Deloitte.

Beyond defense: The business benefits of ISO 27001 certification

Transforming cybersecurity challenges into business opportunities with ISO 27001.

The destructive aftermath of a successful cybersecurity attack extends beyond data loss and financial damage, deeply infiltrating a company's reputation and customer trust—consequences that many executives are all too aware of. They understand that a significant breach could result in a devastating blow to their entity's future success, let alone sleepless nights and consequences to their own career trajectories.

Yet, within this challenging landscape exists a strategic advantage many underestimate—the business value of a resilient cybersecurity program. By leveraging Deloitte's vast experience in this domain, organizations may harness such a program as a protective measure and a powerful tool to boost business. It bolsters customer confidence, attracts new business relationships, may potentially allow entry into new contracts, and aids in effortlessly meeting regulatory compliances.

One tested strategy is implementing a thorough information security management system (ISMS) in line with the globally recognized International Organization for Standardization (ISO) 27001 standards to capitalize on these benefits. With Deloitte's skilled guidance, achieving this certification affirms your organization's commitment to maintaining stringent security controls, providing a continuous cycle of management, monitoring, and improvement. This can help safeguard your business and deliver a strong message about your dedication to information security, propelling your reputation in the market.

Achieving security through ISO 27001

While there is no ironclad solution to cybersecurity, organizations may take steps to safeguard their systems and reduce their exposure significantly. Leading practices involve developing or adopting a structured framework that provides the foundation for a strategic, broad, and repeatable approach to achieving information security across an organization. One such framework is ISO 27001, which is considered globally by many IT professionals,[1] academics, and regulators to be the global standard[2] for ISMS.

ISO 27001 was developed jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The standard specifies the life cycle characteristics of a strong ISMS, from its initial establishment and implementation to its ongoing maintenance and continuous improvement.

However, the specific requirements of your organization's ISMS are not defined by ISO 27001. Rather, the standard calls for a risk-based approach that takes into account the particular characteristics and needs of your organization, including such factors as industry, size, structure, legal and regulatory requirements, contractual obligations, culture, risk appetite, and business activities and objectives.

The ultimate goal of an effective ISMS is to preserve and enhance the confidentiality, integrity, and availability of information. Achieving this goal requires attention to much more than the secure configuration of IT systems; rather, it extends to people, processes, policies, and practices.

More than 90 security control requirements are identified in ISO 27001 allocated into four categories:

1. Organizational controls
2. People controls
3. Physical controls
4. Technological controls

Depending on your organization's specific needs, some of these categories may require more emphasis than others. A broad risk assessment process provides the basis for allocating resources and attention effectively.

Organizations that adopt ISO 27001 can be assessed and, if qualified, certified as compliant with the standard. Achieving the certification may not be easy, but an effective adoption of ISO 27001 can enhance security programs' quality assurance and can also provide marketplace recognition for competitive advantage[3]—particularly in today's world of heightened concerns over security.

Potential benefits of ISO 27001 implementation

Cybersecurity issues, prevalent since the inception of the internet, have gained acute criticality due to the continuous expansion of the IT universe and a concurrent increase in malicious actors. These challenges have reached such a magnitude that they influence business decisions, potentially determining whom organizations engage in or avoid in their business transactions.

The implementation of ISO 27001, the internationally recognized information security management standard, is a favorable solution in this landscape. ISO 27001 offers a practical framework for managing information security risks and safeguarding information assets. The benefits are essential and twofold: it may enhance IT security and positively influence overall business prospects and performance.

Applicable to various types of organizations, irrespective of size or sector, ISO 27001 implementation has critical advantages that make it a viable countermeasure to the ever-present cybersecurity issues.

1. Enhanced IT Security

The implementation of ISO 27001 denotes adopting an international standard for information security. This action facilitates organizations in identifying, managing, and reducing a multitude of threats to which their information is routinely exposed.

One of the principal interests of organizations adopting this standard is to utilize ISO 27001 as a catalyst for enhancing IT security, and rightly so, as the benefits it provides are expansive. Entities developing an ISMS that conforms to ISO 27001 may significantly improve information security in three primary dimensions: confidentiality, integrity, and availability.

