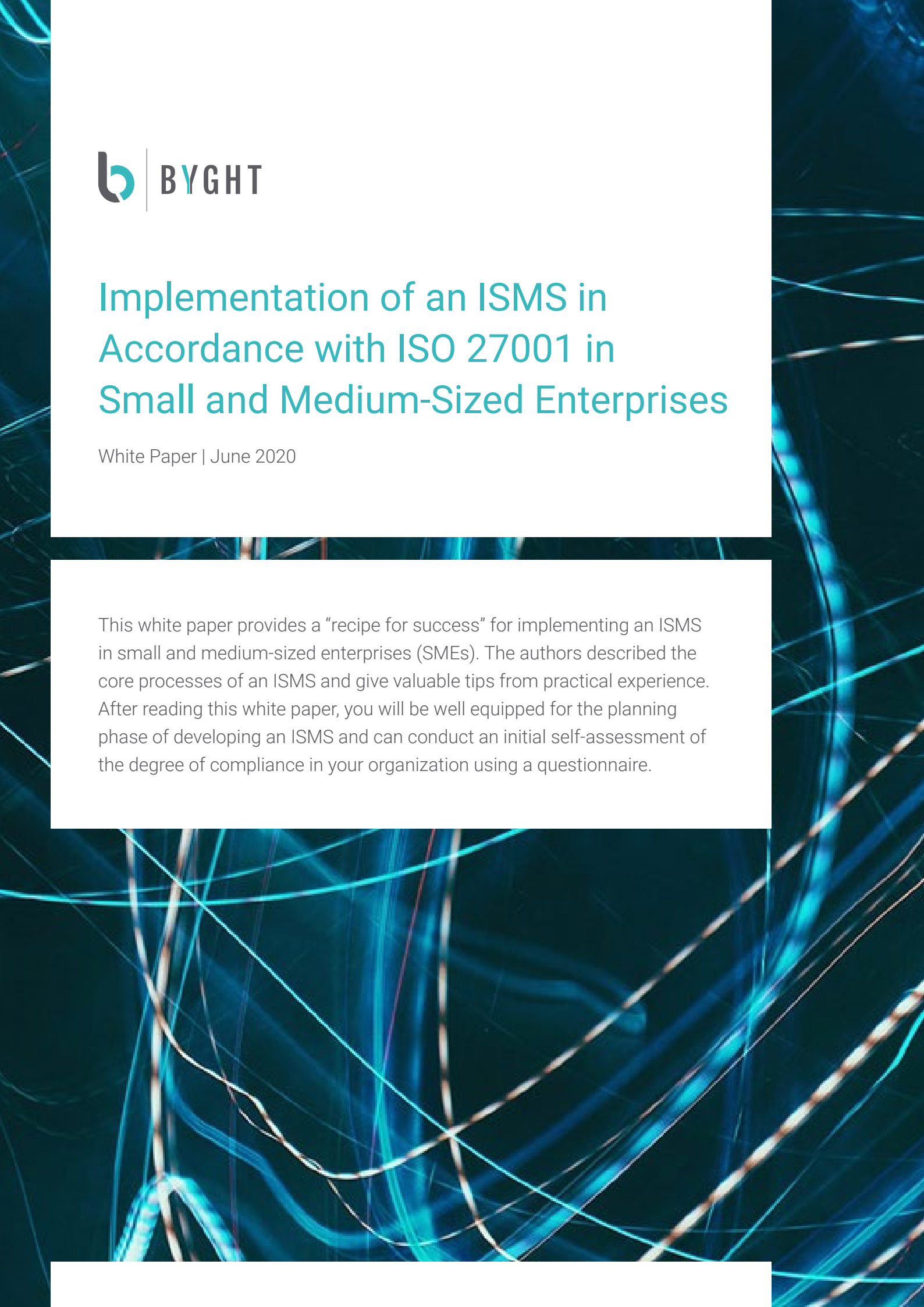


BYGHT

Implementation of an ISMS in Accordance with ISO 27001 in Small and Medium-Sized Enterprises

White Paper | June 2020

This white paper provides a “recipe for success” for implementing an ISMS in small and medium-sized enterprises (SMEs). The authors described the core processes of an ISMS and give valuable tips from practical experience. After reading this white paper, you will be well equipped for the planning phase of developing an ISMS and can conduct an initial self-assessment of the degree of compliance in your organization using a questionnaire.

