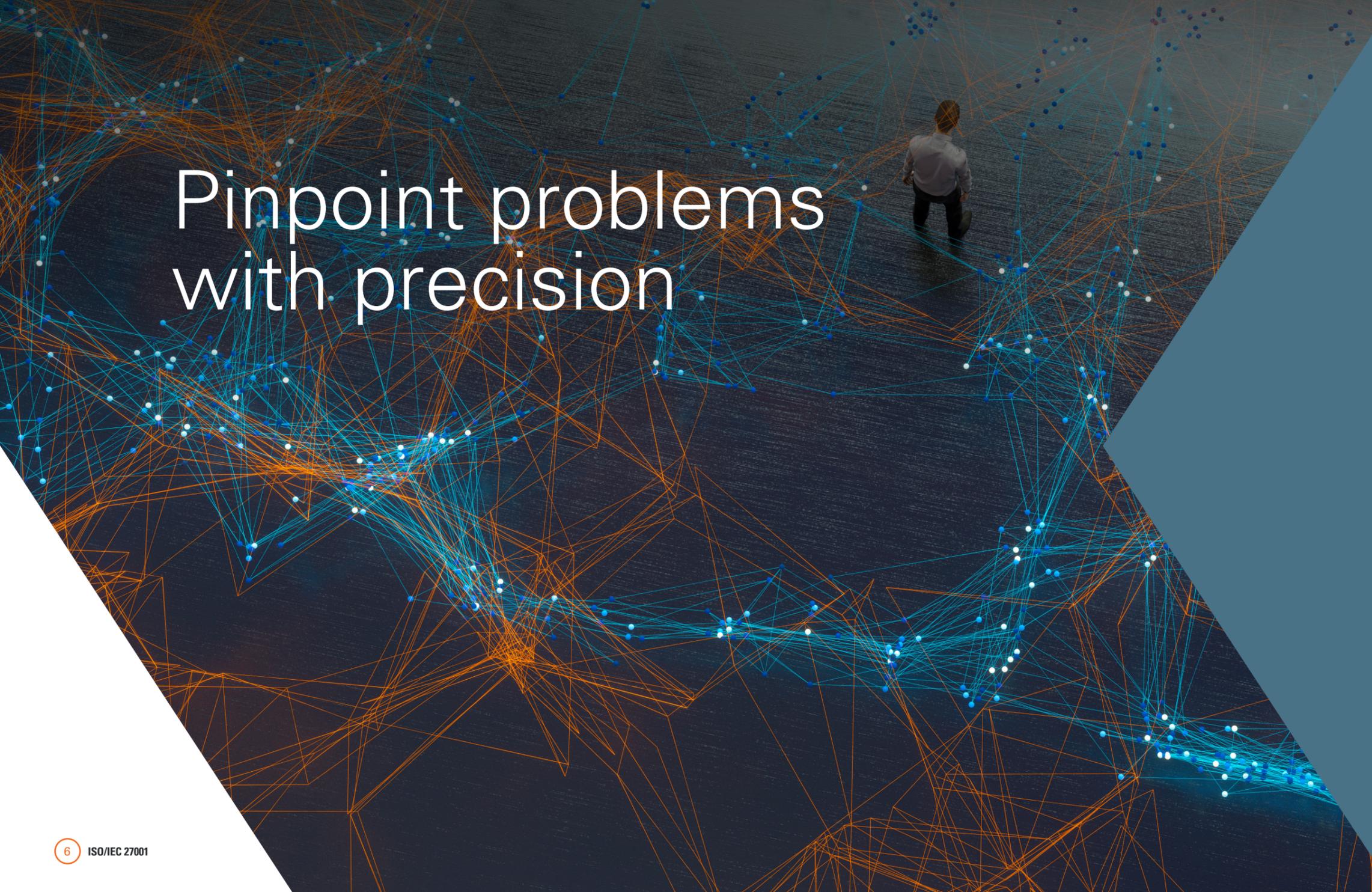
Based on the CIA Triad

The standard aligns with the CIA Triad, which provides vital security features. It helps you to avoid compliance issues, ensuring business continuity, and prevents reputational damage.