Confidentiality helps ensure that sensitive information, including but not limited to customer data, intellectual property, financial records, health information, and legal documents, is shielded from unauthorized parties, whether external attackers or insider threats. It restricts access to such information to solely authorized individuals.

The dimension of integrity not only covers the accuracy and completeness of data but also includes the implementation of controls permitting only authorized alterations to the information. Furthermore, integrity extends to safeguarding data consistency throughout its life cycle, including periods when the data is in transit.

Availability, the third critical aspect, involves consistent maintenance and monitoring of the ISMS to support that information is accessible to authorized users and systems whenever required. This facet considers not just outages instigated by cyber incidents but also issues like hardware failures, server capacity limitations, scheduled maintenance, and human error, which could potentially affect the availability of information.

In sum, ISO 27001 serves as a strong and broad solution for enhancing an organization's information security management system.

2. Legal and regulatory

Beyond IT security enhancements, adherence to ISO 27001 may positively affect many other business areas. One prominent example is in the realm of legal and regulatory compliance. ISO 27001 may bolster adherence to data protection and privacy laws such as the European Union's General Data Protection Regulation (GDPR) and the California Privacy Rights Act (CPRA). It also supports standards like the Payment Card Industry Data Security Standard (PCI DSS).

Moreover, ISO 27001 either underpins, mirrors, or informs other IT security frameworks, encompassing the NIST Cybersecurity Framework (CSF) and the Trust Services Criteria of the System and Organization Controls (SOC) 2 framework.

This proves particularly beneficial in industries that handle sensitive or personal data and are bound by regulations necessitating certain levels of information security. Following the ISO 27001 standard may facilitate organizations in demonstrating compliance with these stipulations, thereby integrating enhanced information security with legal and regulatory adherence.

3. Risk management

ISO 27001 provides a sound framework for an effective risk management strategy, which may significantly boost an organization's resilience and adaptability.

The systematic approach of identifying, analyzing, and addressing information risks aids in safeguarding valuable data and intellectual property. This enhances the organization's ability to maintain business continuity, even during unexpected disruptions, allowing for smooth and uninterrupted operations.

Implementing ISO 27001's risk management can instill greater confidence among stakeholders, including clients, partners, and investors. When they perceive the organization's commitment to identifying and mitigating risks, it reinforces their trust and can lead to stronger business relationships.

The risk management component of ISO 27001 brings numerous benefits, from helping bolster business continuity and enhancing stakeholder trust to potentially avoiding financial losses and strengthening regulatory compliance. This leads to a more resilient, trustworthy, and competitive organization.

4. Cost savings

Implementing ISO 27001 significantly contributes to realizing tangible cost savings for businesses. It does this primarily through its focus on proactive identification and mitigation of potential threats and vulnerabilities.

The ability to anticipate and preemptively address security threats before they escalate into major incidents means organizations can avoid the often considerable financial implications of data breaches or system failures. These implications can range from immediate costs, such as crisis management, system recovery, and potential fines, to long-term costs, like customer loss, damage control, and brand reputation repair.

Furthermore, the systematic approach to risk management that ISO 27001 promotes can lead to more efficient use of resources. Assisting businesses to understand their risk landscape and prioritize their risk mitigation efforts endeavors to provide that resources are not wasted on low-impact threats but instead focused on managing high-impact risks. This leads to a more cost-effective allocation of resources, contributing to overall cost savings.

ISO 27001 can also result in indirect sales through improved stakeholder confidence and customer trust. When customers and partners trust an organization's commitment to information security, it can lead to increased business opportunities and long-term collaborations, thereby positively influencing the organization's bottom line.

Potential benefits of ISO 27001 certification

The ISO 27001 certification serves as a compelling testament to your organization's dedication to information security. This third-party endorsement affirms that your organization satisfies the requirements set by the ISO 27001 standard, thereby substantiating the efficacy of your ISMS. It may provide a seal of assurance to various stakeholders, including management, clients, and auditors, delivering several advantages:

1. Reputational

While it's uncommon to see organizations openly boasting about their impregnable cyber defenses or flawless data protection records in advertisements or news articles, mainly due to the risk of becoming targets for attacks, these assertions can be effectively conveyed in more controlled settings.

