27001 Academy

Applicability of ISO 27001 divided by industry

This is a list of the most common issues ISO 27001 helps to address. Some of the issues are typical for a particular industry, while other issues are relevant for all industries.

Industry	Issues to resolve	How ISO 27001 can help
All industries	Complying with a growing number of legal and regulatory requirements	ISO 27001 gives a very good framework for identifying all the requirements and defining a systematic way to comply with all of them; further, most of the information security legislation is based on ISO 27001 anyway.
All industries	Defending against a growing number of security incidents (i.e., hacker attacks, industrial espionage, embezzlements, hardware failures, etc.)	ISO 27001 provides a methodology to counter different types of threats – physical, cyber, internal, natural, etc. It is very good at merging different types of security activities into a single system.
All industries	Prioritizing investments in security	By assessing risks according to ISO 27001, you will have a clear picture of which safeguards must be implemented quickly.
All industries	Decreasing the cost of security incidents	The basic logic of ISO 27001 is to try to prevent incidents – in most cases, the cost of ISO 27001 implementation is much lower than the cost savings achieved because of incidents that were prevented.
All industries	Providing a tool for top management with which they can understand and control security issues	ISO 27001 has several sections dedicated to top management – how it has to be involved in managing information security, and which information it has to receive. Best of all is that ISO 27001 helps information security professionals start presenting their work in business language, which is the language understood by top executives.
All industries	Gaining competitive advantage in tenders	Many large companies, financial organizations, and government agencies prefer suppliers who are ISO 27001 certified.

Industry	Issues to resolve	How ISO 27001 can help
All industries	Defining security roles and responsibilities	ISO 27001 requires clear definition of who is responsible for what related to security; it also provides a natural way of identifying who should be responsible for which area.
IT companies (cloud providers, software developers, etc.)	Convincing customers their information is safe	By obtaining an ISO 27001 certificate, companies provide proof (issued by a certification body) that they protect the information in accordance with the leading information security standard.
Various service providers (online and offline)	Decreasing the penalties due to unavailability of their service	Implementation of ISO 27001 increases the level of resilience of an organization – as a consequence, the number of incidents is lower, and their duration is shorter.
Financial institutions	Finding the methodology for managing operational risk	Managing information security risks is part of the operational risk management; therefore, ISO 27001 provides a methodology for managing a larger part of operational risks.
Health organizations	Protecting the health records	ISO 27001 provides a methodology for protection of all kind of information – especially the information that is considered the most sensitive (e.g., customer or patient personal data).
High-tech companies	Protection of intellectual property	ISO 27001 provides a methodology for protection of all kind of information – especially the information that is considered the most sensitive (e.g., know-how, product development, etc.).
Consulting companies	Finding the methodology to help resolve their clients’ security issues	ISO 27001 provides step-by-step flow for consulting companies to implement information security safeguards in their clients’ companies.