CONTENTS

Introduction

A GOOD ISMS IS, ABOVE ALL, EFFECTIVE

Establishing a certification-ready ISMS requires, among other things, creating many new documents. Cultivating an awareness for security and establishing new processes within the company are also unavoidable. This can be especially challenging for SMEs, where resources are often in short supply.

The market for security experts who can take on the aforementioned tasks within the company is not overwhelmingly large – to put it positively. Costly external consulting services and complex, expensive ISMS tools seem unavoidable. In this white paper, we would like to demonstrate an alternative approach and provide SMEs with a "guiding light" to help them establish a suitable ISMS. Our motto here is: "As much as necessary, but as little as possible." That does not mean sacrificing an appropriate level of security. On the other hand, an ISMS should not get in the way of the core business, it should help shape the business to be as secure as possible.

It is important to start and not put off the seemingly insurmountable challenge that is ISO 27001 certification.

In principle, we rely on collaborative and agile methods when developing and operating an ISMS. Fewer complex tools, fewer individual makeshift solutions in huge Excel spreadsheets. It is important to start and not put off the seemingly insurmountable challenge that is ISO 27001 certification.

In the end, it is about continual improvement and not about achieving 100% at the certification audit. Because one thing is very clear: There is no such thing as 100% security. Above all, opportunities for improvement should be identified and implemented in a structured way when operating an ISMS. If this drive can be demonstrated to the auditor during the audit, a lot has already been achieved.

As much as necessary, but as little as possible

In addition to ISO 27001 certification, the constantly increasing number of threats is another good argument in favor of investing more time and consideration in the security structure of the company. When damages to the company, such as loss of image, data losses, and interruptions in business operations, can be reduced by implementing appropriate technical and organizational security measures, not only is the auditor happy but management is happy as well. Therefore, a good ISMS is, first and foremost, effective, and only then should we concern ourselves with meeting all the requirements laid out in the standard. A good auditor will see that and include it in their evaluation. Again, everything can still be improved – and this improvement can continue until the surveillance audit the next year.

There are, however, naturally some "hard facts" that are required in order to pass an ISO 27001 ISMS audit. The absolutely necessary and effective facts are presented and described in the following.

Contents and structure of ISO 27001

CHAPTERS 4–10

ISO 27001:2013 is an international standard describing the requirements for setting up, implementing, maintaining, and continually improving an ISMS.

The standard is divided into two sections: the obligatory management framework and Annex A. In contrast to the controls (measures) in Annex A of the standard, which can be deselected with justified reasoning as part of the Statement of Applicability (see below), implementing the requirements from Chapters 4–10 is mandatory. Using the following table, you can conduct an initial self-assessment of the degree of compliance in your organization.

Chapters 4–10

Chapters 1–3 of the standard cover basic topics which do not require implementation. Sections 4–10 must be implemented.

NOTE: Don't let the years listed in the version numbers of the standard confuse you. Sometimes ISO 27001:2015 or ISO 27001:2017 is also mentioned. In this case, reference is being made only to the German translations. Regardless of which number is stated, the basis for the certification is still the English version from 2013.

Chapter	Questions
4. Context of the organization	1. Have stakeholders been identified and their (potential) effect on the ISMS documented? 2. Has the scope of the ISMS been defined? 3. Have the legal requirements in the context of the ISMS been identified?
5. Leadership	1. Is management fulfilling its obligations by, among other things: • Establishing an information security strategy, • Integrating the ISMS into business processes, • Providing the necessary resources, • Measuring the effectiveness and continual improvement of the ISMS, and • Raising awareness among employees at all levels? 2. Has management adopted an information security policy and made it known? 3. Has management assigned roles, responsibilities, and authorizations within the ISMS and is management receiving the appropriate reports from these people?

Chapter	Questions
6. Planning	1. Have measures for handling the identified risks and opportunities been established? 2. Has a process for identifying, assessing, and treating information security risks been established? 3. Is a Statement of Applicability for Annex A documented? 4. Have the objectives of the ISMS been determined and has a plan to achieve them been established?
7. Support	1. Have the necessary resources for the ISMS been provided? 2. Do the relevant people have the required competencies to carry out their roles within the ISMS? 3. Has awareness been raised among all employees regarding • The ISMS policy, • Their duty to cooperate within the ISMS, and • The consequences of non-compliance with ISMS requirements? 4. Has internal and external communication been determined within the ISMS? 5. Is the information and evidence required by the standard for measuring the effectiveness of the ISMS documented and managed?
8. Operation	1. For planning and control, the organization must establish and document a series of processes. For this purpose, one process counts toward each of the following: • Meeting the information security requirements, • Controlling measures, • Controlling tasks that have been outsourced to service providers, and • Considering information security in planned changes. 2. Is a risk assessment performed regularly and in the event of significant updates? 3. Is risk treatment performed?
9. Reviewing the performance	1. Is there a process for monitoring the effectiveness of the ISMS? 2. Are regular internal audits performed? 3. Is there an audit program? 4. Is a management review performed regularly that takes into account at least the points contained in Chapter 9.3 of the standard?
10. Improvement	1. Is non-conformity with the requirements of the ISMS responded to with adequate measures? 2. Are the established measures assessed with regard to their necessity, introduced if necessary, and checked for effectiveness? 3. Is continual improvement ensured within the ISMS?