Behind the scenes, in contexts such as responses to Requests for Proposals (RFPs), business pitches, proposals, presentation decks, and meetings with current or prospective clients, organizations can safely highlight their recognized IT defenses, vigilant measures, and commitment to continuous improvement. Here, the risk of inviting unwanted attention from potential adversaries is minimal.

In these scenarios, claims of strong IT security are significantly reinforced by an ISO 27001 certification. This certification serves as a concrete testament to the organization's commitment to information security, providing documented proof of its dedication to managing and protecting data as per a globally recognized standard.

Achieving ISO 27001 certification bolsters the credibility of an organization's cybersecurity claims and enhances its overall image and reputation. It demonstrates that the organization has broad, internationally recognized processes in place to manage and safeguard its data, which can instill greater confidence in its stakeholders and promote business growth.

2. Business opportunities

In today's competitive and security-conscious business environment, ISO 27001 certification is becoming increasingly vital for securing contracts, particularly in public-sector work and heavily regulated industries. Such opportunities often present lucrative, long-term engagements, potentially leading to follow-up work and strengthening credentials for future bids.

Certain sectors or organizations even consider ISO 27001 certification a prerequisite for business engagement. Consequently, possessing this certification can open doors to new business opportunities that might have been inaccessible otherwise.

For clients, the ISO 27001 certification is a tangible symbol of an organization's steadfast commitment to data security. In our current data-centric era, this commitment can significantly enhance their trust in your organization. Moreover, it can provide a noteworthy competitive advantage by influencing clients' choices favorably, thereby boosting client acquisition and retention rates.

Thus, in a bid to win contracts, secure continuous business engagements, and gain a competitive edge, ISO 27001 certification emerges as a vital asset. It exemplifies an organization's commitment to data security, enhances its reputation, fosters client trust, and opens up opportunities for business growth.

3. Reduced need for client audits

ISO 27001 certification plays a multifaceted role in streamlining audits, easing regulatory compliance, and fostering client confidence, thereby contributing to efficient resource management.

When a business can showcase its ISO 27001 certification, clients may forego the need to conduct their own audits. This certification acts as an objective testimony that the organization has met an internationally recognized standard of information security, which can save both time and resources for the involved parties.

From an auditor's perspective, the development of an ISMS as a requirement of the ISO 27001 certification simplifies and accelerates an entity's ability to respond to questionnaires from customers and third parties as well as potentially questions from auditors. This third-party endorsement (achieving an ISO 27001 certification) signifies that a review of the organization's ISMS has already been done. This indication can save notable time and resources when fielding questions from outside parties. In addition, by preparing an ISMS, entities may be better organized and more prepared to address questions from an auditor, leading to a more efficient auditing process.

Additionally, ISO 27001 certification aids in maintaining regulatory compliance1,2. It serves as evidence that the organization is addressing its legal and contractual obligations related to information security by making regulatory considerations an integral part of the ISMS. This certification can assist in avoiding potential fines or penalties and affirm a positive standing with regulatory bodies.

An ISO 27001 certification may enhance operational efficiency by reducing the need for multiple audits, streamlining the auditing process, and helping maintain regulatory compliance, all while fostering trust among clients and regulatory bodies.

4. Continuous improvement

Obtaining an ISO 27001 certification is not just a one-time event but involves an ongoing process of regular audits, which may ensure consistent compliance with the standard and foster a culture of continuous improvement within the organization's ISMS.

The recurring audit process embedded in the ISO 27001 certification can be considered a cornerstone for maintaining the effectiveness and relevance of the organization's ISMS. Through these regular audits, potential areas of weakness or non-compliance are identified, providing valuable insights that help drive improvements in the system. This continual refinement makes the organization's ISMS more resilient to new and evolving threats.

The process of continual improvement can foster a proactive and security-oriented culture within the organization. It can heighten the awareness and understanding of information security across all levels of the organization, leading to more informed decisions and actions regarding data protection.

Preparing for certification

Preparing for and attaining ISO 27001 certification can be a complex and demanding process that can be obtainable with the right specialists. A phased approach will help organize efforts and activities toward building a sustainable, ongoing ISMS.

