IRM360
Integrated Risk Management Solutions

Securing an ISMS with the help of Tooling

What to look for when selecting Tooling?

NIS2

ISO 27001

ISAE 3402

SOC2

ISO 42001

White paper
11 January 2024

Ref: White paper ISMS Tooling-2024 v1.0.docx

Table of content

1. Why this White Paper and for whom?

With this White Paper, we want to inform interested parties about securing an information security management process, also known as the Information Security Management System (ISMS). This White Paper discusses issues such as information security, standards such as ISO 27001 and the question: 'when is an ISMS necessary?'.
Different types of tooling are explained, including the selection process.

2. What is Information Security?

The concept of information security can be described as protecting and maintaining the confidentiality of information, integrity of information and availability of information. With information security we mean the protection of business equipment such as servers, computers, networks and all the stored data stored. It also includes risk awareness among staff and emergency recovery for continuity after an information security incident.

In this context, all forms of information are included. This ranges from the spoken word, information on paper, confidential information written on a whiteboard, stored and communicated information, including analogue information. Having an insight into what information and systems are being used, what dependencies there are on business processes, is essential for good security and risk management. We are becoming increasingly dependent on digital information, and this is crucial because if security is inadequate, an organisation runs the risk of incidents, data breaches and even grinding to a halt.

2.1. Information Security and Cyber Security

In an increasingly digital world, the focus is shifting from analogue information to digital information. Cyber Security focuses mainly on the digital (Cyber) information and is therefore a part of Information Security. Cyber Security focuses in particular on the following areas:

1) Malware, Ransomware
2) IoT (Internet of Things)
3) Digital data breaches
4) DDoS attacks
5) Hack attacks for industrial espionage or on the supply chain
6) Phishing (e-mail) or smishing (via SMS)

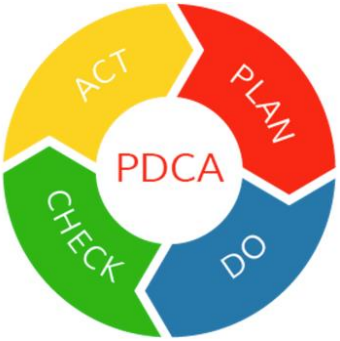
Technology and risks are changing rapidly. Where ,20 years ago, we first worried about "war driving", this was when hackers tried to hack into the local network via Wi-Fi. Now you run the risk of being hacked via IoT (internet of things) devices such as a coffee machine if it has an internet connection.

We can all imagine the threat burglars pose and install a good lock, cameras, a burglar alarm and possibly a security service. If these measures are taken, they often already have a preventive effect. This makes the chance of a successful break in smaller, and with "limited" measures the chance of being caught bigger.

In 2024, cyber risks are entirely different. We cannot see the threat anymore. The whole world is connected to the Internet, so the threat can come from everywhere. Therefore, part of the criminality shifts to cybercrime. While this threat might not be visible anymore, it can still pose a great risk. If hackers gain access to critical business data, they have the means to shut down or extort an entire organisation.

3. What is ISO 27001 and ISMS?

ISO 27001 is the international standard for information security. It describes the process of controlling information security risks, or the Information Security Management System (ISMS). The ISMS is therefore not a system or a tool, but describes the whole of activities to realise the management of information security. These activities can also be seen as norm requirements so that it can be demonstrated to an auditing body in order to be certifiable for an ISO 27001 certificate.



These requirements concern matters such as information security policy, controls, risk analyses, measures, verification of the operation of the process and the risk awareness level of employees, etc. There is an overview of control measures (Annex A measures) that you must implement. If a control measure does not apply, you can declare it "Not applicable". These measures are not described in detail in the standard. In practice, you can use your own measures or the measures from the ISO 27002 best practice set, or from other standards such as the NIST CSF or the CIS Controls.

4. Why certification?

It is becoming increasingly common that suppliers are required to be ISO 27001 certified. Certification offers added value in demonstrating that the ISMS is secured as a process and that information security is taken seriously by the organisation. It also indicates that the necessary measures have been taken to ensure the confidentiality, integrity and availability of information in relation to risks and that we want to improve.