Contents and structure of ISO 27001

ANNEX A

In addition to these ten chapters, ISO/IEC 27001:2013 also includes Annex A, which contains 114 specific measures. These are divided into the following 14 categories:

Chapter		Number of measures
A.5	Information security policies	2
A.6	Organization of information security	7
A.7	Human resource security	6
A.8	Asset management	10
A.9	Access control	14
A.10	Cryptography	2
A.11	Physical and environmental security	15
A.12	Operations security	14
A.13	Communications security	7
A.14	System acquisition, development and maintenance	13
A.15	Supplier relationships	5
A.16	Information security incident management	7
A.17	Information security aspects of business continuity management	4
A.18	Compliance	8

Recipe for success

DOCUMENTATION AND ORGANIZATION

For an ISO 27001-certified ISMS, “documentation” means in particular creating information security policies. There are several mandatory policies that must be presented during an audit.

However, the standard does not contain information on the extent of these policies. On the contrary, the standard explicitly states that the extent of the documented information can differ from organization to organization. Decisive factors here are, in particular, the size of the company and the type of products and services. The person responsible for information security at an SME should always keep that in mind when it comes time to write the policies. Rather than focusing on extensive documents, it is more important that the requirements laid out in the policies are actually implemented within the company as a key part of the company culture. This is one aspect that can be checked easily during an audit and is therefore often checked for exactly this reason. A negative example is excessive security requirements for the company's own software development that are defined in a policy but cannot be complied with in practice. It is important to find a balance and to regularly review such documents and improve them if necessary.

MANDATORY POLICIES

- Information Security Policy
- Policy for risk management
- Policy for security incident management
- Policy for suppliers, service providers and contractors
- Policy for the classification and management of information
- Policy for secure IT operations
- Policy for human resources and access rights management
- General information security rules for all employees

Scope and Statement of Applicability

In addition to policies, there are many other documents specific to the standard that must be presented during an audit. **This includes, first of all, the** scope **and what is known as the** Statement of Applicability (SoA). Together they are the initial point of reference for the auditor, enabling them to form an image of the scope and the circumstances of the ISMS and of the company.

The Statement of Applicability is a document outlining all 114 controls from Annex A of ISO 27001. The Statement of Applicability serves to verify and document which controls are applied and to justify their selection. As an alternative, controls can also be deselected with justified reasoning if the requirements are not applicable to the scope of the ISMS. As an example, organizations can deselect the control *“A.14.2.1 Secure development policy”* if they do not develop software themselves. In practice, however, all the controls are often applied, and it is only sensible or possible to deselect controls in individual cases.

The requirements must be implemented within the company as a key part of the company culture.

Control		Applicability	Reason for deselection	Reason for selection	Linked documents
A.5	Information security policies				
A.5.1	Management direction for information security				
A.5.1.1	Policies for information security	✓		adopted best practices	Information Security Policy
A.5.1.2	Review of the policies for information security	✓		adopted best practices	Policy for the organization of information security
A.6	Organization of information security				
A.6.1	Internal organization				
A.6.1.1	Information security roles and responsibilities	✓		adopted best practices	Policy for the organization of information security
A.6.1.2	Segregation of duties	✓		adopted best practices	Policy for the organization of information security
A.6.1.3	Contact with authorities	✓		adopted best practices	Policy for information security
A.6.1.4	Contact with special interest groups	✓		adopted best practices	Policy for information security
A.6.1.5	Information security in project management	✓		adopted best practices	Policy for information security

Excerpt from a Statement of Applicability

In order to understand which of the 114 controls apply, it is important to think about the scope in advance. The scope, often referred to as the field of applicability, describes in writing the limits and applicability of the ISMS. It is typical in larger organizations to only certify individual business areas instead of the entire organization. But it is possible to exclude individual areas in smaller companies as well. For example, if an international site that only conducts sales activities is not covered by the ISMS, that must be described in the scope.

