Your partner
in progress

Accelerating Innovation and Building Trust

With Certification to ISO/IEC 27001

Build a secure digital future for your organization

Increasing reliance on digital tools, technologies, and services throughout the supply chain is driving the need for a more proactive information security approach to combat new threats[1].

With an Information Security Management System (ISMS) in place, organizations keep the data they are responsible for safe, effectively protect customers, minimize risks, and unlock new growth opportunities across industries and regions.

In this guide, we'll explore how organizations can leverage the international standard ISO/IEC 27001 (Information Security Management System)[2] to strengthen their cyber resilience, both internally and externally, and improve operational efficiency. We'll also show how ISO/IEC 27001 certification helps accelerate innovation and build stakeholder trust.

[1] The World's Third-Largest Economy Has Bad Intentions — and It's Only Getting Bigger, Bloomberg, sponsored.bloomberg.com/quicksight/check-point/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger, April 2024

[2] ISO/IEC 27001 - Information Security Management System, BSI, www.bsigroup.com/en-GB/products-and-services/standards/iso-iec-27001-information-security-management-system/, 2024

Today’s evolving IT landscape

Change is constant within technology. In the last decade, we’ve seen significant, paradigm-shifting breakthroughs, from artificial intelligence and the Internet of Things (IoT) to quantum computing and robotics.

Many of these technologies are already ingrained in our everyday lives; from electric vehicles to smartphone virtual assistants. For example, the percentage of AI-powered smartphones is predicted to hit 54% by 2028[3].

To harness the full potential of these technologies, organizations need strong information security protocols in place. For example, ensuring secure use and storage of both large and small data sets across wider supply chains.

Let’s look at three areas of focus for organizations navigating this landscape.

Build digital trust in innovative solutions

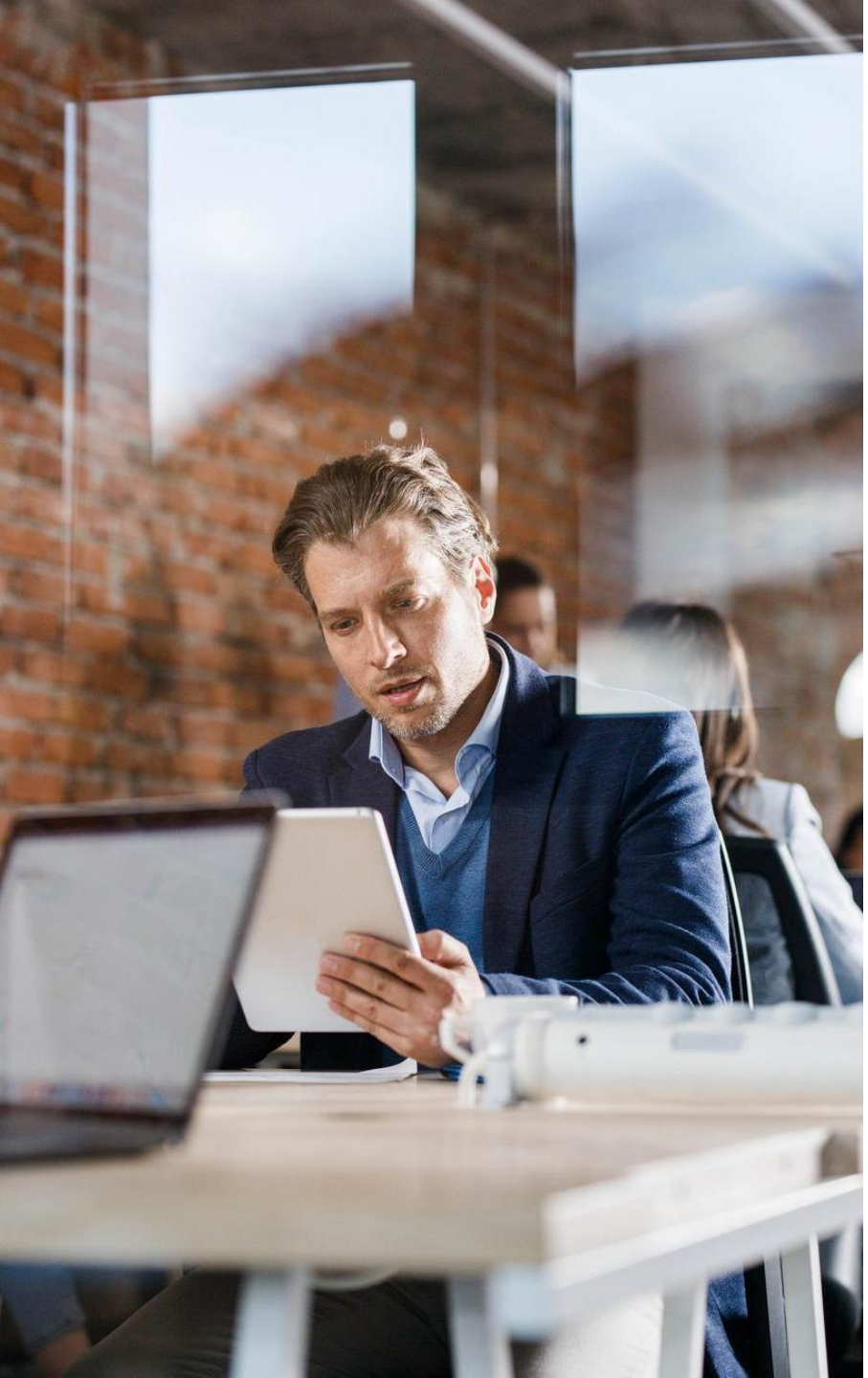
Ensuring that information across the supply chain embodies the three foundations of information security: confidentiality, integrity, and availability[4], increases the performance and trust of solutions like AI. This process builds digital trust, where stakeholders and consumers are confident in your ability to manage and secure the data used in—and generated by—these technologies.