Readiness

- Confirming the implemented ISMS is integrated with existing management systems, processes, and culture.
- Identifying, understanding, and assessing current-state ISMS capabilities, processes, and controls.
- Augmenting those controls or implementing new ones, with a specific focus on compliance with ISO 27001.
- Building a sustainable, ongoing ISMS.

Remediation

- Developing remediation plans for deficiencies of relevant controls.
- Assigning ownership and responsibility and establishing a timeline and roadmap for remediation.

Internal assessment

- Teaming up with internal audit to define the requirements to assess the performance of the ISMS.
- Confirming the ISMS is effectively operated and maintained with evidence of continual improvements.

External compliance

Before pursuing ISO 27001 certification, be sure to:

- Check documentation to confirm that the management system elements are in compliance with the ISO 27001 standard.
- Confirm the controls implemented are operating effectively.

How Deloitte can help

Deloitte is a leader in providing integrated certification solutions for various standards, such as SOC, ISO, NIST, and other regulatory and contractual requirements. This is done by skillfully mapping requirements and controls; using a focused, risk-based approach; and finding similarities to increase efficiency and reduce duplication.

Deloitte helps organizations to align frameworks and reporting vehicles with existing compliance requirements. By using the ISO standards, which offer a well-known and respected system of guidelines and principles, Deloitte can help organizations connect different frameworks and regulations. For example, using ISO 27001, an international standard that provides a framework for ISMS, creates a structure in which the relevant security controls are selected to help meet applicable regulatory and compliance requirements. Examples of these applicable and potentially integrated regulatory requirements could include GDPR or the Health Insurance Portability and Accountability Act (HIPAA). It provides a common language for organizations, regardless of the specific compliance requirement, enabling them to show the effectiveness of their security measures in a universally accepted way.

Moreover, the ISO framework allows the identification of common controls across different compliance requirements, enabling the creation of a common controls framework. This is a vital component in aligning different compliance standards, eliminating the need to meet each requirement individually. Instead, the common controls framework helps organizations to implement an integrated, consistent, and efficient approach to their IT security and risk management processes. Therefore, by using ISO standards and developing a common controls framework, Deloitte can support organizations to achieve an effective, efficient, and streamlined route for multiple compliance objectives.

Deloitte can help organizations with different needs and maturity levels to follow the ISO 27001 framework, no matter how experienced they are. Deloitte is a global leader in IT risks, controls, and information security, and has skilled professionals who are experts in ISO frameworks. Our professionals have prestigious certifications, such as the CISA, CISSP, and ISO 27001 lead auditor; and have experience conducting IT audits in various industries. We have extensive experience in leading ISO readiness and control-gap assessments for large, diverse organizations. For entities that need more assistance, Deloitte has knowledgeable cybersecurity and ISO team members to help entities set up a security program according to the ISO 27001 standard, including creating policies and procedures, performing risk assessment, and providing audit support. For organizations that are getting ready for their ISO 27001 Certification or that are expanding an existing certification, Deloitte can provide ISO 27001 certification services. Deloitte's wide range of services and expertise in the field enable us to support organizations to address cybersecurity through a comprehensive framework and ultimately build trust with external stakeholders.

Contacts

Shannon Kramer
Principal
Tel. +1 (213) 996 5918
Email: skramer@deloitte.com

Daphne Lucas
Partner
Tel. +1 (403) 461 3629
Email: dalucas@deloitte.ca

Katherine Fortune Kaewert
Managing Director
Tel. +1 (323) 770 3717
Email: kfortune@deloitte.com

Valentyn Sysoiev
Senior Manager
Tel. +1 (403) 604 2422
Email: valsysoiev@deloitte.ca

Amit Pai
Manager
Tel. +1 (415) 783 5180
Email: ampai@deloitte.com

---

1. Microsoft, "ISO/IEC 27001:2013 Information Security Management Standards," December 7, 2023.
2. Michelle Drolet, "ISO 27001 certification: What it is and why you need it," *Forbes*, March 23, 2022.
3. Charu Pelnekar, "Planning for and Implementing ISO 27001," ISACA, July 1, 2011.
4. Microsoft, "ISO/IEC 27001:2013 Information Security Management Standards"; Drolet, "ISO 27001 certification: What it is and why you need it."