DataGuard

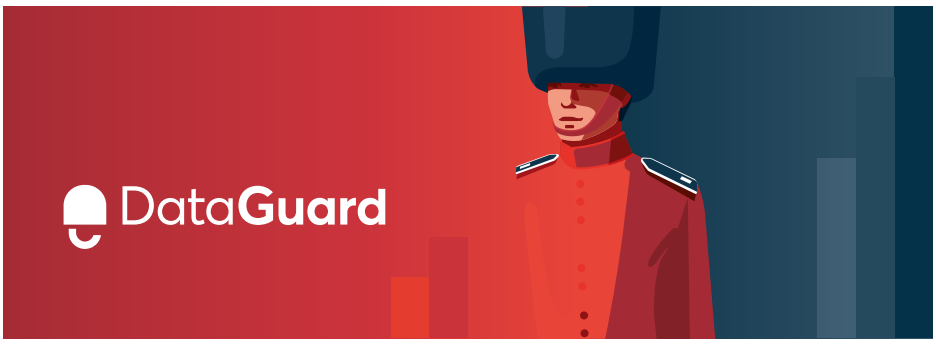
WHITEPAPER

# INFORMATION SECURITY FOR BEGINNERS

- What is information security?
- How can information assets be protected against cyber attacks and data leaks?
- Learn how an ISMS (information security management system) can protect your company

# ABOUT DATAGUARD

Combining human expertise and industry experience with a web-based platform, DataGuard is the end-to-end solution for managing privacy and information security. More than 2,000 customers trust our "Privacy-as-a-Service" and "InfoSec-as-a-Service" offerings to comply with regulations like the (UK) GDPR, achieve and retain certifications such as ISO 27001, or manage consents and preferences with ease. With over 150 employees in Munich, Berlin, and London, we help businesses to efficiently integrate compliance into their processes, thus achieving airtight compliance, efficient risk minimization, and added value through awareness, trust, and transparency.




**2,000+**

**CUSTOMERS**

**40 THOUSAND**

**PEOPLE TRAINED IN PRIVACY**

**30 MILLION**

**PEOPLE PROTECTED**

# CONTENTS

# INTRODUCTION

In 2019, an average company processed some 13.53 petabytes (1 petabyte = 1,000 terabytes) of data – that is 39% more than in 2018! (Source: Dell)
In today's world, every process depends on the right data being available. Data is increasingly exposed to complex risks, including physical threats such as fires and flooding, unauthorised access, cyberattacks and data leaks, not to mention the risk of data processing errors compromising its integrity.

Whenever data is lost, unavailable or stolen, companies can expect financial damage, reputational damage, and even legal consequences. As the amounts of data we deal with continue to increase alongside technological advances, so do the requirements necessary to keep them safe.

Due to the recent global pandemic the number of employees working from home accessing the intranet from their private domestic Wi-Fi, or even using their smartphone to run business apps, has increased drastically. The consequence of this: the potential threats and risks just keep increasing.

A study conducted by Dell showed that 82% of organisations surveyed suffered a disruptive event (such as data loss or system downtimes) in 2019. In 2018, that figure was just 76%. Further, a majority of those surveyed (68%) worry their organisation will experience a disruptive event within the next 12 months.

Information security is all about protecting data and corporate assets from unintentional, self-inflicted incidents as well as from prying hacker attacks.

CHAPTER 1

# AN INTRODUCTION TO INFORMATION SECURITY

Information security (or InfoSec for short) covers all the ways an organisation may protect their sensitive information, including policies and procedures to prevent unauthorised parties from accessing company information.
Information security is a growing, constantly evolving field that covers a wide range of topics. In addition to technical equipment, the security of a company's processes and business activities are a focal point as well as the qualification and trustworthiness of involved persons, whether staff, management, or suppliers.

**THIS CHAPTER COVERS:**

- Information security describes the protection of corporate assets following at least three objectives.
- Information security is gaining in importance as protecting corporate assets continues to become more vital while at the same time more challenging.
- Information security plays a role across all industries. It is especially important in highly software-driven and digital companies as well as for those in highly regulated industries.

## Definitions: Information security terms

**Information security** describes the protection of information assets following at least three objectives:

- Confidentiality → Ensuring that information can only be accessed by authorised persons
- Integrity → Ensuring that information is protected against tampering and corruption
- Availability → Ensuring information is available at all times and can be restored if problems occur

While there are some international standards and norms that define the requirements for information security and the measures necessary to ensure it, there is no legally binding framework in place.

In terms of information security, information assets include all data, information and goods that represent added value to an organisation's operations and are vital to achieving business objectives.

For example:

- Hardware, software, data, databases, processes, and applications within an information system
- Devices, clouds, and other components of IT environments that process information
- Applications, general support systems (GSSs), staff, equipment, and collective system groups

To further define information security, it is helpful to take a closer look at the terms *data, information, and knowledge.*


**Data:** Whether analogue or digital, the word 'data' is technically the plural of 'datum' and can refer to any character, value, or quantity with factual or statistical quality. In English, it is a mass noun, like *'rice'* – which means it is uncountable and treated as a singular. For instance, *175.98 cm* is a piece of data. Data forms the basis of information and knowledge. For that reason, data security is a frequently discussed element of information security: without safe data, there can be no safe information.