This is important for organizations which handle large volumes of personal and/or sensitive business data, in industries such as healthcare, automotive, and social media services[5]. Many organizations are leveraging best practice standard ISO/IEC 27001 to help with this.

What are digital supply chains?

The definition of information technology supply chains is wider than the traditional purchaser and supplier relationship. A typical business providing a digital service will have data storage, communication, security and operational solutions, among other systems they use, that make up their supply chain.

[3] Share of AI-capable smartphone shipments worldwide from 2023 to 2028, Statista, https://www.statista.com/statistics/1482520/ai-smartphone-shipment-share-worldwide/. Sept 2024
[4] What Is ISO 27001? A Comprehensive Guide, https://www.urmconsulting.com/information-security/iso-27001, Urm Consulting, January 2025
[5] The 7 Industries Most Vulnerable to Cyberattacks, Syteca, https://www.syteca.com/en/blog/5-industries-most-risk-of-data-breaches, March 2024



Strengthen resilience against breaches

To protect themselves in an evolving landscape, organizations are increasingly shifting from reactive to proactive information security strategies[6]. This enables them to safeguard themselves by aligning security controls with both immediate and long-term business objectives.

Within this strategic shift, new technologies are employed by IT and security teams to match evolving cybercriminal behaviours. Initial protection layers are implemented as a foundation, then augmented by proactive threat identification, detection, response, and recovery, providing a holistic, controlled approach to information security.

Some organizations are leveraging AI and machine learning capabilities to detect, respond to, and recover from security incidents more effectively as part of their managed process[7]. To harness these systems, continuous updates and refinement of models are needed—additionally driving the need for robust information management and security protocols to be followed.

With the shift to proactive security strategies and advanced technologies being employed, IT and cybersecurity's role has been elevated to both a protector and a business strategy enabler[8]. Professionals in these teams, such as IT technicians, cybersecurity specialists, and compliance managers play an essential role in building digital trust internally and externally, using the guidance of ISO/IEC 27001.

[6] Strategically Building Breach Resilience, BSI, https://www.bsigroup.com/en-GB/insights-and-media/insights/blogs/strategically-building-breach-resilience/, 2025

[7] The Impact of AI and ML on Cybersecurity, BSI, https://www.bsigroup.com/en-US/insights-and-media/insights/blogs/the-impact-of-ai-and-ml-on-cybersecurity/, 2024

[8] Cyber security, BSI, https://www.bsigroup.com/en-GB/our-expertise/digital-trust/cybersecurity/, 2025

Secure environments through compliance

Recently, there has been a change of focus for new legislation, with many scrutinizing organizations' management of cybersecurity and data throughout their supply chain[9].

