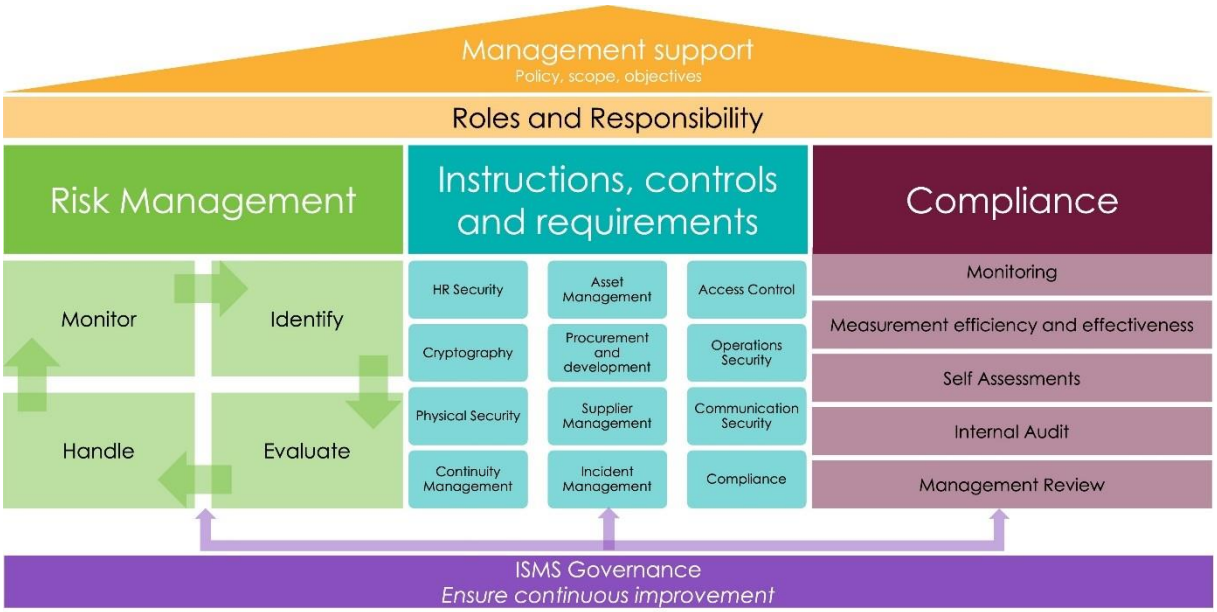
TRANSCENDENT GROUP INSIGHT

ISMS challenges, and how you can solve them

In this article, we'd like to help you understand what an Information Security Management System (ISMS) is, what challenges we usually see with ISMS in organizations, and how you should implement and operationalize an ISMS today.

First - what is an Information Security Management System (ISMS)?

It's common to think of an ISMS as a set of policies and procedures, but it is much more than a stack of documents. ISMS is a framework that provides a systematic approach for managing and continually improving information security in the organization. The ISMS is often represented as a plan-do-check-act cycle or the document hierarchy pyramid, but by doing it this way, it's easy to miss essential building blocks of the ISMS. To illustrate what an ISMS should consist of, it can be helpful to think of it as a house, where you have management commitment as the roof to ensure that you keep "the rain" out and roles and responsibilities as the supporting beam. The three main pillars in the house are risk management (risk-based approach), security controls (what to do, by whom, and when), and compliance (to ensure you do the right things and do the things right). The foundation of the house is the ISMS governance to help you ensure continuous improvement and that all the building blocks are holding together.



Model produced by Eli Sofie Amdam, Transcendent Group

Let's start by looking at some common challenges with an ISMS today:

- The ISMS exists only on paper and does not affect the organization or company.
- The ISMS does not reflect how the organization works and operates today.
- Consultants have implemented the ISMS without involving the organization, so the result is an ISMS not reflecting the organization, and it dies because of a lack of internal ownership.
- The ISMS focuses on the Management System (MS) but is weak in the Information Security (IS) part.
- The ISMS is outdated and in conflict with modern ways of working.
- The ISMS has been sold and "implemented" by someone without enough knowledge, and their template has not been adapted to the organization.
- Management thinks they are "safe" because they have a certified ISMS, but they don't understand the scope and applicability of the ISMS, nor do they understand that ISMS does not necessarily equal a robust cyber security defense.
- Cloud Security Engineers and Architects are blocked from implementing best practices in the cloud because the ISMS is adapted to an on-premise environment.

