THE BUSINESS CASE FOR A CERTIFIED INFORMATION SECURITY MANAGEMENT SYSTEM

In today's world, data is currency. That means all the information that an organization uses to operate — such as financial data, intellectual property, or employee details — needs protection in the form of an information security management system (ISMS). Through an ISMS, information security is established through systematic controls of all processes, people, and technology that touch the data.

The benefits of a good ISMS can be huge and include the disposal of data, access to information, protocols for mobile telecommunications, and even the security of servers and other physical infrastructure. Organizations can also focus their ISMS on a specific type of data, such as consumer data, or they can address all data at all levels of the organization.

The goal of an ISMS is to ensure the continuity of the organization's processes, in case of a security breach, and to minimize the risk of a breach in the first place. However, for organizations in certain industries with high-value data in the cloud, such as pharmaceuticals, financial services, and utilities, an ISMS is often embedded as part of the culture.

ISO 27001 is the global standard that organizations can use to build an ISMS. The standard provides a scalable framework for documentation and internal improvement, such as corrective actions for systems acquisition, development and maintenance, cryptology controls, third-party supplier relationships, communication security, operations security, and the security of the physical environment.

The costs of an ineffective information security management system can be disastrous for an organization. Just in the last few years, some of the world's largest companies have suffered data breaches that have cost them millions of dollars. The volume of compromised records from these breaches is staggering: Yahoo! (3 billion), Marriott Bonvoy (383 million), Equifax (145 million), and Facebook (50 million).

Intangible Costs of Data Breaches

Besides the tangible loss of data, there are other ways a noncompliant ISMS can cost your business that may be less obvious, but they are just as destructive.

Your reputation can take a hit.

Companies that do their due diligence are likely going to shy away from organizations that have experienced an operational disruption, a data breach, or both. Ending up in the headlines about the latest security breach could dissuade prospects from working with you or might cause existing clients to reconsider their contract. Trying to mitigate reputational damage is also costly — hiring a crisis management team and implementing a strategy can cost millions.

You may see internal vulnerabilities.

Now that the global workforce has become accustomed to remote work, organizations are exposed to increased risk. Attackers are drawn to remote work environments because home networks are often not professionally managed and often involve outdated software or devices that are easier to breach. Besides attacks on remote-working infrastructure, organizations are also under threat by malicious insiders who gain access to the remote system, as well as by email scams that could trick employees who are not sufficiently trained to recognize these risks.

The customer perception of you may fall.

If a client is sharing proprietary information with your organization, what safeguards can you demonstrate to give them peace of mind? As clients demand greater transparency at every level of your business, companies must demonstrate measures and procedures to protect the confidentiality, availability, and integrity of client data. This means using industry best practices and regularly updating them to keep up with the latest threats.

How DEKRA Audit Helps

As previously discussed, an ISMS provides a strict set of policies, procedures, and technical controls that protect the integrity of an organization's data. DEKRA Audit can provide an unbiased assessment showing what previous internal audits may have missed.

ISO 27001 certification with DEKRA helps organizations comply with legal requirements and meet the needs of their customers. In addition to technical measures, ISO 27001 certification recognizes the importance of documentation associated with high-level information security management, which considers all relevant operational risks.

The certification process is a building block to help prevent and mitigate risk. Through it, your organization will gain the scalability to build on whatever your clients may require of you in the future. Our certification audit ensures that all procedures and policies are properly implemented. Your organization can then introduce a robust information security strategy that systematically meets internationally recognized standards, as well as the expectations of your customers, regulators, and partners.

Would you like more information?

Contact Us

DEKRA
On the safe side.

DEKRA Audit
dekra.us/audit
sales.us@dekra.com