EXAMPLES OF INFORMATION SECURITY OBJECTIVES

- Sensitizing all employees to the topic of information security
- Ensuring data center access security
- Availability of 99.9% of data connections
- Early detection of security incidents
- Continual increase in the maturity of the ISMS
- Fulfilling customers' confidentiality requirements for their data
- Complete documentation of operating procedures to ensure availability
- Reliable support of business processes through information technology
- Ensuring the continuity of operations within the organization
- Continual identification, assessment, and treatment of risks to information security

The description of the scope is therefore also of interest to the company's own customers and other management system stakeholders, since it enables them to understand which areas and topics are covered by the ISMS and which are not.

In addition to the company's own customers, there are additional stakeholders who have certain expectations and requirements of the ISMS. This can include, for example, the company's employees, management, lawmakers, supervisory authorities, and service providers. All of these **stakeholders and their requirements** must be recorded in a separate document. For the sake of simplicity, this document can be a simple table. As with all the documents, the information must be checked regularly to ensure it is up to date and updated if necessary.

Another aspect that is worth considering is **the information security objectives**. The company strategy established by management serves as the basis for shaping and establishing the information security objectives. Especially at the beginning of the ISMS implementation phase, it is recommended to define a few information security objectives that make sense for the organization in question. These should strike a balance between implementation effort and usefulness. The established information security objectives should also be as easy to measure as possible.

In addition to the documents described, additional documents are also required for an audit. The following information box provides an overview of these documents.

MANDATORY ISMS DOCUMENTS

- **Scope** (also known as field of applicability)
- **Statement of Applicability (SoA)**
- **Stakeholders and their requirements**
- **Information security objectives**
- Planning of ISMS resources
- ISMS rolls and responsibilities
- Legal and regulatory requirements
- Internal and external communication within the ISMS
- Audit program
- Management report
- Risk treatment plan

Recipe for success

RISK MANAGEMENT

The risk management requirements pursuant to ISO 27001 are described in the management framework of the standard. 'In principle, creating a process for identifying and assessing information security risks is required in order to "prioritize the analyzed risks for risk treatment."

Of course, when repeated it must also lead to "consistent, applicable, and comparable results." To do so, it is important for the first step to be establishing a policy which lays out the company's risk management procedure. The policy should contain at least the following points.

Identify – assess – treat

ISO 27001 otherwise contains little about risk analysis methods, which provides a lot of freedom in implementation – but at the same time very little support. Help can be provided by the supplementary ISO 27005 or the method provided by the German Federal Office for Information Security (BSI) in its BSI IT-Grundschutz. For SMEs, a combination of these two methods can be a good option. This allows companies to benefit from the flexibility of the ISO standards and the templates and supporting information from the BSI. A process that is as lean as possible but still leads to "consistent, applicable, and comparable results" could look something like this:

CONTENTS OF THE POLICY FOR RISK MANAGEMENT

1. Risk identification
2. Risk assessment
3. Risk treatment
4. Reporting

Risk management process

Identify risks

First, think about which information, business processes, or IT systems are especially critical for your business operations. Then, ask your internal experts and also use threat catalogs, like the one from the BSI, to identify relevant risks.

Assess risks

The second step involves evaluating the identified risks. To do so, estimate the impact and probability for each risk.

The risk value results from the probability and impact and can be determined in what is known as a risk matrix.

Treat risks

A treatment strategy should be established and documented for the risks with the highest value.

Probability and impact

It is important to give thought in advance to an assessment model for risks. This is the only way to ensure comparable results and to prioritize the identified risks for risk treatment. The ISO 27001 standard does actually have rough guidelines for estimating the consequences of a risk occurring (impact) and the probability that the identified risks will occur. The standard does not go into more detail at this point.

A four-tier model for assessing the two influencing factors of impact and probability is common and also recommended by the BSI (see the following information box). In order to achieve comparability of the risks, they can be classified in a risk matrix. The risk value identified by this matrix indicates which risks should be prioritized for treatment.

A risk-based approach to treatment means tackling the greatest risks first. A sensible strategy would be to concentrate on the "high" and "very high" risks and consider the rest as accepted.