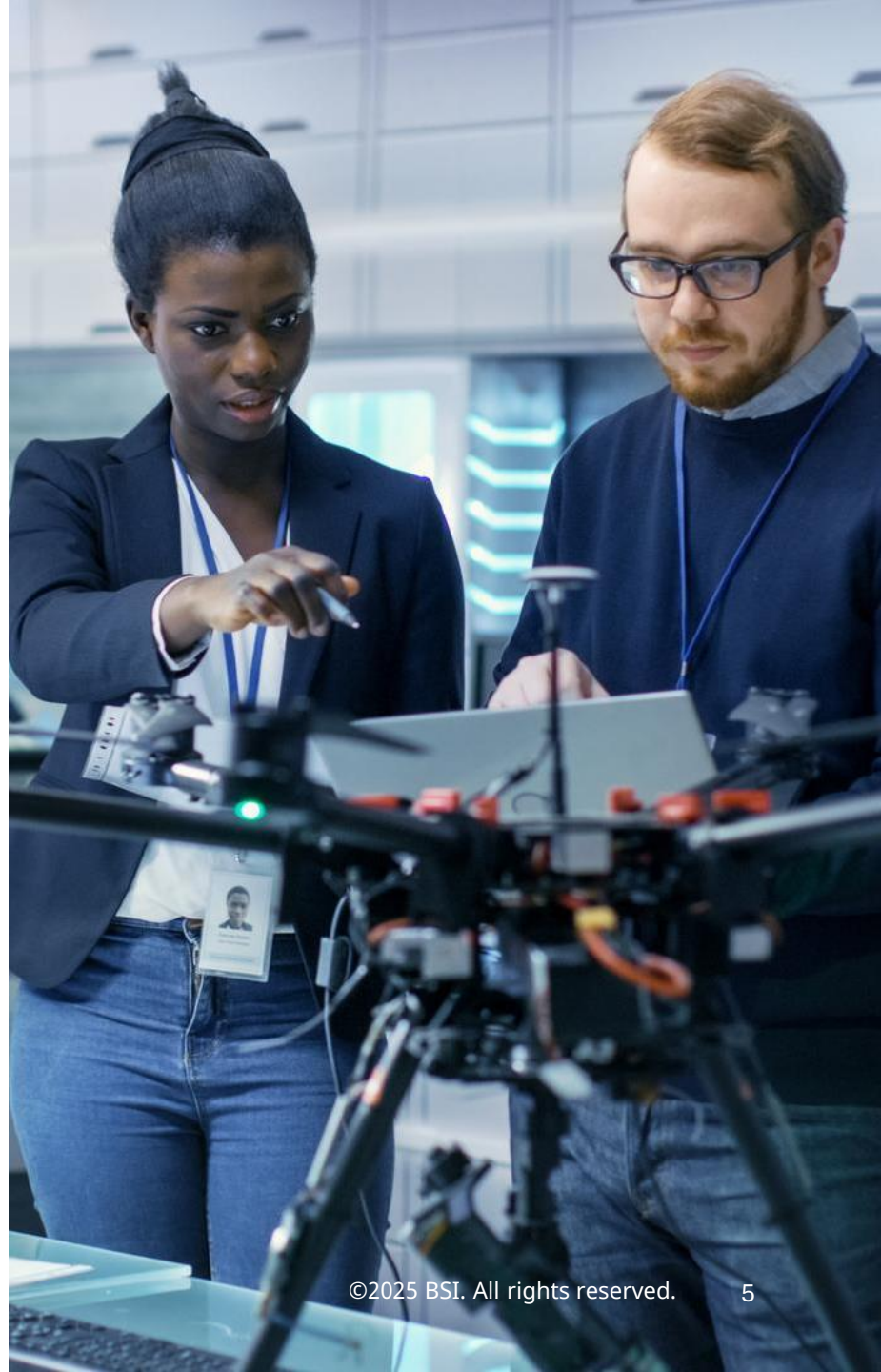
In addition to new legislation, international frameworks and standards are being released[10] that focus on supply chain cybersecurity. Certification to these standards allows organizations to effectively evidence their compliance, improve the security of their solutions, and contribute to a more resilient society.