4.1. Is certification easily acquired?

Securing the ISMS and certification is not something that should be underestimated. It is not a one-off project but involves process assurance with annual activities. An ISMS also entails the necessary administrative recording. It requires a documented management system in which not only IT-related matters are described but also the performance of risk assessments, policy, procedures, guidelines such as codes of conduct for employees and attention to risk awareness. The ISMS also addresses issues such as leadership, planning, supporting processes, legal requirements, implementation, monitoring, measurement, evaluation and improvement as important requirements. For proper assurance of the process, it is advised to secure the necessary knowledge in the organisation. If you do not have this in-house, additional training is recommended or you can bring it in externally.

We therefore recommend only implementing an ISMS if you must or wish to obtain ISO 27001 certification and have the necessary resources and knowledge in-house or hire them externally. Certification bodies test whether you follow the standard in the implementation of all the aforementioned matters. After obtaining the certificate, an annual control audit is performed, so it is not a one-off action. Not every organisation is mature enough for this or has sufficient resources.

An ISMS is no guarantee that you will not be hit by a security incident. You do reduce the chance of an incident occurring and, in the event of an of an incident, are able to act more adequately and reduce the damage. It increases your organisational cyber-resilience. But not every organisation that wants to be cyber resilient needs an ISMS. More about this in the next section.

4.2. Do I need an ISMS to be Cyber resilience?

In the previous section, we stated that implementing an ISMS is not easy. If your organisation has limited resources, implementing an ISMS can be a challenge. In addition, securing an ISMS according to ISO 27001 involves the necessary administrative commitments, but that is just how the standard is structured: a list of standard requirements. In addition, implementing, securing a process, a Plan-Do-Check-Act cycle, is not a one-off project. Because there are recurring activities every year.
If a certificate is required, an organisation has no choice but to comply with these standard requirements, otherwise they will lose the certification. If not, there are other ways to increase Cyber Security.

4.3. Cyber Security and the limitations in ISO 27001

It was explained in chapter 3 that ISO 27001 is a standard for certification of the management process and does not explicitly deal with measures. The Annex A measures mentioned in ISO 27001 do not cover everything.

For these reasons, there are also various additions to the ISO 27001 standard such as (we will not mention them all, there are about 35 including ISO 27001 and ISO 27002)

- ISO/IEC 27017:2015 focused op Cloud services
- ISO/IEC 27018:2019 focused op on securing privacy information in the Cloud
- ISO/IEC 27032:2012 Security techniques for Cyber Security
- ISO/IEC 27701:2019 focused on Privacy Management

A disadvantage of this set-up lies in the fact that these "extra" sets are based on the fact that, in most cases, you should already have an ISMS in place. If you have not implemented an ISMS but are looking for Cloud- or anti-Ransomware focused measures, then an ISMS may not be the solution, and it is better to choose from standards that directly fit the current need.

Many organisations are currently rightly concerned about the many Ransomware attacks. Securing an ISMS or obtaining an ISO 27001 certificate will not cover this risk immediately but will reduce it in the long term.

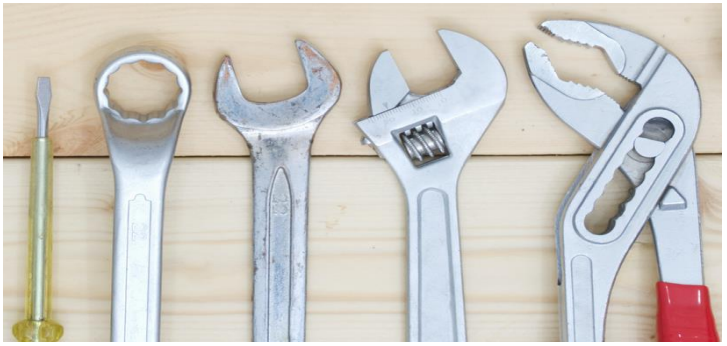
Securing a risk management process is after all based on a set of risks and the importance is determined by the "Chance x Impact". Based on this risk score measures are taken.

Looking back at the list of cyber threats mentioned in paragraph 2.1, it should be possible to draw up a set of basic measures.
A risk is in fact valued on the basis of probability times impact. If the basis is sufficient, the probability becomes less and therefore the risk score becomes less. A company fire can be catastrophic, but with a basic measure of fire detection and a fire extinguishing system, the probability is lower and so is the risk.