What should you do if you have one or several of these challenges?
If you are going to implement an ISMS in the future - what should you think about?
We'll try to answer these questions sequentially, so please stay with us.

#1 - Business understanding

You can start by getting a solid understanding of what the business does and how it operates. Why is the organization alive today? Do they sell shampoo? Do they provide health services? Do they sell car parts? Are they an online store?

We need to remember that the reason for us building and maintaining an ISMS is not because of the ISMS itself. It is because the organization has risks connected to cyber security, and they want to reduce this risk to an acceptable level. This means that two companies most likely have two completely different needs when it comes to an ISMS, maybe one of them doesn't need an ISMS, and perhaps the other one needs a very detailed ISMS.

It's also smart to find out what the business strategy is. Are they going to grow fast? Go into different markets or countries? Provide new services? Work from home? Acquisition of other companies? And so on.

#2 - Current IT landscape and strategy

Okay, great, you currently understand the business side of things. It is now time to dig deeper into the IT landscape and the IT strategy. Some of the questions you'd like to get answered here are typical: How does the IT landscape look today? On-premise? Cloud only? A good mix? Do they develop any software themselves, or do they only rely on off-the-shelf software? How many people work with IT? Where do they work from, and what capabilities do they have?

After getting a good picture of the status quo, it is time to look forward. What is the IT strategy of the organization? How will the above questions be answered 3-5 years from now?

#3 - Is anything in place from before that can be updated or re-used?

You don't need to start working from scratch if you can use what the organization has from before. Do they have any policies? Standards? Routines? Risk assessments? Control frameworks? Gap-analysis? Application portfolio? Some of this might need to be updated or changed, but that will most likely save you several hours of work compared to starting from scratch.

#4 - Gap analysis against a well-known framework

Having a good understanding of the current cyber security defense, where the organization performs strong and where the organization performs poorly, also gives you a good insight into where the ISMS needs to dig deep and where you most probably can use less time. It is also good for you to know where the most significant risks are today (on a high level) compared to starting to implement an ISMS without a clue on where to focus.
Could you find a suitable framework to help you establish and implement the ISMS? Usually, an ISMS is based on ISO/IEC 27001 and 27002, but this is not a necessity to implement an ISMS in the organization. Which standard or framework fits your organization best? Even ISO/IEC 27001 is quite clear that you can design controls as required or identify them from any source other than ISO 27002. Other frameworks that fit your organization better can be CIS V8, NSM (basic principles for ICT security, a Norwegian framework), NIST CSF, CSA CCM, or maybe something completely different.

You can read more about gap analysis and how you can and should do this in a previous article from Olav:
https://www.o3c.no/knowledge/rethinking-your-approach-to-a-cyber-security-defense

#5 - Create a plan, find your core team, and define the scope

You are not able to do this work on your own. And if you did, the ISMS would most likely be left dead the day you started doing something else. Your role in implementing the ISMS is understanding the big picture and keeping the work moving forward, not deep-dive into every subject and routine. Let those from the organization that usually performs the task or process you want to take control of figure out how they can make the ISMS fit them and not them fit into your ISMS. One example is to involve HR to enrich their joiner-mover-leaver process to be more secure than before, instead of writing the routine on your own and then just handing it over to them. Guess what will happen, then? Nothing.

We see many organizations starting with an extensive scope or a scope that gets bigger (scope creep). This ends up with the ISMS never being implemented. It is usually better for you to start with a smaller scope and implement that before you continue with the next step. Making things too big will make them fail. An ISMS is something that should live and be updated and looked at regularly (weekly/monthly), not something you do once and let go.