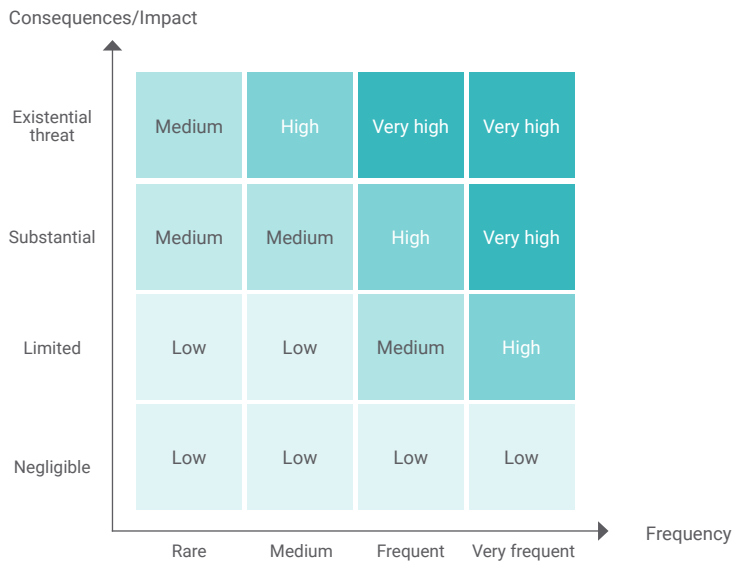
Classic possibilities for handling a risk are:

- **Risk avoidance** (discontinuation or adaptation of an activity)
- **Risk reduction** (identification of security measures)
- **Risk transfer** (i.e. insurance)
- **Risk acceptance** (management bears the risks)

For each of the high and very high risks, one of the aforementioned treatment options should be established in a risk treatment plan.

The results of risk management and the treatment plan should be part of the yearly ISMS reporting to management.

Risk matrix



Frequency/Description

Rare: According to present estimates, event could occur at most once every five years.

Medium: Event occurs once every five years to once a year.

Frequent: Event occurs once a year to once a month.

Very frequent: Event occurs several times a month.

Impact/Damages

Negligible: The effects of the damage are minimal and can be disregarded.

Limited: The effects of the damage are limited and manageable.

Substantial: The effects of the damage can be considerable.

Existential threat: The effects of the damage can reach an existentially threatening, catastrophic extent.

Source: BSI Standard 200-3 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_3.html (last accessed on May 4, 2020)

Recipe for success

INTERNAL AUDITING

Since internal audits are often not part of daily operations, we will first clarify several terms. The audit program is first and foremost. It is useful to create an audit plan and an audit report for the individual audits.

All upcoming audits are documented in the **audit program**. Supplier audits and external audits (e.g. certification audits or customer audits) should be listed here in addition to internal audits. To ensure the necessary support, have the audit program officially approved by management.

When the audit program is completed, the next step is preparing for the first internal audit. Preparation takes place in what is known as the **audit plan**. This serves, on the one hand, for planning (naming the audited area/object, the date, the time, and the rooms) and, on the other hand, for coordinating and informing all audit participants.

During the internal audit itself, the primary goal is to identify opportunities for improvement. Ensure a positive audit atmosphere right from the beginning in order to identify relevant opportunities for improvement. Quality is more important than quantity. When you are auditing your own colleagues, a certain amount of tact is called for. Even if the focus is on weaknesses/opportunities for improvement, positive insights from the audit should also definitely be included in the **audit report**.

The extent of an audit depends heavily on the area or object being audited. However, make sure you take at least half a day to look through documents, conduct interviews, and inspect IT systems. It is useful to plan in some time between sessions to sort out your thoughts and take notes for the audit report.

Think of internal audits as a tool to improve information security within the company. Use audit reports to give the findings the necessary emphasis. Start simple. Soon you will see that the internal audits become more routine each time.

Checklist for conducting internal audits

Activity	Timing
Creating the audit plan	4 weeks before audit
Coordinating with the area to be audited • Scheduling • Naming the contact persons	2–4 weeks before audit
Providing the final audit plan	2 weeks before audit
Conducting the audit	Audit
Coordinating measures and schedules with the audited area	2 weeks after audit
Providing the audit report	3 weeks after audit
Transferring the measures into the internal ticket system	4 weeks after audit

Recipe for success

INFORMATION SECURITY INCIDENTS

There is no such thing as 100% security. A security incident can cause, for example, information to not be available to the necessary extent or to fall into the wrong hands at any time.

Two examples: The online shop has to be shut down temporarily due to a cyberattack, or; an e-mail with important documents was sent to the wrong recipient.

