Whitepaper —
IT SECURITY ASSESSMENTS AND RISK MANAGEMENT

DEKRA

A path to a certified system by narrowing the risk footprint

by Neil Simons, Information Security Regional Excellence Manager, DEKRA Audits

There are many, diverse paths to information system security. The individuals within organizations that have been chartered to protect the availability, integrity, and security of the systems and data under the organization's control have numerous challenges to providing the protections the organization and its interested parties (such as customers, regulators, and partners) demand and expect. What is certain is that every organization that has data, communicates electronically as a course of business, or computes and/or stores information as a function of technology must take and maintain a protective position when it comes to Information Systems Security Management

Increasing Range of Threats

The nature and extent of Information Security threats is an ever-growing dynamic, as the best of human innovation meets the worst of human nature. As our technology and reliance on Information Systems increases in areas such as mobility, IoT (Internet of Things), and distributed integrated systems, so too does the threat to the integrity, security, and availability of these technologies. The volumes of information we rely upon to keep our lights on and homes warm is staggering, and potential interruptions to the normal course of doing business can have unimagined effects. The solution lies in all of us taking an active and accountable approach to information systems security management.

If it has connectivity, computes, stores, or processes data in any form, it is at significant risk. The liability for those of us whose roles are to protect the organization's reputation, information, and ability to conduct business are increasingly under scrutiny. Should failure occur, there can even be personal liability, so it is key to have a risk management plan to get through it. A certified Information Systems Management System (ISMS) can enable this type of risk management.

INDIVIDUAL INFORMATION

The Five Collections

In February 2019, an unknown actor released five databases of individual information, including Personal Identifying Information (names, addresses, social security numbers, dates of birth, credit card information, bank data, passwords, and more) for more than 2.1 billion individuals taken from over 800 attacks.

CORPORATE VIOLATION

Marriott Corporation

In December 2018, it was identified that for an extended period of years the corporate reservations and rewards programs databases within Marriott Corporate computing was breached. As a result, the EU fines to the corporation are anticipated to easily exceed $915M USD as just the fines for “failure to protect.” Fines under GDPR are based in corporate gross revenue.

What to Do?

With so many alternatives in how to prepare for, deter, detect, interrupt and potentially recover from a security violation, how is an organization to decide how to proceed or even where to start? Chances are, your organization has begun to address information system security matters with single-point solutions (such as two-factor authentication, endpoint protection, creating formal policy around password sharing, running a phishing awareness program. or selectively responding where and when a weakness or risk is identified.

This “point solution” approach is the most common method used in business today to attempt to meet to the problem in the market. It certainly makes you feel as though the organization is being protected — after all, the probability of any small, midsize, or even large organization being subject to an issue seems miniscule. The problem is that the “point solution” is really no solution at all. Each portion is a step in reducing the risk footprint of the organization deploying it, but the question to ask is: What is the strategy to meet future information security needs in an ever-evolving world of threats?

Each activity, response, program, control, or technology put in place to help protect the organization’s data reduces the security risk exposure. The objective is to make and maintain a minimal risk footprint for your organization, customers & suppliers. Moreover, the challenge is really to manage these activities, programs, and technologies on an ongoing basis, striving to continue to reduce risk in measurable and meaningful ways. A formal ISO 27001 Certified ISMS brings this solution into perspective and is attainable by nearly any organization.

IOT INCURSION

Target Corporation

In 2013, Target Corporation was penetrated and over 40 million customers’ credit card transaction data was harvested and then sold on the dark web. The actors attained access through a third-party HVAC vendor to the corporation, which exploited a weakness in internet firewall and network security through the connectivity to the monitoring of heating systems.

What is needed and the only true methodology to prove its value is an approach that manages the risk an organization faces in proportion and accordance with the effectiveness of the solutions deployed. A solution where the evolution of threat is mitigated by the continuous improvement of an evolving solution set that assures maximized benefit. This is where an Information Security Management System returns this value to the organization.