**Information:** Information arises when data is put into a specific context, i.e., through syntax or correlation. The piece of data *'175.98 cm'* turns into a piece of information when it is included in a table in a row labelled 'body height'. Spelled out, the piece of information would thus read: *the body height is 175.98 cm*.

**Knowledge:** Knowledge is derived from pieces of information that are associated with one another and processed. *'John Doe is 175.98 cm tall'* is an example of knowledge one might have about a certain person.

So, when we discuss data availability and knowledge management below, we are simply looking at knowledge in its different levels of abstraction.

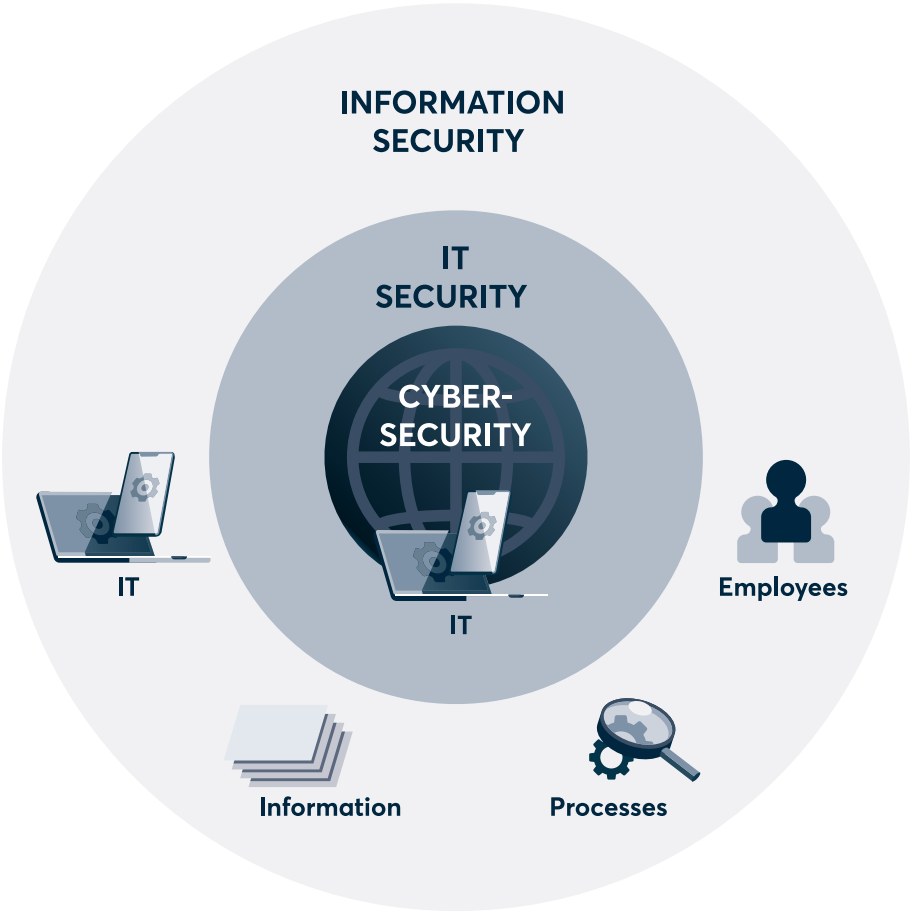
# Don't get it confused: information security vs cybersecurity vs IT security

The term **IT security** is sometimes misleadingly used as a synonym for information security or cybersecurity. The difference: **information security** focuses on the protection of information. The information itself is the asset. It exists independently of IT or cyberspace and requires protection in all its forms – whether as a file bursting with printouts or unique company knowhow in your employees' brains.

**IT security** refers to the IT infrastructure: everything from computers, servers, clouds and even wiring and the like must be secure and protected from access by unauthorised persons. The purpose of an IT system is to transport and process information.

Finally, **cybersecurity** should be understood as a branch of IT security. It pertains to the protection of information in cyberspace, i.e., information security on the web.

→ Every IT security measure contributes to information security, but not vice versa. Not every issue surrounding information security also relates to IT security. For example, effective HR Polices can provide information security and will not depend upon an IT solution.



# Information security is gaining in importance

In recent years, numerous laws that directly deal with information security were put into place or updated. This in in part due to the high pace of technological progress and digitisation that pose novel risks to today's business community.

At the same time, awareness is growing among consumers, B2B customers, investors, employees, and other stakeholders. Investors subject companies to an intensive **due diligence process**, during which their information security is put under the microscope. Certifications such as ISO 27001 and TISAX® are playing an increasingly crucial role in the competition for distributors and customers.

**Note:** In industry jargon, the international standard in question is commonly referred to as ISO 27001. But its technically correct name is ISO/IEC 27001:2013.

### Information security is crucial in these industries

Each and every company should take information security seriously, regardless of the company's industry or size. But the topic is especially important in highly software-driven and digital companies as well as for those in highly regulated industries. Take the health care market for instance: the nature of the market demands that companies meet strict minimum standards for information security – for example, to ensure doctor-patient confidentiality.

In the automotive industry, information security is highly related to the product: vehicles are so complex and so many parties are involved in manufacturing that each product must pass through highly regulated approval processes before it can take to the roads. This means that all the actors involved in the supply chain must meet the requirements, from corporations and suppliers of medium-sized parts to advertising agencies and freelance consultants. Any actor involved in the supply chain is required to meet the industry-specific requirements for information security, no exception.