The ISO standards focus on the risk management process. If you go through the process properly, you will automatically arrive at risks, to reduce these risks you take measures, in doing so you comply with basic measures. But in practice, this is often separate from the audit pressure to obtain a certificate and the emphasis is sometimes more on "process" issues that are in the standard, such as properly describing a cause/effect analysis of the context of the organisation, carrying out a management review correctly and on time. Rarely are the basic measures looked at (first). Then you have organisations that are certified but are subsequently hacked, or organisations that are focused on the process but have not yet taken the basic measures.

There are currently various (Cyber) Security standards that can also be used here. In the last chapter, we will discuss the cyber security aspects in more detail.

5. Can tooling help?



As described in the previous chapter, securing an ISMS contains a large number of activities. ISMS Tooling should support the execution of risk assessments, risk treatments, (improvement) task management, controls, audits, evidence, audit planning and the generation of all kinds of certification reports.

Ready-made templates help to set up an ISMS and speed up the implementation. Some tools include a management system for measures to avoid multiple standards and duplication of registrations and activities. This is useful if you need to manage multiple standards. Of course, all activities can also be kept up to date from, for example, spreadsheets, but this is time-consuming and difficult to manage with multiple standards.

5.1. Types of Tooling, ISMS vs. GRC vs. IRM

There are various ISMS tools available. But which one fits my organisation best? In the following paragraphs, a number of ISMS tool types are explained. These can roughly be divided into 3 types.

5.1.1. ISMS Tooling

These are mainly focused on providing ISMS functionality only and focus on a limited number of standards such as ISO 27001. Some vendors also offer privacy. In some cases, such tools are built on an existing application/platform, e.g. SharePoint. For a targeted ISO 27001 certification goal, they are a perfect fit, especially in SMEs.

5.1.2. GRC Tooling

GRC focuses on a much broader area than an ISMS. GRC as a concept blew over from the US in early 2002 in order to make the control and performance of listed companies demonstrable. This was in response to a number of stock market scandals. GRC is aimed at the entire organisation and originated in the Enterprise environment in order to get the organisation demonstrably "In Control". GRC tools can also be used for an ISMS application, but the scope of GRC goes far beyond information security alone. In principle, this means that they offer a great deal of functionality, more than is necessary for an ISMS, and they bring with them more complexity with regard to implementation and management, which makes them less suitable for SMEs or for a limited objective such as merely obtaining an ISO 27001 certificate.

5.1.3. IRM Tooling

IRM tools are usually focused on a management system or risk area. From the Integrated Risk Management (IRM) approach, they usually offer the possibility of using them for one (e.g. an ISMS) or several management systems. This can be done in phases so that the implementation can be carried out in a targeted manner. The greater the range of the IRM provider in available management systems, the greater the overlap with GRC.

GRC vs. IRM Solutions – What's the Difference?

Solution Characteristics	GRC	IRM
Architecture	Closed, Proprietary	Open, Integrated
Content	Compliance-driven	Risk-focused
Design	Technical, Control-based	Business-oriented, Process-based
Market Definition	Ubiquitous, meaningless	Targeted, purposeful
Features / Functions	Rigid	Flexible
Buyers / Influencers	Technical practitioners	Business leaders
Use	Internally-driven, departmental	Ecosystem-driven, cross-business unit, partners/suppliers

Gartner

Tools developed from an IRM approach are less complex in structure, can be used in a targeted manner, offer flexibility/scalability and can usually be implemented in a relatively short period of time. As a result, ISMS solutions based on the IRM philosophy are generally suitable for SMEs, large and enterprise organisations.

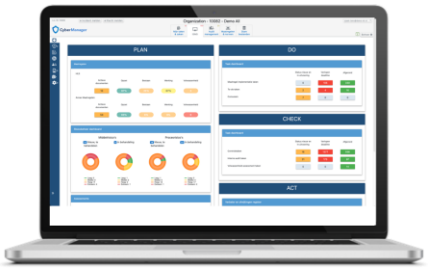
5.2. What to look for when selecting tools

The following list is not exhaustive, but provides an overview of issues to consider when making a selection. The answer depends on factors such as whether your organisation is large or small, simple or complex, mature or immature in the area of ICT or information security processes, has invested functions/roles such as an Information Security Officer, etc.