The standard therefore prescribes several things for information security incidents, most importantly a systematic procedure for reporting and recording them. For this purpose, a process should be firmly established within the company that stipulates clearly when a security incident must be reported and to whom. It is crucial that all employees are aware of their reporting responsibility. This is the only way to ensure that incidents are responded to immediately.

It is crucial that all employees are aware of their reporting responsibility. This is the only way to ensure that incidents are responded to immediately.

It doesn't make sense to reinvent the wheel here. If reporting processes already exist within the company, e.g. a central IT help desk, these processes and locations should be taken into account when establishing the process. The help desk can then, for example, prioritize reported security incidents and consult specific people such as the information security officer or management.

The most important thing to keep in mind is that the process and reporting procedures are useless if employees do not know about them in the critical moment. Therefore, train your employees regularly and also use existing trainings to remind them about the reporting procedures.

Gaining knowledge

The process is established. Now what? Even if threatening incidents hopefully never occur, the process should not simply be put on a shelf and forgotten about. Because one requirement from the standard still remains: Learn from past incidents. Look at security incidents retrospectively and draw conclusions from them about what you can improve in the future. Security incidents happen. The goal, however, should be not to repeat the same mistakes.

Recipe for success

AWARENESS

At least since attacks such as “CEO fraud,” everyone is aware that sensitizing employees to information security issues to one of the most important defense mechanisms.

Appropriately, this is of course also required by ISO 27001. However, the standard allows for a lot of freedom in how this is implemented. As a minimum, it has become established that employees should participate in a training or, for example, an online training on information security at least once a year and that new employees also receive a corresponding training when they join the company.

There are many materials regarding information security best practices and tips available online, many of which are publicly accessible, for example from the BSI. It is also strongly recommended to use the trainings to present documents such as the Information Security Policy and important contents of other relevant policies to the employees. Also use the trainings to make employees aware of processes that are important for all of them, for example reporting procedures for information security incidents.

Finally, don’t forget to have everyone sign a participant list or keep other records documenting participation so you can provide evidence to the auditor that trainings took place.

Example of a poster informing employees of reporting procedures for security incidents.

Recipe for success

ISMS SELF-ASSESSMENT

Annex A of ISO 27001 includes a total of 114 measures. In principle, these must all be met unless you can argue in the Statement of Applicability that individual requirements do not apply to your company.

To ensure that all the relevant requirements from the standard are met, conducting a self-assessment is recommended. This has long been established as a best practice, even if it is not directly prescribed by the standard.

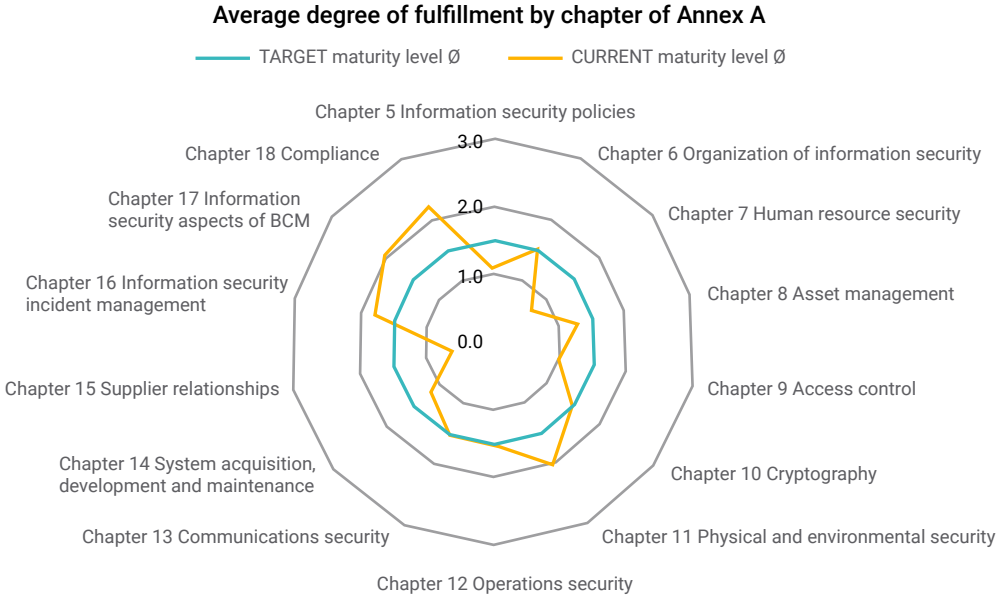
With a self-assessment, you evaluate your current status with respect to the individual measures. To do so, determine a degree of fulfillment, for example on a scale from 0 to 10, in percent, or using an established maturity model. It is best to also simultaneously record evidence that documents the fulfillment of a measure and to record necessary to-dos. The evidence can be very helpful as a reminder during a later certification audit so that you can present the corresponding documentation to the auditor when he/she asks for it.