CHAPTER 2

# INFORMATION SECURITY OBJECTIVES

The three objectives of information security are:

- Confidentiality
- Integrity
- Availability

When a company implements protective measures for information security, they should always follow at least one of these objectives.

**THIS CHAPTER COVERS:**

- The three main objectives of information security are confidentiality, integrity, and availability.
- Extended models include non-repudiation, accountability, and authenticity.

## Confidentiality

'I'm going to tell you something in confidence.' Everyone knows what that means: Don't share what you are about to hear. Confidentiality in terms of information means the same. Information must be protected from unauthorised access by third parties. Who is authorised must be clearly defined.

Measures that seek to protect the confidentiality of information include:

- Encryption of data
- User access control
- Physical and environmental security
- Operational security
- Communications security

# Integrity

A person with integrity is one who is reliable. In terms of information security, integrity means that data or information are protected from being changed (either unintentionally or by unauthorised parties) and are in this way 'reliable'. It's clear to see how confidentiality is a closely related concept, i.e., protecting data/information from unauthorised access. But integrity primarily means protection against unintentional changes. Unintentional changes are more likely occur due to defective systems and processes than through human error.

Measures that seek to protect the integrity of information include:

- User access control
- Asset management
- System acquisition, development, and maintenance

# Availability

What good is confidential and reliable data if it is unavailable to those who need it when they need it? As an objective in information security, availability means building the technological infrastructure that makes data and information available. Or in simple terms: preventing system failure. If data is lost, a further task of information security is to restore operationality as soon as possible – for example through backups.

Measures that seek to protect the availability of information include:

- Risk analysis
- System acquisition, development, and maintenance
- Incident management
- Business continuity management

# The three extended objectives of information security: non-repudiation, accountability, and authenticity

If data is changed, the objectives of non-repudiation and accountability make it possible to attribute the changes in question to one single, indisputable identity – in the best case, an individual person. This can only be guaranteed through end-to-end identity management and change histories – for example, most CRM systems keep a log of when changes are made to a contact and by whom. Thus, multiple users sharing a license results in a lack of non-repudiation and accountability.

The third extended objective, authenticity, describes how real information is and can be determined by a piece of information's characteristics. In order to provide authenticity you would be looking to have transparency as to its source or provenance. Where was the information created, who has "processed" it or added to it?

CHAPTER 3

# THREATS TO INFORMATION SECURITY

When they hear 'threats to information security', most people immediately think of cyber attacks, organised crime, and espionage. And it's true: criminal attacks – in particular on digital systems – pose a serious threat with far-reaching consequences:

In 2020/2021 alone, theft, espionage, and sabotage cost German companies 223 billion euros. In 2018/2019, the figure was only 103 billion euros. According to a Bitkom survey, nine out of ten responding companies had been directly affected by cyber attacks.

And it's not exclusively bad actors, even a company's own employees represent a threat to information security, intentionally or by accident. Further threats include defective systems and processes as well as physical threats through natural disasters.

**THIS CHAPTER COVERS:**

- Information security can be compromised through natural forces; a company's own employees, systems, and processes; and cyber criminality.
- When hackers strike, it's usually to blackmail companies into paying a ransom or simply steal data necessary to launch further hacks. Cyber criminals only rarely seek to gain intellectual property.
- The greatest vulnerabilities for hacker attacks are posed by social engineering, insecure passwords, remote work, shadow IT and insecure cloud solutions.

## Physical threats

It is March of 2021 – in a five-story OVH data centre in Strasbourg, a fire breaks out. 12,000 servers go up in flames, more than 100,000 websites across the world crash and data lost in the blaze will never be recovered. The economic consequences are devastating.
What happened? Many of OVH's customers had neglected to ensure that their data was redundant. In layman's terms, there were no copies, and the companies were as at a loss as the hapless customer at a computer store when prompted to hand over the regular backups they surely perform.

At the end of the day, there is no guarantee that a data centre is safe from fire, water damage or other forces of nature. Thus, one task of information security is business continuity management. Companies must be able to remain operational, even in the event that data stored in a data centre is lost – a risk that any good risk analysis should discover.  When choosing a data centre or a cloud solution that process business-critical information, one crucial factor in terms of information security is a high uptime guarantee.

## Threats due to employees

A **2019 KPMG study** has shown that carelessness, poor training and lack of awareness among employees are among the most frequently mentioned factors that facilitate cyber criminality. And even if the majority of hacks can be laid at the feet of external actors, 48% of companies surveyed recognise that their own employees pose a potential threat.

Cases of data theft by (former) employees rarely make it into the public awareness. On the one hand, such cases are difficult to prove. On the other, it is in a company's interest not to publicise such news – except where required by data privacy legislation.

Typically, a company is most vulnerable to employee data theft during the onboarding and offboarding processes. New employees who will have extensive access to sensitive company data (e.g., IT heads or higher management) should be subjected to background checks. When an employee leaves a company, they should always hand back any information assets in their possession. In theory at least. Whether an employee smuggles customer data out on a flash drive on their last day at work is difficult to prevent in practice.

Often, however, it is not even intentional data theft that makes employees a threat to information security. Instead, it is the 'human factor' itself that poses the greatest vulnerability, in particular in cases of insufficient training resulting in lack of awareness and staff taking risky shortcuts in order to meet deadlines to complete tasks or sometimes plain carelessness.