Managed System Approach

ISO (the International Standards Organization) provides a globally proven methodology and the internationally recognized standards against which a comprehensive management system can be scrutinized. With value-driven controls, virtually any organization of any size, in any industry can utilize this platform to efficiently and effectively reduce and manage their information security risk footprint. Under an established system, people are trained and informed, processes for detection, mitigation, and recovery are established and enhanced, and systems are strengthened through controlled, measurable determinations. At the same time, the system allows for informed decision-making, continuous improvement, and the framework for an organization to enhance its solution with additional controls (such as those needed to meet DoD, NIST or GDPR legal requirements). This can provide the level of assured governance to address the reduction of liability risk for the organization. Your system, if managed properly, can provide legal defensibility in the event of security failure.

How to Make an ISMS Work For You

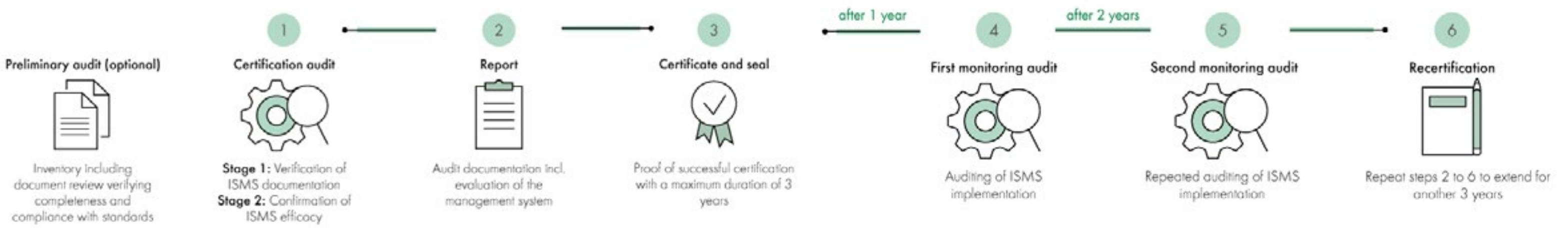
The establishment, maintenance, and certification of an ISO 27001 compliant ISMS can be involve significant investment of time, staffing, technology, and financial costs. However, the value such systems return are proven time and again in organizations worldwide The benefits are cumulative in terms of providing a consistent measures to reduce the risk of the organization in the areas where failure is most often experienced.

The ISO certification methodology is globally proven in bringing accountability and risk reduction for organizations across industries. The steps to gain the benefits of assurance and governance are straightforward, but each carries significant unqiue value. Chances are, you have already started down this path. By implementing point solutions and assigning resources (time, people, and money) to address risks as they are identified, the first steps to Information Security Management are already beneath your feet. The next step is to gain an understanding of your organization’s risk. The proven best approach to doing so is by engaging an informed expert to conduct an assessment and perhaps test against your perimeters and controls.

The assessment should include not only the factors behind the 114 controls indicated in the standard, but also the human and systematic processes and practices: the contingency plans, reporting, and programs for continuous improvement behind the security requirements as informed by your specific situation. An ISO ISMS offers a globally-accepted framework of consistency and accountability where each implementation is unique to the organization that executes it. Through an assessment, most organizations discover that they are already well along the path to certification without even knowing it.

