Navigating your information security journey

A practical guide for SMEs to safeguard information assets, mitigate risks, and build resilience.

Prioritizing information security is key to establishing Digital Trust. Digital Trust is the foundation for secure, resilient, and ethical operations. We understand that knowing where to start when protecting your business and assets can be challenging, especially for SMEs that may not have in-house resources or expertise. This guide has been designed to help you begin your information security journey.

To help you take the next step, we've identified key resources, courses, schemes, and actions that can accelerate your progress. Simply follow our roadmap to safeguard your information assets, mitigate risks, and build trust.

Step 1

An introduction to standards

Learn what a standard is, discover its benefits, and understand how to implement it effectively.

Resources

- **Video:** A beginner's guide to standards
- **Blog:** What are the Benefits of Standards to SMEs?
- **Article:** 5 Reasons Why Standards Matter to Organizations
- **FAQs:** Demystifying Standards: Answers to the Most Commonly Asked Questions

Courses

- The Power of Standards On-Demand eLearning
- Introduction to Management Systems On-demand Training Course

Step 2

Understanding and strengthening your information security

Gain valuable insights and effective strategies to navigate the evolving digital landscape.

Resources

- **Video:** Introduction to ISO/IEC 27001 Information Security Management Systems
- ISO/IEC 27001 client guide
- The Little Book of Cybersecurity
- Digital Trust Resource Hub
- **Success story:** How AdvanceTrack strengthened its infosec credentials as the first UK organization to achieve ISO/IEC 27001:2022
- **Success story:** How Cleardata's commitment to management standards has driven growth and secured new business

Step 3

Buy the ISO/IEC 27001 Information Security Management System standard

Purchase a copy of the information security management system standard, read it, understand the content, requirements and how it can improve your business.

Resources

- ISO/IEC 27001 standard
- ISO/IEC 27001 SME Handbook

Step 4

Empower and upskill with information security training

Explore impactful training courses and qualifications designed to enhance your knowledge and prepare you for success.

Resources

- **Video:** Boosting business with management systems
- **Video:** Drive compliance with team-wide training
- **Brochure:** Digital Trust training brochure

Courses

- Free ISO/IEC 27001 microlearning
- ISO/IEC 27001 Information Security Management Systems Awareness On-demand Training Course
- Lead Implementer ISO/IEC 27001
- Implementing ISO/IEC 27001
- Lead Auditor ISO/IEC 27001
- Internal Auditor ISO/IEC 27001
- All Information Security training courses

@2025 BSI. All rights reserved.

Step 5

Discover Cyber Essentials & Cyber Essentials Plus

Cyber Essentials is a government-backed certification scheme that helps keep your organization's and your customers' data safe from cyber-attacks. The National Cyber Security Centre (NCSC) recommends Cyber Essentials as the minimum standard of cyber security for all organizations.

Resources

- Cyber Essentials client guide
- Cyber Essentials preparation checklist
- Cyber Essentials and Cyber Essentials Plus Certification

Step 6

Implement an Information Security Management System (ISMS)

Establish robust security controls by adhering to the ISO/IEC 27001 standard. Identify risks, implement necessary measures, and continuously monitor and enhance your security posture.

Resources

- ISO/IEC 27001 implementation guide
- ISO/IEC 27001 self-assessment readiness questionnaire

Consider these standards to support your implementation

- ISO/IEC 27002 – Information Security Controls
- ISO/IEC 27005 – Information Security, Cybersecurity and Privacy Protection

Step 7

Conduct a gap analysis

- Schedule a BSI gap assessment to evaluate your readiness.

@2025 BSI. All rights reserved.

Step 8

Get your Information Security Management System (ISMS) certified

Safeguard your information assets, mitigate risks and build trust by embedding rigorous information security practices with ISO/IEC 27001 certification.

Resources

- Certify to ISO/IEC 27001

Step 9

Get support – Let’s shape your organization’s future together.

Congratulations on creating a resilient digital future that prioritizes privacy, safety, security, and reliability. As your partner in progress, we’ll help you become future ready and drive progress towards a sustainable world.

For support and more information, please contact us.

Visit **bsigroup.com**

Call 0345 086 9000

Email **certification.sales@bsigroup.com**

@2025 BSI. All rights reserved.

Frequently Asked Questions for SMEs

Where do we start with ISO/IEC 27001?

Start by understanding the requirements of ISO/IEC 27001 and the benefits it can bring to your business. Familiarize yourself with the standard's structure and key concepts, such as your Information Security Management System (ISMS). You can begin by conducting a gap analysis to identify where your current practices differ from the standard's requirements.

What are the key steps and timelines?

1. Preparation and Planning: Understand the standard, conduct a gap analysis, and define the scope of your ISMS.

2. Risk Assessment: Identify and assess information security risks.

3. Policy Development: Develop policies and procedures to address identified risks.

4. Implementation: Implement the policies and procedures across your organization.

5. Training and Awareness: Train employees and raise awareness about information security.

6. Internal Audit: Conduct internal audits to ensure compliance.

7. Management Review: Review the ISMS performance with top management.

8. Certification Audit: Engage BSI to audit your ISMS.

Timelines can vary, but typically, SMEs can expect the process to take 6-12 months.

How complex is implementation for a small business?

Implementation can be challenging but manageable. The complexity depends on your current information security practices and the resources available. SMEs often face challenges due to limited staffing and budget constraints, but with proper planning and a phased approach, it can be done effectively.

Do we need external support, or can we manage internally?

While it's possible to manage internally, many SMEs benefit from external support. Consultants can provide expertise, streamline the process, and help avoid common pitfalls. However, if you have knowledgeable staff and resources, you can manage internally with careful planning.

What are the common pitfalls, and how do we avoid them?

Common pitfalls include:

- Lack of management support
- Inadequate risk assessment
- Poor documentation
- Insufficient training

Avoid these pitfalls by securing management buy-in, conducting detailed risk assessments, maintaining proper documentation, and investing in training.

How much is this going to cost us?

Costs can vary depending on the size of your organization, the complexity of your Information Security Management System (ISMS), and whether you choose to hire external consultants. These costs typically encompass training, documentation, internal audits, and certification audits.

@2025 BSI. All rights reserved.

BSI Group
Kitemark Court Davy Avenue,
Milton Keynes MK5 8PP
United Kingdom
+44 345 080 9000
bsigroup.com

Your partner
in progress

@2025 BSI. All rights reserved.