## Threats due to systems and processes

Unless the systems for storing and processing data are fit for purpose, the objectives of information security will always remain out of reach. Take the objective of integrity for example: to ensure the integrity of a company's data, its IT systems must make it impossible that data are manipulated without being noticed.

For example, if your company uses a tool that makes it possible to change the number of an outgoing invoice after it's already been submitted, this might result in incoming payments being allocated to the wrong account. It would be better if the invoicing tool you use prevents data such as the invoice number from being changed once an invoice is issued.

Even self-programmed solutions can be prone to error when data is mistakenly overwritten, duplicated or otherwise modified. When that happens, your data no longer meets the integrity requirement. So, your IT system has to function effectively, alone and alongside other systems.

## Threats due to cyber criminality

'Oops, your files have been encrypted!'

It is the spring of 2017. Countless people around the world have just been notified by this aggravating message on their computer screens that they have fallen victim to a ransomware attack. Victims are informed that they can ransom their data back for between $300–$600 in bitcoin. But the aptly named 'WannaCry' crypto virus includes a timer counting down the hours and minutes until all the data on the infected device is deleted forever.

In under three days, **WannaCry** infected more than 200,000 private and company machines in more than 150 countries. In Germany, the Deutsche Bahn had to restrict rail operation because information screens at stations ceased working properly. Some UK NHS hospitals suddenly found health data encrypted and a number of ambulances were diverted, resulting in life-threatening situations for patients across the UK.

WannaCry exploited a vulnerability in a Windows's protocol for printer and file sharing – any computer that had not been updated to the latest version of the operating system was vulnerable.

Whether a company paid the ransom or not, the majority of victims did not see their data again until Microsoft released an emergency patch to shut down the ransomware on all infected systems.

The ransomware was only able to target outdated operating systems. If victims had effective patch management plans in place to ensure the latest Windows update were installed within an acceptable time period from their release since the vulnerability, which was known to Microsoft at the time, this would have been solved. One task of information security lies in the procurement, development, and maintenance of systems. This includes ensuring that all company employees have installed the latest and most secure version of whatever operating system they use.

### What hackers want

Ransomware attacks like the WannaCry incident are an increasingly popular strategy among cybercriminals – up 358% since 2018/19! Losing information such as customer or corporate data through ransomware attacks can cripple a company for hours, days or even weeks, causing damage both to its ability to compete and its reputation.

The goal of most cyberattacks is to pressure victims into paying a ransom for stolen or encrypted data sets. Hackers who steal email login data can use it to launch additional phishing attacks and heist sensitive information from the victim's colleagues and business partners. In another increasingly popular strategy known as 'crypto jacking', the criminal hijacks an unwitting victim's computing power, mining cryptocurrency to line their own pockets.

A 2021 Bitkom study shows that hackers also go after intellectual property. As a related **press release** states: 'Intellectual property like patents or research information were stolen from 18 per cent – an increase of 11 per cent compared to the years 2018–2019. [...] For an innovation-driven economy like Germany's, theft of intellectual property can have dire consequences.'

## Typical gateways for hacker attacks

### #1 Social engineering – the human factor

Social engineering is a blanket term for a number of malicious activities that seek to exploit every system's greatest vulnerability: the user. Hackers might build trust with a company's employees or blackmail them, anything to get their hands on sensitive information such as passwords and credit card information. Typically, communication is digital. Cybercriminals pose as IT support or even the CEO and demand that employees hand over important information stat. (**Here is a detailed Forbes article with helpful tips on guarding against so-called 'CEO fraud'**.)

Once the fraudster succeeds in infusing the situation with stress, overwhelmed employees often lower their guards and might fail to notice that the sender's email address looks odd or the data request itself smells 'phishy'.

### #2 Weak passwords

'123456', 'password1' and 'abc123' – weak yet often-used passwords such as these leave the door open to password spraying attacks, where hackers use software to try to guess a user's password by entering commonly used character combinations. Passwords that have a connection to the user's personal life (e.g., the name of a partner, pet, or favourite vacation destination) make it even easier for hackers with intimate knowledge of their victim to guess their password.

It's no surprise that hackers are so keen on finding out your password. After all, it can be the key not only to your personal information but also to company data such as CRM data banks, email inboxes and more.

### #3 Shadow IT

Shadow IT refers to hardware and software used by employees without the knowledge of the IT department. Typical examples include browser plug-ins and messaging clients. Since they're not part of the company's official IT system, solutions like this are unprotected by the IT security concept. Despite this, insecure solutions are widely used and a potential attack vector for malware or crypto jacking.

### #4 Home office (remote work)

**It is by no means a coincidence that 2020 was a record-breaking year for cyber attacks.** Many companies were relying on processes and systems that simply weren't equipped for the entire workforce to be sent to work at home in short order. As mentioned above, ransomware attacks proved an especially successful strategy. Typical attack vectors for ransomware attacks are infected email attachments, infected downloads, and social engineering attacks.

### #5 Lack of due diligence in introducing cloud services

In a **2019 IDG Research Services study**, about half of respondents (47%) reported cyberattacks on their cloud services. And as attacks of this kind have been on the rise for years, it might seem a reasonable assumption that cloud services put companies at increased risk. But that's not exactly right. The rising number of attacks is simply an expression of the increasing popularity and use of cloud services. Indeed, cloud services are often more secure than internally hosted IT, as they are subject to regular security updates.