Once an organization has the understanding of their risk and

ISO 27001 Certification Process

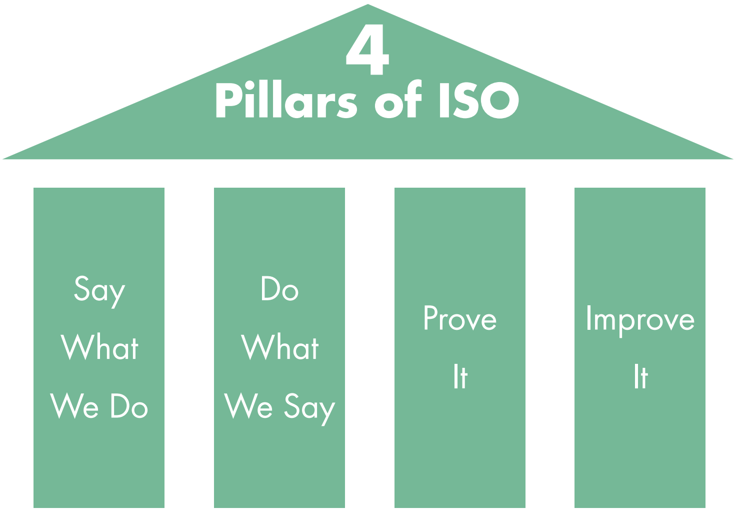

Preliminary audit (optional)
Inventory including document review verifying completeness and compliance with standards
1
Certification audit
Stage 1: Verification of ISMS documentation
Stage 2: Confirmation of ISMS efficacy
2
Report
Audit documentation incl. evaluation of the management system
3
Certificate and seal
Proof of successful certification with a maximum duration of 3 years
after 1 year
4
First monitoring audit
Auditing of ISMS implementation
after 2 years
5
Second monitoring audit
Repeated auditing of ISMS implementation
6
Recertification
Repeat steps 2 to 6 to extend for another 3 years

management opportunities, the IS Management System can be developed and introduced within the organization. Using the guidance provided under the ISO 27001 standard, the activities an organization would "want" to enact become actionable, and they then become second nature as the system matures. Standing up an ISO ISMS is a value-added activity for any organization: the more engaged the system becomes, not only does risk continuously get reduced, but the practices become defensible in the event of a failure. The likelihood and ability for an organization to survive or recover from a security failure increases with each reduction of risk attained. *That is value.*

At this point, an organization may choose to engage a certification body, such as DEKRA, to perform a pre-audit review of their system and its execution against the controls. This optional step may prove worthwhile, as there is no penalty for findings. This means that any issues found (non-conformities to the standard) will not count against certification. This gives the organization the opportunity to understand the strengths and weaknesses of their system and execution and then to address them ahead of the official certification audit.

The Certification Audits

Audits are an opportunity for improvement. Having an independent third party evaluate your Information Security Management System (ISMS) and the execution of your controls, policies, and practices against a governed standard proves to your customers, interested parties, and regulators that the organization is indeed performing its obligations in protecting operational, data, and systems security.



Systems are more likely to be available, data correct and trusted as the risk footprint has been and continues to be driven to an ever smaller, harder to hit, target for error or intention while increasing the ability to sustain operations and recover in the event of an event. There are two main components to an ISO 27001 certification audit: first, the evaluation of the ISMS against the ISO 27001 standard, and, second, the extensive dive into the controls defined under ISO 27002 (and managed under the 27001 system). Throughout this process, there will be no surprises or "gotcha". moments. From beginning to end, transparency is a key component of the process. After all, this involves saying what you do, doing what you say, proving it, and improving it going forward.

Once these two stages of audit have been completed by the organization and certifying body, the report will indicate any non-conformities (major or minor) that require correction to attain or maintain certification, as well as a listing of opportunities for improvement (which do not count against the attainment or maintenance of the organization's certification.)

When an organization attains certification, it is valid for a three-year period. In years two and three, full audits are not required. Instead, surveillance audits are planned and executed. These audits are abbreviated versions of the certification audit and are focussed on the areas of non-conformance previously documented and assuring continued compliance to the standards established and will go deeper into areas of concern if discovered. If non-conformities are discovered, organizations are given the opportunity at any stage of audit to satisfactorily address them to the certifying body's satisfaction before any negative action is taken. In the fourth year, a full audit is once again scheduled, in which all controls are evaluated for recertification.

Once the mystery is removed, it's a very straightforward process that virtually any organization in any industry may choose to pursue as they discover the risks faced within the organization. The existing processes, technologies, and people are incorporated into the ISMS to attain the reduction in the security risk footprint.

DEKRA Audits
Certification and training in ISO 9001, ISO 14001,
ISO 27001, ISO 50001, AS9100, and many more!

1120 Welsh Rd.,Suite 210, North Wales, PA 19454

1-800-768-5362
sales.us@dekra.com
www.dekra.us/audits