ISO/IEC 27001 and Why It Matters for Your Business

JUSTIN SHERMAN

APR 8, 2018 | REGULATORY COMPLIANCE

ISO/IEC 27001 is a set of standards for infor
created by the International Organization for
Electrotechnical Commission, both independ
ISO/IEC 27001 is part of the broader ISO/IE
"[help] organizations keep information asset

As we'll discuss below, the 27001 specificati
internally auditing your security posture to e
points within ISO/IEC 27001 should play an
and information security.

What is ISO/IEC 2700

ISO/IEC 27001 provides standards for enterprises, governments and other organizations to use and maintain their information security management systems. As the ISO defines it, an ISMS is a systematic approach to securing sensitive company information. This can be anything from financial data to intellectual property to employee details to third-party information. And although it has the word 'system' in it, an ISMS isn't constrained to just technology. People and processes are an equally important part of securing information your business uses day-in and day-out.

Because the ISO is a non-governmental organization who writes general compliance principles – not how to implement them – the organization has no authority in and of itself to enforce "violations" of its standards. That said, many institutions that do have legal or regulatory authority rely on it for guidance. It has even been referred to as the "umbrella" for ISMS policies because of this fact.

WHO CARES?

If your business wants to comply with a specific set of industry standards, it's highly likely that ISO/IEC 27001 plays a role – or at least has similar high-level guidance. This is the case with everything from J-SOX in Japan to the Data Protection Directive (DPP) in Europe to the Payment Card Industry Data Security Standard (PCI DSS) in the United States. Many regulations that already apply to your organization can be aided by following the ISO/IEC 27001 guidelines.

You can also receive certifications directly on these standards through which an affiliate organization can certify your business' ISMS. Not only does this improve your brand image with clients, but it will also make you stand out from (or catch up with) your competitors. In today's market environment, cybersecurity is obviously a benefit. We can even imagine a certificate better attracting technical staff or incentivizing organizations to partner with you. If others can trust how you manage and secure your information, that's obviously a huge benefit for your business. ISO/IEC 27001 strengthens such trust.

(In the event none of that is convincing, check these statistics: by the end of 2016, well over 1.6 million ISO/IEC certificates were recorded worldwide – over 33,000 of them specifically for ISO/IEC 27001.)

WHAT EXACTLY DOES ISO/IEC 27001 SAY?

ISO/IEC 27001 uses a top-down, risk-based approach to information security management systems. One of its strongest features is that it's not technology-specific – it doesn't matter which devices or operating systems your business is running; you can still apply the standard's principles.

As already mentioned, the standard outlines high-level planning and processes. For instance, clause 6 deals with planning, which includes information security risk assessments and general security objectives; clause 8 deals with operation, including the execution of security goals and the regular testing of those goals (i.e. setting and evaluating benchmarks); and clause 9 focuses entirely on performance evaluation, including monitoring, analysis, internal audits, and management reviews.

The specification then dives into more specific detail on specific security techniques, from information exchange procedures to clock synchronization to password management. This

detail is designed to help businesses plan out their security policies in a checklist-oriented fashion.

For instance, the specification gives the following structure for access control policies:

1. Introduction
2. Policy Statement
3. Roles and Responsibilities
4. Information/Systems Access
5. User Registration/De-Registration
6. Secure Log-On Requirements
7. Physical Access Controls

As numerous security experts have pointed out, ISO/IEC 27001 compliance is important for everyone from IT staff all the way to CEOs. Businesses can use the standards to establish high-level security policies that then cascade down the organization, turning into more detailed procedures at each level (e.g. translating from policy goals into operational tasks into technical rules).

NEXT STEPS?

Much like many regulatory guidelines, ISO/IEC 27001 isn't exactly light reading. The documentation is long, detailed, and complex. It should be clear at this point, though, that such compliance is incredibly important.

You should turn to an ISO/IEC 27001 expert to audit your organization and understand the next steps to compliance. Filling existing gaps is especially important. It's obviously possible to do so yourself, but it'll likely take significantly more time and money than the alternative. Regardless, once you are compliant, invest resources in getting certified and *staying* certified. If there's one thing that we know for certain in cybersecurity, it's that stagnancy is death, so constantly reassessing policies and procedures to strengthen ISMS is essential.

Find out how Tripwire can help your business comply with ISO/IEC 27001 by getting touch with the team, here.

Editor's Note: *The opinions expressed in this guest author article are solely those of the contributor, and do not necessarily reflect those of Tripwire, Inc.*

TOPICS

ICS Security
Cloud
IT Security and Data Protection
Latest Security News
Regulatory Compliance
Government
Vulnerability Management

ABOUT

About
Contributors
Write for us
Privacy Policy
Tripwire.com

CONTACT US

US Headquarters
308 SW 2nd Ave Suite 400
Portland, OR 97204

Direct: 503.276.7500

International Offices

SEARCH