But not all clouds are created equal. Some providers and solutions are fraught with breaches with respect to information security and data privacy. There is no way around it – before you start working with a new cloud service provider, due diligence is essential: is the provider's information security management system certified? How has the service provider held up under penetration testing? What contractual guarantees does the service provider offer? Ensure that your SLA (Service Level Agreements) are reflecting the service your organization requires.

CHAPTER 4

# BUILDING AN INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

When it comes to information security, an ISMS ensures transparency, repeatable processes and measurable KPIs. Put simply, a well-implemented ISMS means there are no more information security surprises lurking around the corner. Benjamin Franklin is said to have made the following statement that sums up the inverse point of an ISMS nicely: "When you fail to prepare, you prepare to fail."

Putting an ISMS in place can only be successful when management truly backs the undertaking and provides the necessary resources. Mere lip service won't do. A company's Information Security Officer (ISO) needs the trust of management, who in turn must give the ISO the ability to act. Without it, the ISO can't bring together the people, tools, and processes necessary to ensure information security.

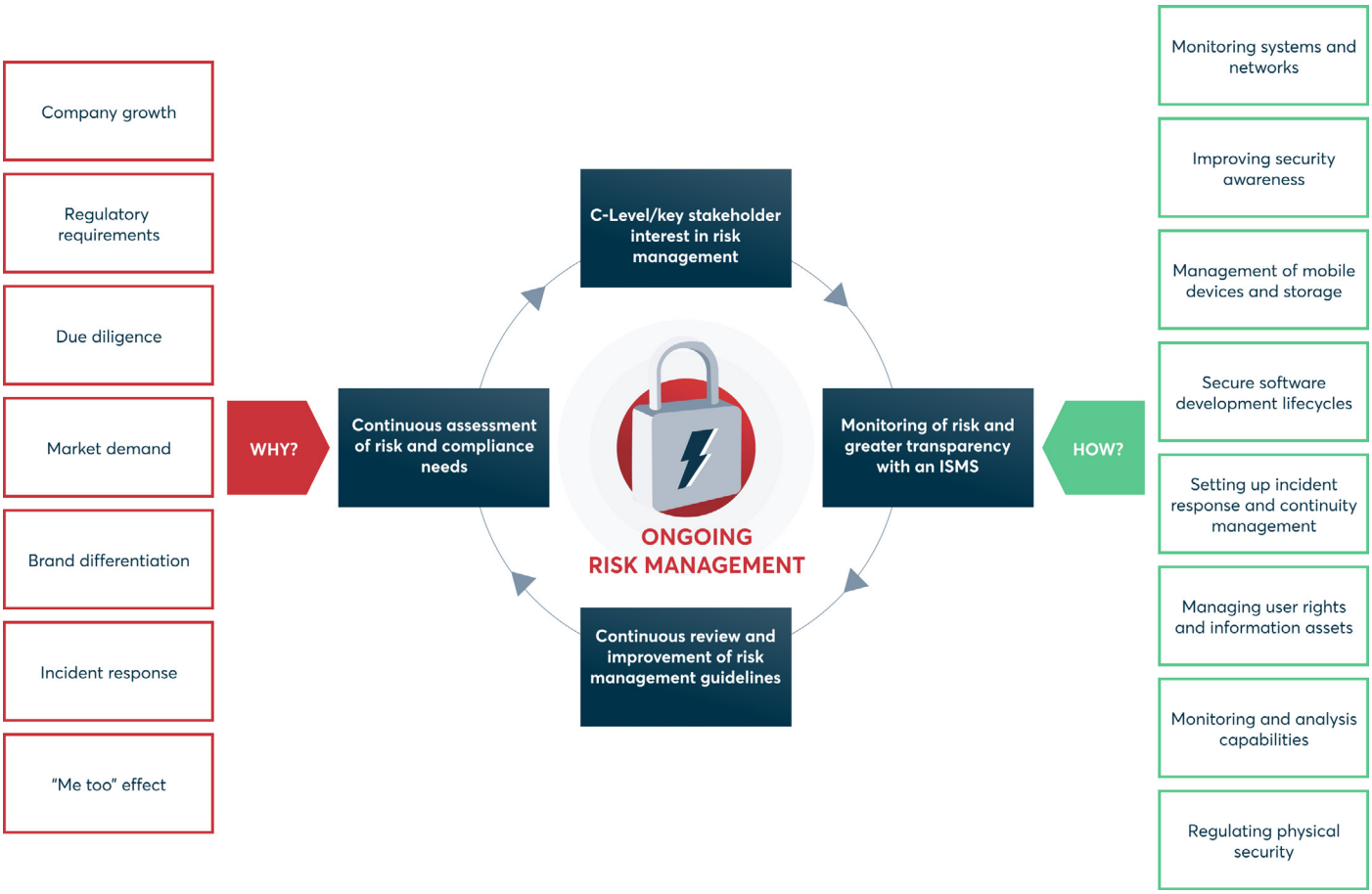
## THIS CHAPTER COVERS :

- An ISMS makes it easier for companies to calculate and control information security risks.
- In industries with complex, regulated supply chains such as automotive or health care, an ISMS is a key requirement for market participation.
- Moreover, while rarely a legal requirement, an ISMS is highly valuable and useful to all companies.
- Management is always responsible for introducing and running an ISMS (top-down approach).
- How the ISMS will look with respect to implementation and scope will depend on an organisation's individual appetite for risk.

