ISO 27001

Tiennot van Dilst- Principal Consultant / Delivery Manager – Comsec Benelux

During my career as a CSO and Security Consultant, I have worked with the ISO 27001 standard on various occasions.

As a consultant I have helped various medium and large organizations in assessing and implementing the standard, whereas as a CSO I have been on the other side of the coin, being fully in charge of implementing the standard within the organization in which was working for.

I have also encountered the different pitfalls associated with implementing the standard and getting (part of) the organization certified.

I am writing this article in the hope that I can ease the mind of people in the Information Security field wanting to start to work with the standard, or who are looking to work with an external organization to support their implementation process.

So what is the ISO27001 Standard?

First of all, let me try to explain to you what the ISO 27001 standard (formally known as ISO/IEC 27001:2013) is all about. Many people are under the impression that when an organization is certified, it must be a secure organization…. I'm sorry to destroy that illusion for you but it is unfortunately not true. Being certified means that the organization has an information security management system (ISMS) implemented that, if maintained correctly, will enable the organization to manage their risks, implement and consolidate the selected and approved measurements and controls to mitigate those risks, and bring the risks down to an acceptable level.

The ISO 27001 standard does not provide a golden ticket showing you which controls you should implement. However, it does provide you with a management system which enables you to implement those controls. When implemented correctly, the management system will deliver continuous improvement of these implemented controls. The measures and controls themselves can differ from organization to organization, however the majority of organization conform to a standard control set, which is supplied as an annex to the standard, and which is fully described in the ISO 27002 guide, which focuses on the actual security controls.

Nevertheless, there are some controls in every ISMS that keep the management system operational which we cannot go without. For example, having a formal policy in place, a security organization, periodic reviews/audits and having an improvement process in place.

So two organizations can both be ISO 27001 certified, but have completely different control sets. In the Netherlands I have encountered this several times. Specifically, I have seen organizations where they are ISO 27001 certified but using the controls supplied by the Dutch health care standard NEN7510.

In short: "ISO 27001 describes the requirements of the ISMS and you can certify parts of your organization or processes if they are working according to this management system, whereas ISO 27002 provides you with an implementation guide on how to implement the commonly used controls. (ISO 27002 is not a standard to which you can certify).

It's all about scope…

Especially (however not exclusively) in the IT department, when a company is looking for a service provider and requesting information, the suppling organization will try to baffle you with all the certifications they have. You will see that they say, almost by default "we are ISO27001 certified, so you should not worry about security". In the meantime, they won't tell you what is the exact scope of their certification. Lesson number one in this case should be to always ask them to explain to you exactly which part of the organization is certified, or even better ask them for their "statement of applicability", which will show you the scope of the certificate and which controls have been implemented.

On the other hand, when you looking to implement the standard in your own organization, make sure you find out exactly which part of your organization you want to be certified. In many cases, certifying your complete organization will overshoot the goal. Always keep in mind the additional value of having a certification and make sure that the important processes and assets (including their supporting processes) are in scope.

While other processes might not be in scope for the certification, they can work according to your ISMS.

From unknowingly being at risk to willingly taking a risk….

So here we are, we are aware that the standard is about having a management system in place, and we know now what is important enough is to have in scope, what's next? First of all, we need to consolidate the management system, meaning that we have to make sure that the right environment is set to create and maintain an ISMS. In many cases you will see in this phase that companies will create a security role or organization, describe the strategic policies (based upon the mission and vision of the company, local law and legislation and in some cases other factors like the position of the organization in the society, public interest, physical location etc.), and make sure we know what the important risks to the organization are. From these high level risks, we can filter operational risks, asset risks and process risks and think of (and document, and approve), measurements to bring the risk level down to an acceptable level.

After implementation, the organization should check if the controls and measures are implemented correctly (Internal audits, technical reviews etc.), and management should be informed about the process on a regular basis. This cycle usually takes 3 months to a year and repeats itself annually.

Again, it's not about fully mitigating the risks, it's about knowing what your risks are and bringing them to an acceptable level.

Part of a normal schedule for activities within an ISMS could be:

Activity	**Reoccurrence**
Risk analysis	Annually
Review and update of policies	Annually
Review of the ISMS by management	At least once a year
Internal audits	Depends on what being audited: • Controls which consolidate the management system - annually • Controls which are part of the ISMS will depend on the importance of the measurement and the process or asset it is protecting. Can vary from once every 3 months to once every 3 years. Most controls should be reviewed at least once a year .
External audits	Every three years, a thorough ISMS review should be carried out, although every year the auditor will check if the ISMS is working correctly

<u>You should always try to do better…</u>

As I said before, every ISMS is created to guarantee a continuous improvement cycle. Points to improve are detected by doing the audits and reviews. Alongside that, it is important to have a process in place to detect and mitigate incidents. The main goals of the incident management process are to:

- To detect and address breaches and or vulnerabilities in a timely manner;
- To pinpoint the root cause of the incident;
- To learn from the incident.

<u>Some tips based upon my experience:</u>

- **Certification is not the goal:** In my career I have encountered organizations for which being certified was the goal. Even though I can see why, I would strongly suggest against it and especially not communicate it like that within the organization. My experience is that a lot of money, time and effort is spent in these cases and then, when the first certification audit is passed successfully, attention drops again, old habits reappear and, by the next cycle, most things need to be urgently redone right before the audit. Better to have the focus on the continuous improvement process so that the ISMS will start to work for you and not just guarantee a certification but rather also improve and streamline your organization and processes
- **Make use of the knowledge of your employees during internal audits:** No need to have an internal auditor check every measure in every process or system. One of the tactics I used was to have the system administrator of system A periodically check the implementation of the

controls on system B (not administered by him) and document the status. In that case, an internal auditor only has to check the reports and see if the controls have been checked correctly

- **Stay away from disciplinary procedures:** If an incident occurs by mistake, make sure that whoever caused the incident is not punished. Try to learn from it as an organization without placing someone on the wall of shame.
- **Start with the People:** To implement an ISMS you will need the cooperation of everybody in the organization. Raising awareness throughout the organization is a great way to get everybody on board so start with that as soon as possible.
- **Controls not in place:** Do not panic, if it is not one of the controls designed to keep the ISMS working, you won't fail an audit over it. Make sure it is well documented and in most cases I would advise to document it as a security incident and go through the incident management process to determine why it was not correctly implemented and what is the best course of action to correct it. Use the knowledge to learn from so that next time it won't happen so easily.
- **Make use of an external consultant:** Usually implementing an ISMS is not the primary business of an organization and in most organizations, especially when starting the implementation, there is not much experience available. Hiring a professional consultant can immediately provide you with the experience you need, taking away a lot of the headaches you will encounter. When hiring a consultant make sure they understand your business and speak the language of your company.

Of course the points described above only scratch the surface. In subsequent articles I will dive deeper into the material. However, if you have any questions, do not hesitate to contact myself or my Colleagues at Comsec.

Tiennot van Dilst CISSP CEH

Tiennotvd@comsecglobal.com