In addition, integrate the self-assessment into the audit program as an "internal audit." Methodologically, the self-assessment differs from the classic audit, but it can also be invoked as a check and looks good during the certification audit.

Another advantage of self-assessments is that you can easily establish an easily measurable and effective KPI. You can, for example, calculate a maturity level or degree of implementation for each chapter of Annex A based on the self-assessment and visually present it in the following diagram. Also report this KPI to management and work with management to steer your ISO 27001 implementation project as well as additional improvements over the course of the upcoming certification cycles.

Evaluation of a self-assessment

The degree of fulfillment of the individual measures has been measured from 0 to 3 and visually presented here aggregated at the chapter level. The green line represents the TARGET maturity level and the orange line represents the CURRENT maturity level.



Recipe for success

REPORTING

In a healthy management system, management bears the responsibility and therefore makes crucial decisions, establishes the strategy, initiates important changes, and updates ISMS objectives.

To enable management to perform these tasks, they must receive regular reports on the status of the ISMS through what is known as a management review.
Such reporting to management should take place quarterly or twice a year, but at the very least once a year. Come to an agreement with management regarding the frequency, but make sure you don't overcommit at first.

Regarding what this review should look like, the standard directly specifies a series of contents to be included in the management review. This includes, for example, the status of measures, results of internal audits and risk management, and more (see ISO 27001, Chapter 9.3).

The contents for the management review can in theory be compiled quickly. However, they must be complete and available in a format that enables reporting. Digital tools can help store results and documentation in a central location and consolidate them into a report, if possible automatically.

In practice, it has been demonstrated that the contents are often already available but are often incomplete or not in a form in which they can be reported. Therefore, it should be ensured during ISMS activities throughout the year that certain topics can be transferred to the management review at the end with minimal effort. If the documentation is scattered in a sea of Word documents, Excel tables, and e-mails, this creates a lot of work and can result in an incomplete, inconsistent, or error-ridden report.

Therefore, while the processes are being carried out, ensure at the critical points that the results are already complete and centrally available. Doing this especially at the following points is recommended:

- When measuring the KPIs and information security objectives
- When controlling measures
- When documenting security incidents
- In risk management, for each risk and its treatment
- When documenting the results of internal audits
- When evaluating the self-assessment

In addition, there are also two things that definitely belong in the management review but are not generated in currently existing processes:

1. The response from stakeholders, for example when a customer, a government agency, or similar contacts you regarding information security.
2. The areas that have a significant influence on the ISMS. This could be, for example, new products or substantial changes to products, new core business processes, new sites, or a newly introduced security solution such as a SIEM solution.

If you take notes for yourself on these two topics during the reporting period, nothing stands in the way of a successful management review.
Once everything is combined into the management review, it is discussed with management. Take notes here, too, since the response from management, for example, regarding new or updated objectives, new measures, etc. also belongs in the management review. Add this in afterwards and have the management review signed by management.

Recipe for success

CONTINUAL IMPROVEMENT PROCESS (CIP)

Setting up an information security management system is not a one-time activity. The ISMS must be continually checked for suitability, adequacy, and effectiveness.

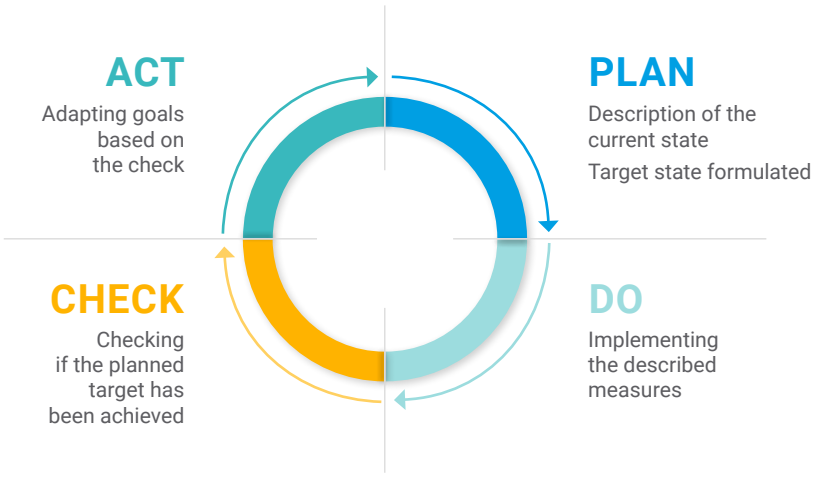
For successful certification, exactly that must be demonstrated to the auditor. Do I identify weaknesses in my information security? Is my ISMS and therefore information security being continually improved? Precisely these improvements are achieved by applying the aforementioned practices. Potential for improvement is identified, for example, in the risk analysis, the ISMS self-assessment, or lessons learned from security incidents. It is crucial that this potential for improvement is converted into measures and tracked.