# The goal of an ISMS

Management systems for information security in companies are process-oriented and – as the name suggests – always a management-level responsibility. That is, an ISMS follows a top-down strategy. Management can delegate tasks related to implementation, but not the responsibility itself. Management can match the level of measures and mechanisms that they implement to their level of motivation, scaling the degree of information security in their company processes correspondingly. After implementation, management must continue checking and controlling the scope, intensity, and progress of individual measures on an ongoing basis.

Put simply, the goal of an ISMS is not to ensure maximum information security. Instead, an ISMS allows an organisation to achieve their desired level of information security. The decisive factor here is the organisation's appetite for risk. A company must have an overview of the information in its possession and the risks it is exposed to – as well as what it would cost if the risks materialised. On the basis of this knowledge, management can decide by how much said risks should be reduced through an ISMS. So ultimately, an ISMS is an instrument of financial risk management.



There are many good reasons to implement an ISMS. For example, if your business operates in a largely unregulated market, you can stand out to target customers by adhering to strict standards for information security and thus gain a competitive edge. In any case, an ISMS will increase the value of organisations because without one, companies don't have a clear overview of their own processes and information assets. When looking for investors, an ISMS will pay off instantly: Without one, it is possible to carry out **due diligence** to a limited extent only.

Forces inherent to the market you operate in also play a role. Take the automotive industry for example: for a company to enter this highly regulated market and act as a supplier in the supply chain, it must meet the industry requirements and have an ISMS in place. Suffering an information security incident is itself enough of a reason to act and implement an ISMS in your company. But it goes without saying that it would be better if it never even had to come to that in the first place.

## Implementing an ISMS in your company

The requirements for establishing, implementing, maintaining, and continuously improving an ISMS are specified in the international standard ISO 27001. In terms of structure and operation, an ISMS basically follows a traditional PDCA cycle. (PDCA stands for plan, do, check, act.)

1. **Create an ISMS guideline.** Why do we, as a company, want to set up an ISMS? What are our goals? How will we organise our ISMS? Who will play the part of Information Security Officer (ISO), what resources will they have at their disposal, what measures will they put in place?

2. **Identify and classify assets.** What assets/information do we want to protect? How sensitive are these assets/this information anyway? In the automotive industry, for example, drawings of a vehicle in the planning stage would be significantly more sensitive than photos of a test model in a road test just prior to roll-out.

3. **Establish ISMS organisation and risk management structures.** What tools do we want to use? What financial and staffing resources will the ISO have at their disposal? What structures should the ISO establish?

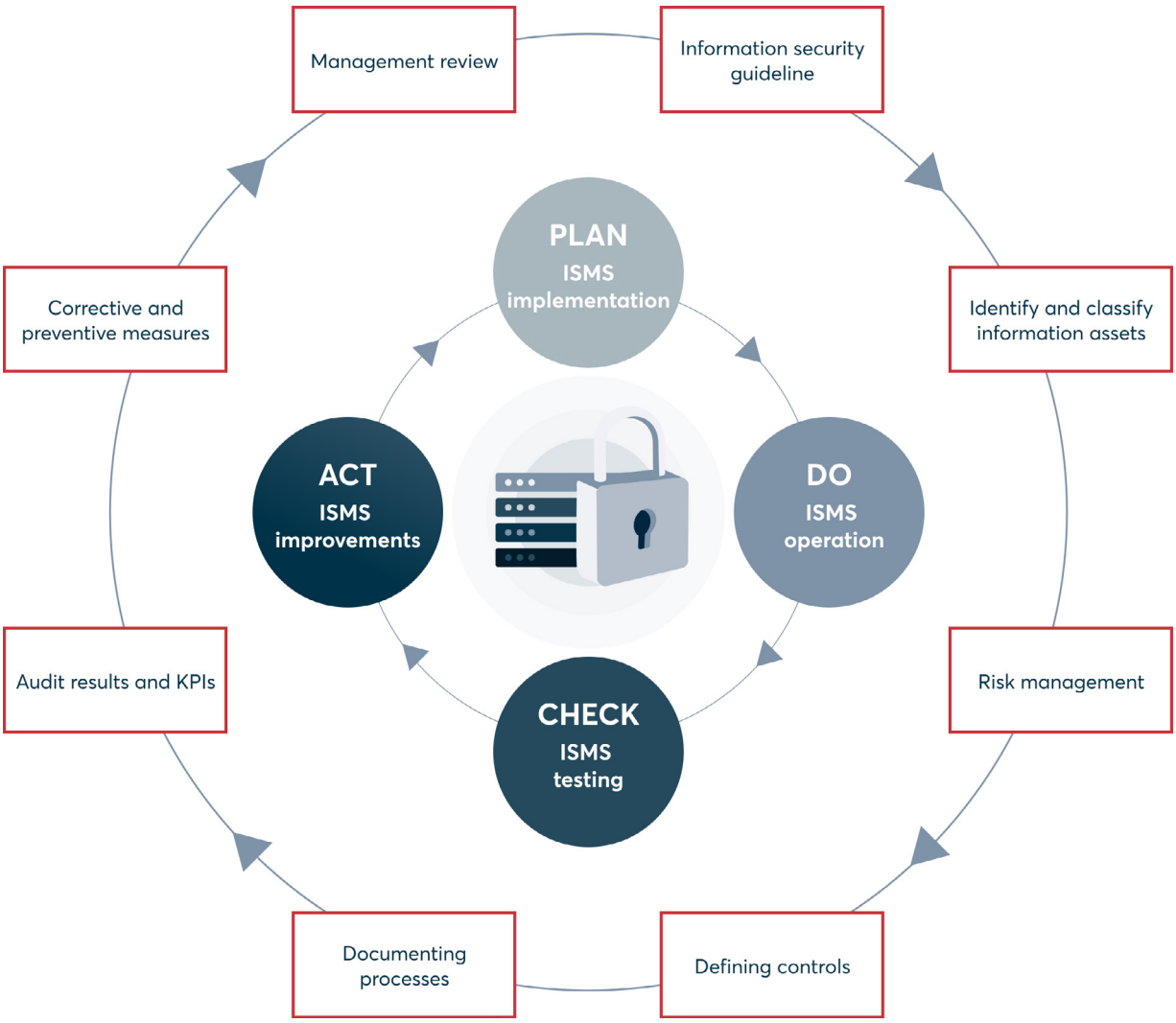
4. **Develop control mechanisms.** How can we check whether our ISMS is effective and protects our corporate assets the way we want it to?