Legislation that aligns with ISO/IEC 27001 is in action globally. Key examples include:

- NIS2
- HDS France
- TISAX
- Aerospace EASA Part IS
- HIPAA

India's advancement

Recent evolution in India's cybersecurity legislation closely follows ISO/IEC 27001. Under its IT Act 2000, India has created the National Critical Information Infrastructure Protection Centre, overseeing a scheme where critical infrastructure organizations must demonstrate compliance with ISO/IEC 27001[11].



[9] Global supply chain compliance with data privacy regulations, Supply Chain Dive, https://www.supplychaindive.com/spons/global-supply-chain-compliance-with-data-privacy-regulations/727194/. September 2024

[10] Cyber security rules saw big changes in 2024. Here's what you need to know, World Economic Forum, https://www.weforum.org/stories/2024/10/cybersecurity-regulation-changes-nis2-eu-2024/. October 2024

[11] A comparison of cybersecurity regulations: India, PWC https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/india.html, September 2024

Secure your digital information with ISO/IEC 27001

As a cornerstone of international best practice, ISO/IEC 27001 meets changing needs in the market, promoting continuous improvement. The standard works as a foundation for digital trust across industries and regions.

The standard is a starting point for information security management; a universal bedrock that can enable compliance across a variety of needs.

ISO/IEC 27001 contains general requirements and controls designed to be applicable for all, but is also flexible enough that organizations can iterate on it, introducing controls that they need for a specific industry or geography.

Alongside the technical controls and structure it provides, the standard also focuses on creating a positive culture of information security and resilience against breaches, guiding the processes and culture of organizations to support cyber resilience. In particular, it adopts a top-down approach, focusing on how organizational leadership is important for information security[12].

[12] Who will Lead the ISO 27001 Implementation Project Within Our Organization, ISMS online, https://www.isms.online/iso-27001/who-will-lead-the-iso-27001-implementation-project-within-our-organization/ May 2024

Key benefits of ISO/IEC 27001

In addition to the standard's technical and operational guidance, there are several key benefits organizations can unlock by utilizing ISO/IEC 27001:

Global market expansion

By following ISO/IEC 27001 protocols, organizations can strengthen compliance against a wide range of regional and industry-specific legislation. ISO/IEC 27001 has a large-scale influence on the development of information security and ISMS-focused legislation. The global reputation of the standard makes it a potent advantage for unlocking new markets as a symbol of trust.

Build digital trust

The systematic, risk-based approach of ISO/IEC 27001 builds customer and stakeholder trust and confidence. With a proactive approach and sensitive data protected throughout the supply chain, investors, consumers, and employees look for the standard in organizations they engage with.

Keep up with industry best practices

ISO/IEC 27001 helps teams evolve and grow alongside industry best practices as it is continuously reviewed and updated. This ensures teams have the skills and processes needed to manage and audit their ISMS on an ongoing basis, alongside a clear framework for training and implementation.

Key components of ISO/IEC 27001

ISO/IEC 27001 follows the ISO Harmonized Structure[13].

The purpose of the ISO Harmonized Structure is to bring consistency and alignment across ISO Management Systems, ensuring core terms, definitions, and text are used consistently. This is helpful for organizations with more than one management system in place.

To bring unity across information security, ISO/IEC 27001 follows 6 key aspects:

Stakeholder focus:
Organizations must understand the needs and expectations that customers, employees, and partners have of information security management.

Support of the ISMS:
Organizations must display the necessary resources to operate an ISMS, including people, tools, and infrastructure.

Leadership:
Management must demonstrate commitment to ISMS policies and objectives, ensuring alignment with the organization's strategic goals.

Planning:
Organizations must identify knowledge of risks and opportunities relevant to the ISMS, set objectives for the system, and show tangible plans to achieve them.

Operational planning and control:
Organizations must establish plans and processes for operational aspects such as monitoring, training, incident response/recovery plans, and evaluation against new risks.