If possible, use existing ticket systems or task planning tools to document responsibilities and target dates. For reporting, making the information security measures assessable and selectable using flags or tags is recommended. As an alternative to a ticket system, the most common ISMS systems on the market offer solutions to record and control the function and measures.

ISO 27001 does not require a concrete minimum level of information security, but it very clearly requires the management system and with it the security within the company to be subjected to a continual improvement process.

A concrete model for implementing continual improvement is not specified. However, the most commonly used model is the PDCA cycle (also known as the Deming cycle). According to this model, which follows a Plan-Do-Check-Act cycle, the planned (plan) and implemented (do) activities in the management are continually checked (check) for effectiveness and changed (act) if necessary.

PDCA Cycle



Summary

A SIGN OF SECURITY

An ISO 27001-certified ISMS is increasingly becoming a competitive advantage. With it, you make a strong statement that your information, data, and systems are secure. After all, as a forward-thinking business, you have to be able to rely on resilient IT. And not only you, but your customers as well.

Take advantage of the opportunity and think of the ISMS as a holistic tool for improving information security in your company one step at a time and allowing you to respond quickly and appropriately to threats and technical developments through the processes the system has put in place.

Don't be intimidated by the many requirements laid out in the standard. Often, many security measures already exist within the company and just need to be described for the audit. Also use existing processes to control measures and report incidents. You don't need to reinvent the wheel.

The initial certification in particular is about presenting the necessary documentation and providing evidence for the processes. The security measures from Annex A of the standard do not have to be implemented down to the letter. However, necessary measures need to be identified and a plan for how and when they will be implemented needs to be demonstrated.

ISMS solutions for SMEs

When implementing an ISMS, an appropriate ISMS tool can help, for example, to control risks, create documentation, and provide the company with a guide for establishing the management system. During the procurement process, make sure that the solution is also tailored toward SMEs. Too often, once they are in use ISMS solutions turn out to be too complex for SMEs in which information security is a one-man show.

In addition, the work required of the information security officer can be drastically reduced if the ISMS tool already contains templates for policies and other documents specific to the standard. In the ideal case, these documents only have to be adapted to the specific company context in order to be used. The person responsible for information security then has more time to implement the requirements within the company.

Don't be intimidated by the many requirements laid out in the standard. Also use existing processes. You don't need to reinvent the wheel.

To increase employees' acceptance of the policies, it makes sense to include affected employees at an early stage in the creation process. For example, have your own administrators read and comment on technical policies – and take their feedback seriously. Only then will the ISMS truly become a part of the company culture.

About Byght

WE ARE FORGING A NEW PATH – ALWAYS SMART, ALWAYS SIMPLE

JOHANNES MATTES

Long-time network and security engineer for a Hamburg internet service provider. Extensive experience as an information security officer, CISO, and security architect, always enjoys working with new methods.

Qualifications

- Information Security Officer - ISO (TÜV)
- ISMS Auditor/Lead Auditor ISO/IEC 27001
- CISSP

E-mail: johannes@byght.de | Phone: +49 (0) 40 - 66892413

LUCA GRAF

Previously worked as a consultant for small companies and international corporations in a variety of fields with a focus on holistic information security. Experience as an information security specialist in the financial sector, with a passion for organizational and process topics and governance.

Qualifications

- M.Sc. Global Management & Governance
- ISO (TÜV) & ISMS Auditor/Lead Auditor ISO/IEC 27001

E-mail: luca@byght.de | Phone: +49 (0) 40 - 66892613

BYGHT

Byght GmbH
Christians-Platz 8, 22844 Norderstedt, Germany

www.byght.de

Authors: Johannes Mattes, Alexander Luca Graf