- Is only a documented ISMS sufficient, or is functionality also needed for correctly performing assessments, risk management, audit management, etc.?
- Should other management systems also be supported/integrated (in the future), such as privacy management, business continuity, cyber security and quality?
- Am I looking for a GRC, IRM or ISMS solution?
- Should risk awareness of staff be part of the solution?
- Am I looking for a professional tool for the information security staff?
- Should control activities be carried out in addition to internal audits?
- Should privacy aspects such as data breach management, processing register, execution of (pre)DPIAs be possible to integrate?
- Is fast implementation required due to certification requirements?
- Are templates desirable to facilitate rapid implementation?
- Do multiple standards from ISO 27001 need to be mastered?
- To what extent are additional dashboards needed for my organisation that are consistent with the ISO 27001 implementation? Consider legislation such as NIS2, DORA and other Cyber Security (EU) legislation, for example?

- Do I look for a SaaS solution or On-Premise? Take the following considerations into account, especially regarding SaaS:
  - Are you the owner of the data?
  - Are things arranged with regard to a SaaS agreement, SLA, is the supplier for example ISO 27001 certified?
  - Where is the data located? The Netherlands, within the EEA
  - Does the solution follow the model of the intended management system solution/standard?
  - Are there connection possibilities, APIs? Especially with SaaS solutions, these should be available!
  - Do I run the risk of Vendor Lock-in? Pay attention to customisation possibilities, that in itself is nice but makes a Lock-in risk only bigger (see also paragraph 6.3)
  - o The strength of SaaS lies in the investment and management of the solution by the vendor. This should translate into low licensing and maintenance costs.
- Does the software offer good security such as encryption, Two Factor Authentication, Single Sign-on applications (AzureAD/ADFS, OKTA, SAML)?
- The strength of SaaS lies in the investment and management of the solution by the supplier. This should translate into low licensing and maintenance costs.
- Does it suit my organisation/users?
- How many users should work with it?
- What are the one-off and annual costs?
- What are the implementation costs and duration?
- Is implementation support available, possibly via partners?
- Does the supplier offer training opportunities?

6. IRM360 CyberManager



6.1. CyberManager ISMS

The CyberManager ISMS management system is based on the (IRM) concept. You can perform all steps to implement and secure the ISMS process.

With the Plan-Do-Check-Act functionality, you can realise, demonstrate and certify the control of your ISMS process:

- ISMS dashboard for information security;
- Various assessments, risk analysis and risk register;
- Measures tasks (incl. reviews) & standards management;
- Management review and Statement of applicability reports;
- Incident management;
- External audit management;
- Internal audit, audit planning and controls and improvement tasks;
- E-Learning for risk awareness;
- Optional vulnerability scans;

There are measure templates available for SMEs, Accountancy, Care, Municipalities and also various other norm frameworks in the field of privacy or information security such as MedMij, WPG, SUWI, COBIT, ISO 27017, ISO 27018, ISO 42001, CSA-Star, ISAE-3402, SOC2, NIS2, CSIR or for example the IEC-62443.
QuickStart guides make the introduction of an ISMS management system even easier. Implementation partners can be brought in if additional expertise or resources are required.

IRM360 offers Privacy (PIMS), Cyber Security (CSMS), Business Continuity (BCMS), Artificial Intelligence Management System (AIMS), Quality (QMS) and Financial Risk (FRMS) Management Systems in addition to the Information Security management systems (ISMS). As a separate system or as an integrated Management System.

6.2. Migrating to the CyberManager ISMS without vendor lock-in

As indicated in section 5.1, there are various types of Tooling that you can use for an ISMS. Often, the previous choices were prompted by the state your organisation was in at a given moment, or the possibilities and availability at that time.
Are you stuck with a certain Tooling choice because of so-called vendor lock-in? And are you confronted with major (financial) consequences when switching to another application?

This depends mainly on the possibilities of the application you want to switch to! With financial solutions, we often see that there are import/migration tools from one application to another. But the administrative process is much more fixed, a general ledger is simply a general ledger, and that also applies to invoices, journal entries etc.

To offer this possibility, we have built in a facility to quickly and easily transfer the design, existence and operation of measures and management systems such as a running ISO 27001 management system with Setup, Existence and Operation scores, dashboards and relevant evidence, and to easily maintain an (existing) certification process without high costs.

Want to know more about the IRM360 management systems and the CyberManager?

Visit www.irm360.eu and request an online demo.
We will gladly show you!