Performance evaluation and improvement:
Organizations must monitor, measure, and evaluate ISMS performance and conduct internal audits to ensure compliance with ISO/IEC 27001 and continuous improvement.

[13] The Harmonized Approach to Management System Standards, BSI, https://www.bsigroup.com/en-GB/training-courses/the-harmonized-approach-to-management-system-standards-on-demand-training-course/. 2024

A note on Statement of Applicability

While all Harmonized Structure management system standards require organizations to conduct a risk assessment and then apply a treatment plan, for ISO/IEC 27001, a further step is required.

Within Annex A of the standard, there is a comprehensive list of 93 reference security controls, applicable to most organizations. These must be considered as part of the risk treatment plan, and any controls not needed by an organization should be omitted.

Additionally, if a reference control set doesn't fully address a particular risk faced by an organization, they can incorporate controls from other appropriate sources (such as other standards in the ISO 27000 series) or create their own specific controls.

The organization must then create their Statement of Applicability, consisting of:

- Justification for any reference security control included;
- The status of implementation for each (fully implemented, in progress, not started);
- And justification for any reference control sets within ISO/IEC 27001 that are being excluded.

Unlock opportunities with ISO/IEC 27001 certification

Certification enhances the benefits of ISO/IEC 27001 and helps organizations pave the way for new opportunities. By having your ISMS independently assessed by an accredited third party against ISO/IEC 27001’s specific criteria, three additional advantages are available:

Build trust

Inspire confidence with internal and external stakeholders. Certification validates that you are operating with the latest international best practices and are being audited by industry experts, enhancing your brand's reputation.

Drive growth

Certification turns IT and security cost centres into an asset, as organizations can use their compliant ISMS practices as a competitive differentiator. This, alongside the credibility independent certification brings, can unlock access to new customers, markets, and industries.

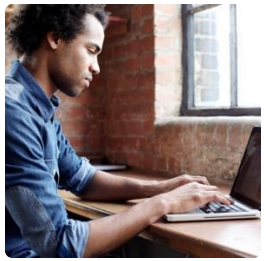
Accelerate innovation

Achieving certification means a robust security and information management system is in place, enabling you to take advantage of technologies such as AI or automation. With a foundation of digital trust and secure processes, organizations can make continuous improvements to existing products and services, as well as identify new opportunities for growth and innovation.

Your partner in progress

For decades, we've helped businesses shape their digital processes and accelerate meaningful progress towards a more secure future. We have a wide range of services across cybersecurity and information management, with supporting ISO/IEC 27001 solutions[14] including:

[14] ISO/IEC 27001 - Information Security Management System, BSI, https://www.bsigroup.com/en-GB/products-and-services/standards/iso-iec-27001-information-security-management-system/, 2024



Courses and qualifications

Solidify your foundational knowledge and practical skills in managing information security, cybersecurity, data and privacy, AI, cloud security, and more, with our digital trust courses and qualifications.

Pre-certification assessments

As an optional early-stage review, a **Gap Assessment** is conducted by our experts to pinpoint areas where your existing ISMS does not meet the requirements of ISO/IEC 27001. Following this stage, a **Pre-Assessment** is recommended to ensure everything is in place before the official certification audit.

Assessment and certification

We conduct the formal certification audit to evaluate your ISMS against ISO/IEC 27001. This comprehensive, accredited review ensures that all aspects of your information security management system conform and are effective. Once you've successfully completed the certification audit, BSI awards you with an internationally recognized certificate.

Why BSI?

As a trusted and accredited partner for organizations and their information security systems globally, BSI is the leading certification provider for ISO/IEC 27001.

Certification is just one aspect of our deep expertise. We developed the BS 7799 standard which was adopted as the basis for ISO/IEC 27001 and are part of the committee that developed both ISO/IEC 27001 and the wider ISO/IEC 27000 series of standards.

With history spanning the development and ongoing certification of ISO/IEC 27001, we are uniquely placed to accelerate your progress, whatever your industry or size. Our auditors are positioned globally to help you on your information security journey, with remote, hybrid, and in-person capabilities. Building both your knowledge and your digital capabilities, we partner with you to create a secure digital future, teeming with possibilities.

To learn more about our information security capabilities, visit our website, or speak to a member of our team.