5. **Operate the ISMS.** What processes do we put into action in day-to-day business? How will we integrate and document them?

6. **Check results and KPIs.** Questions like this must be routinely addressed: what are the results our ISMS achieves? What key performance indicators (KPIs) are we able to derive from them?

7. **Make corrections and take precautions.** Where do we need to make changes to get better results? What can we do to prevent risks?

8. **Review by management.** Are the goals and general orientation of our ISMS still a fit for us? Does management need to course-correct? Management should review the ISMS with questions like these at least once a year or when there is a major change to the organisation.



CHAPTER 5

# ISMS CERTIFICATION

Companies that have a certified management system for information security benefit in a number of ways, not the least of which is the systematic identification and minimisation of risks to your IT systems, your business activities and processes and finally your own employees' conduct at work.

In other words, companies with a certified ISMS are able to manage their information security risks to a high degree of excellence that is demonstrable to the outside. This will increase the confidence that customers and potential partners have in your company's ability to perform. It is impossible to overstate the competitive edge this will afford you on the market. An ISMS can also serve as proof of compliance with industry and other legal requirements, such apply to operators of critical national infrastructure (CNI).

One thing is certain: any investment and effort you put into certification is sure to pay off – especially if you're facing a due diligence check. After all, the process will be significantly swifter and easier if your company already has ISO 27001 certification. As an added bonus, ISO 27001 certification often greatly increases company value.

## THIS CHAPTER COVERS:

- ISO 27001 is the gold standard for information security management systems.
- ISO 27001 certification for your company's ISMS is advisable if you wish or are required to provide proof of your information security to third parties.
- Certification by an accredited body is strongly recommended.
- The associated costs will greatly vary by company size, the complexity of the information security processes and the scope you wish to have certified. Based on our experience, for smaller companies with only one location, implementation to certification will incur costs of € 10,000 (£7500).

# Industry-specific certification schemes for information security management systems

ISO 27001 is the gold standard for information security management systems. However, the individual industry or market as well as national legislation may make other standards relevant. Take Germany for instance, where the **Federal Office for Information Security (BSI)** has developed the standards BSI 200-1 and BSI 200-2. As a 12-step system for implementing a compliant ISMS, is an especially interesting standard to local authorities and small and medium-sized enterprises.

When working with U.S. federal information systems, **NIST (National Institute of Standards and Technology) Special Publication 800-53** is the relevant standard – or, with respect to financial reporting, the international **Service Organization Control standards SOC 1 and SOC 2**.

# Accredited ISO 27001 certification

ISO 27001 certification for your company's ISMS is advisable if you wish or are required to provide proof of your information security to third parties. But certification isn't free. Not only do you have to pay for auditing itself but putting in place the requisite measures can also eat up a good deal of resources. It would therefore be aggravating if, for your efforts, you do not successfully pass the certification audit and all you get is a certification that is worth little or, worse, nothing.

→ **Click here for a list of all UKAS-accredited bodies.**


There are a number of national and international accreditation bodies around the world. EU law stipulates that each member state have one single national accreditation body – such as the Deutsche Akkreditierungsstelle (DAkkS) in Germany or the Hellenic Accreditation System (ESYD) in Greece. In the USA on the other hand, there are multiple accreditation bodies that serve different standards, among them the ANSI National Accreditation Board (ANAB) for ISO 27001 accreditation. The UK follows the EU model, with one solely appointed national accreditation body, **the United Kingdom Accreditation Service (UKAS)**. Currently, UKAS has accredited more than 150 certification bodies in the UK alone, 24 of which specifically offer accredited ISO 27001 certification. And while UKAS does offer ISO 27001 accreditation to foreign certification bodies as well, certifiers around the world typically pursue recognition by an international accreditation body such as the International Accreditation Board (IAB). Certification bodies accredited by IAB perform audits according to ISO 17021, an international standard for auditing management systems.