#6 - Adapt the ISMS to the organization in question and integrate it with existing processes

As mentioned earlier, every organization has different needs regarding an ISMS. Processes, standards, policies, and risk assessments can not be copied/pasted from one organization to another. The only way for an ISMS to give value is if it's tailored for the organization, making it relevant. You can base the ISMS on the business understanding you gained in point 1. Use

knowledge about the organizational structure, strategy, risks, needs, and culture when you write your policies, procedures, and requirements.

Work actively to avoid security becoming an extra add-on, but instead being integrated into existing roles, processes, tools, and routines. For example, please don't set up a new security configuration management process but ensure that security is integrated into the current configuration management process. You can add an extra checkpoint in a checklist or a mandatory field in the tools you use, compared to creating new routines the employees have to follow in addition to their day-to-day work tasks.

#7 - Documentation != document

Documentation does not necessarily equal word and PDF files stored on Sharepoint. Documentation can also be policy as code, workflows, automation, etc. Please document where it is easy to be kept alive and where employees usually spend time during the workday. Here is a hint - that is not on Sharepoint!

#8 - Make sure you have backing from top management and intermediate managers

It would be best if you had backing and sponsors. Top management needs to understand why an ISMS is essential, what it provides, and how it works. They then need to communicate the importance of the work to the organization. So, you should make sure and use time with top management until you and they feel confident with implementing an ISMS.

Next up is intermediate managers. Everyone knows that they are the ones to make things happen in the organization and are the ones most employees deal with daily. If their closest manager doesn't care about information security - why should they? If teams are busy and focusing on other work, you need their manager to prioritize them, allocating time and resources so that they can make time for the ISMS work. Ensure that you have the tone at the top and a strong tone in the middle.

#9 - Security culture and communication

Security culture has been under-communicated within cyber security for years. It does not help that you have the most robust technical security professionals if the culture in the organization is:

"not my responsibility; IT will fix that."
"I'm not going to report this to IT security; I might lose my job."
"That will not happen to us; everyone else gets hacked, not us."

A strong security culture is when someone reports to you that something strange happened on their computer because they understand the importance and responsibility, not when they do it because they are afraid of punishment. You also have a strong security culture when people want themselves and the organization to be and stay secure because they understand that this is everyone's responsibility. And you have an excellent culture when people line up to help implement the ISMS!

So, how do we get there? They need to understand the why and the how. This is not something you solve in a day or two; it will probably take you several years if you don't have the right culture from before.

#10 - Training and Awareness

The why and the how are usually solved with training and awareness. Help people do the right thing by sharing your competency.

You should probably do several things here, but here are some examples:

- One general Cyber Security course that is mandatory for all employees (again, make it relevant and tailored for your organization). Everyone should take this course as part of the joiner process and yearly.
- Specified courses tailored for different departments. Developers have a different need than finance, and finance has another need than HR.
- Be careful with e-learning and generic courses; they end up with a compliance check that everyone clicks through, compared to a tailored approach where people get motivated to learn.

To facilitate actual behavioral change among employees, the employees must be motivated and feel capable of changing. Both require relevant training and awareness.

Asking questions is usually much better than trying to persuade. Ask the employees why Cyber Security is essential for the organization. Ask them who is responsible and why. Create a dialog where you activate as many as possible. Remember, making other people talk and think about Cyber Security is what you want to achieve here, not for you to shine.

Summary

There are many things to consider and keep in mind when implementing an ISMS. The most important, however, is to start with a small scope, involve internal resources, don't use someone else ISMS, and update it regularly. Technology, risk, and threats are not static - so why should your ISMS be?

If any questions, feel free to reach out to one of us on LinkedIn or by mail:

Eli Sofie Amdam, Transcendent Group

✉: eli.sofie.amdam@transcendentgroup.com
: https://www.linkedin.com/in/elisofieamdam/

Olav Østbye, O3 Cyber

✉: Olav@o3c.no
:https://www.linkedin.com/in/oestbye/