Based on the principles of confidentiality, integrity and availability, ISO/IEC 27001 covers:

- Information security policies
- Communications security
- Organization of information security
- Supplier relationships
- System acquisition, development and maintenance
- Asset management
- Human resources security
- Access control
- Information security incident management
- Cryptography
- Compliance
- Information security aspects of business continuity management
- Physical and environmental security
- Operations security





Pinpoint problems with precision

The standard can help you to spot and fix several crucial vulnerabilities.

ISO/IEC 27001 helps you protect myriad information, such as financial data, intellectual property and customer details.

You can pinpoint risks and implement security to suit your business, as well as continually review and refine processes, even for the long term.

Key vulnerability areas

- Individual IT log-on and passwords
- Virus checking, IT backup routines and off-site storage
- Tables of authorities, often financial or press statement-related
- HR practices
- Handling of complaints
- Business and disaster recovery/continuity planning
- IT fault reporting
- Use of email, fax, internet and photocopier guidelines
- Document or file access limitations

Using our extensive experience of the pain points organizations face on the road to certification, we deliver a range of tailored services to support you every step of the way.

A step-by-step certification process

ISO/IEC 27001 has a clearly defined and established certification process.



Implementing ISO/IEC 27001

It is essential that ISO/IEC 27001 is implemented correctly to reap all of the rewards.

Key implementation considerations

-  Ensure senior management support and commitment
-  Engage the entire organization through internal communications
-  Compare your existing system with the new requirements
-  Obtain worker, customer and supplier feedback on current systems
-  Create an implementation team
-  Define roles, responsibilities and schedules
-  Start with the basic principles
-  Use training and incentives to encourage employee involvement
-  Share knowledge on the standard and consider internal auditor training
-  Regularly review the system to ensure continual improvement



Why our ISO/IEC 27001 services?

With expertise in all major industries, we understand each sector's pain points and have the technical skills and logistical capabilities to ensure realistic outcomes.

What we offer

An audit against ISO/IEC 27001 from SGS will help your organization to stand out from the crowd by supporting you to develop and improve processes, as well as increase skillful talent and sustainable customer relationships.

In addition, we offer a range of complementary services:

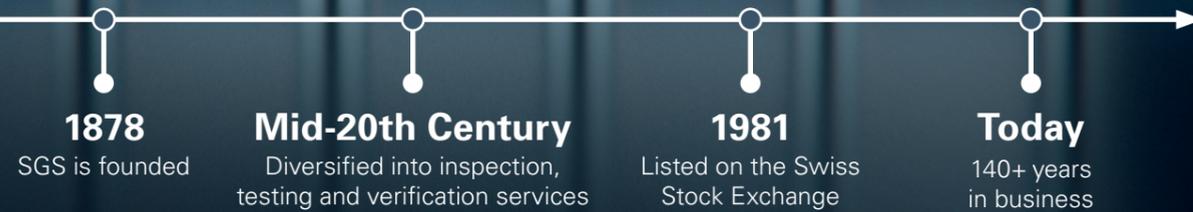
- ISO/IEC 27001 Internal Auditor Training Course
- ISO/IEC 27001 Introduction Training Course
- ISO/IEC 27001 ISMS Auditor/Lead Auditor Training Course

With a global presence, we have a history of successfully executing large-scale, complex international projects. We speak the language, understand local markets and operate consistently, reliably and effectively globally.

About SGS



OUR HISTORY



About SGS

SGS is the world's leading inspection, verification, testing and certification company. SGS is recognized as the global benchmark for quality and integrity. With more than 96,000 employees, SGS operates a network of over 2,700 offices and laboratories around the world. Enhancing products, processes, systems and skills is fundamental to your ongoing success and sustained growth. We enable you to continuously improve, transforming your products, services and value chain by increasing performance, managing risks, better meeting stakeholder requirements, and managing sustainability. With a global presence, we have a history of successfully executing large-scale, complex international projects. Our people speak the language, understand the culture of the local market and operate globally in a consistent, reliable and effective manner.

WWW.SGS.COM

SGS Headquarters
1 Place des Alpes
P.O. Box 2152
1211 Geneva 1
Switzerland



WHEN YOU NEED TO BE SURE