Certifications not confirmed by the international accreditation body are often not recognised by business partners. Indeed, most contracts that require ISO 27001 certification do mean certification by an accredited body. For this reason, it is strongly recommended that a company pursue certification through an accredited body.

## ISO 27001 certification: the costs

For companies seeking ISO 27001 certification, implementation itself generally incurs the greatest cost. Meeting the various requirements can take months or even years, and third-party consultant services, often a must, rarely charge daily rates under € 1,500 (£1300).

The certification process itself pales in comparison to the run-up to it. But when it comes to your company's implementation measures, the proof is in the pudding: if the certification body decides your company falls considerably short of compliance and you fail the audit, you'll have to arrange a new audit – the process starts over, and the costs increase.

A medium-sized company with 100 employees and relatively low process complexity per 15 to 20 employees can roughly expect an audit to wrap up in one day. For larger companies, audits will be more time intensive. The actual duration will naturally depend on how complex your information security processes are as well as on the scope you've defined for your ISMS to cover. Based on our experience, for smaller companies with only one location, certification will run about € 10,000 (£7500). Certification bodies will provide an exact figure upon request.

## Recertification: the how and when

Putting information security measures in place is not a one-off project but a continuous process. For this reason, your company's ISMS will need to be recertified from time to time. To stay compliant with ISO 27001, your certification will need to be renewed once every three years through an entirely new audit process. And the certifying body is required to carry out less extensive checks every year. If serious deficiencies are uncovered, certification can be revoked even before the three-year cycle is up. What's more, ISO 27001 also requires companies to perform annual internal audits on their own.

CHAPTER 6

# THE INFORMATION SECURITY JOB MARKET

Today, there is a global shortage of some **3 million cybersecurity professionals**. The **financial daily newspaper mint reports** that this lack of professionals is a key worry for firms in 2022. And it's no surprise, as the information security job profile brings together to a unique skill set – a plurality of competencies that are rare in today's jobs market, taken even on their own: in addition to a high degree of IT literacy, applicants also need to demonstrate in-depth knowledge of the standards and laws relevant to the field. Moreover, the job is also one that frequently demands an aptitude for communication and negotiation. After all, information security processes can only work when all the involved company divisions cooperate – getting them to do so is just one more task where the cybersecurity professional must shine.

**THIS CHAPTER COVERS:**

- On the job market, information security experts are a hot item.
- There is no dedicated degree program for a career in information security: graduates in computer science and business administration are equally qualified.
- More important than a degree are previous experience and knowledge about ISO 27001 and information security management systems.

## Requirements for a career in information security

Many roads lead to information security. Computer scientists can receive training in ISO 27001 or pursue a number of different industry certifications such as Security+ and Network+ from CompTIA. Graduates in business administration are also great candidates for advanced training and certification as an Information Security Officer. Today, many universities even offer masters programs in cybersecurity. But it should be noted that a degree is not a requirement for a career in information security.

Even more important is previous experience in the fields of:

- Implementing IT security (with a good grip on critical infrastructure)
- Setting up an ISMS
- Certifying an ISMS in accordance with ISO 27001 / TISAX®
- Managing information security incidents
- Staff trainings and awareness-raising activities
- Negotiations and project management

Information Security Analyst, Information Security Officer and similar jobs are highly respected positions that often bring in a six-figure salary.

## (Chief) Information Security Officer: an overview

A **Chief Information Security Officer (CISO)** or **Information Security Officer (ISO)** focuses their attention and efforts on securing the interests of the company. The job is something of a balancing act between protecting information assets and ensuring seamless business operations. Normally, the position is directly subordinate to top-level management and works closely with the IT department as well as the compliance and legal teams.

The responsibilities of the CISO include:

- Protecting corporate assets from attacks and data breaches (in cooperation with the Data Protection Officer and IT)
- ISO 27001/27002 and TISAX® certification
- Introduction of an information security management system
- Choosing suitable methods and tools
- Risk management and advising company management
- Communication between departments

CISOs are often computer scientists or computer scientist graduates with advanced training or specialisation in the field of information security, in addition to years of experience. The responsibilities of the job are not legally defined; a CISO's day-to-day activities will depend greatly on the company itself and the respective industry. However, there are special cases in the public sector where the job profile is legally defined.

Depending on the company, the position of CISO can be filled by an internal employee or an external service provider.

* TISAX® is a registered trademark of the ENX Association. DataGuard is not affiliated with the ENX Association. We provide consultation and support for the TISAX® Assessment only. The ENX Association does not take any responsibility for any content shown on DataGuard's website.

# Outsourcing information security

Not every company has the resources or the will to implement and manage information security. In some cases, the internal team might be overworked and overwhelmed by the heavy documentation load. Perhaps the team doesn't have the right expertise for a certain project or fails a due diligence audit... When faced with challenges like these, it's best to turn an external service provider for guidance.

The advantage: external services are quick to purchase, and the service provider's experience means you skirt the timely onboarding process. A good provider will assign you a personal contact, your go-to for all the challenges your company faces with the know-how from past experience to overcome them.

Another win: it's cheaper to hire an external service provider than to pay the salary for a full-time company position. At DataGuard, our customers pay just between € 500 and € 2,000 (£400 - £2000) a month, depending on the complexity of their needs.