Deloitte.

EU Directive calls for better Information Security Management for Critical National Infrastructure

September 2014

Summary

Legal stipulation by a forthcoming EU directive will require that Critical National Infrastructure providers are able to demonstrate to the public that they have an established Information Security Management System to deal with security threats. For many organizations, this will mean that they need to formalize their current security procedures, prominently among them they need to formalize there risk assessment, integrate all security activities into a management system, implement and monitor the necessary security controls and ensure they are prepared to be audited. Although the timeframe for issuing the directive remains uncertain, our experience indicates that the implementation of an Information Security Management System is a long-term endeavor and should be started sooner rather than later.

Based on our experience, and anchored in ISO 27001, Deloitte can provide well-tested, optimized and tailored information security management approaches that can decrease implementation time while enabling a business-driven and holistic solution.

We believe that each organization should consider the following questions when determining what action is required:

- Do we (really) have all governance documents that are required for an Information Security Management System?
- Do we have a formalized risk assessment process and is information security risk analysis driven by business, organizational culture and environmental context?
- Do we (really) have all relevant security controls?
- Do we measure and control that all security controls work as we have designed them?
- Can we report incidents with all the necessary information within the required 24 hours?
- Do we have a process to ensure continuous improvement of our Information Security Management System?
- Can we show that we cover all risks?
- Would we pass an external review of our ISMS?

If the answer to any of the above is “no”, “maybe” or “do not know” you should read on

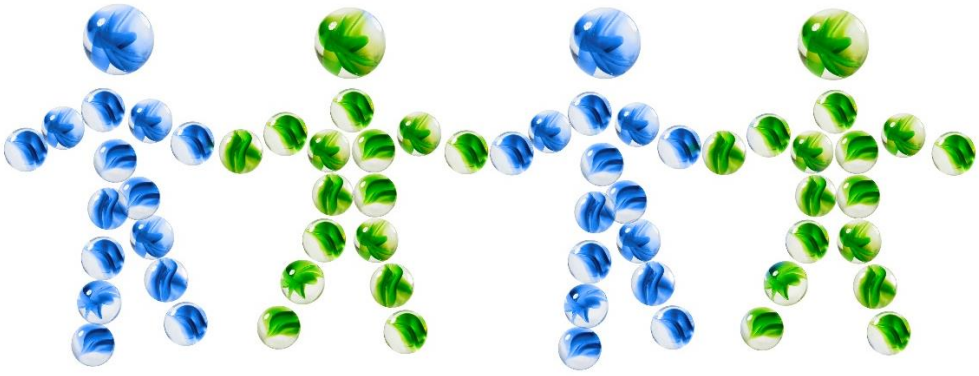
Contents

New EU Directive for network and information security

Society has become increasingly dependent on information systems and the supporting networks. Security breaches of those critical information systems and networks can severely harm society. With that in mind, the European Union is preparing a directive that will require operators of critical infrastructure, in areas such as energy, transportation, banking, health care, e-commerce, social media and public administration, to take appropriate steps to manage information security risks.

A cornerstone of this upcoming directive is that all EU member states will have to establish a competent authority that stipulates and controls, based on acknowledged security standards, that information security addresses relevant risks. For Sweden the expectation is that “Myndigheten för Samhällsskydd och Beredskap” (MSB) will become the competent authority. The fact that MSB has issued a prescript (föreskrift) which requires Swedish public administration to have an Information Security Management System (ISMS) based on ISO/IEC 27001 and a Business Continuity Management System (BCMS) based on ISO 22301, makes it reasonable to assume that the same requirements will be applied to critical infrastructure providers. According to the directive, supervision by the competent authority can be done either by performing audits themselves or by requiring critical infrastructure providers to attest to their own compliance, via self-assessments and supported by relevant documentation.

Furthermore, the directive will require national security incident management capabilities. In Sweden the established CERT.se, managed by MSB, will be given responsibility for performing national incident management. For critical infrastructure providers this will imply a reporting obligation to CERT.se for security incidents, and create expectations of their incident management capabilities, which must allow the collection of all required data, delivery of that data to a sufficient quality and establishment of routines for communication with the CERT.

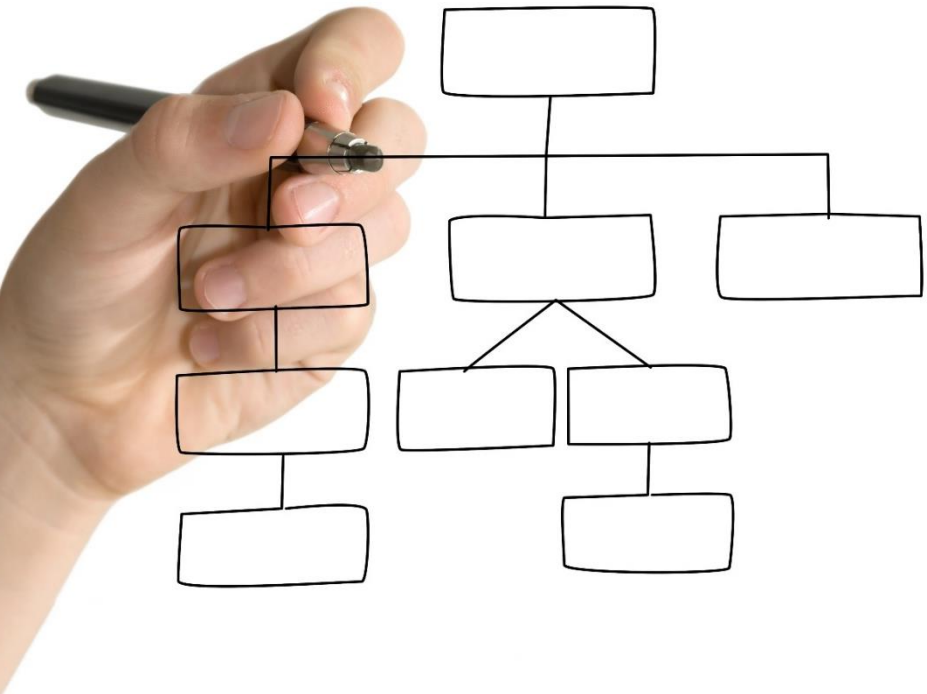


Embracing the change

We have a security policy and people working with it – no problem!

This is just the same thing we are already doing – aren't we?

Based on our experience, these are fairly common reactions among decision makers. However, assuming that having a security policy and security personnel is enough or that nothing has changed will likely be proven to be incorrect. Although most organizations have some high level steering documents and have deployed a number of security controls, they lack the Information Security Management System (ISMS) required for systematic management of information security risks. Often, we see that the link between risk exposure, security governance and the deployed security controls is not well-defined. As a consequence, the level of security protection provided is uncertain. Furthermore, we often find that the deployed security controls are not operating effectively due to a lack of governance. This increases associated costs, as either the controls do not prevent security breaches or are deployed where the risk exposure does not justify it. We also regularly witness overly ambitious (and therefore overly expensive) security controls being deployed. Finally, our experience is that information security is often treated as an add-on to existing development and operations procedures, creating friction and inefficiency.



How to improve the existing security approach to become an Information Security Management System?

If the existing approach is not sufficient, the reasonable next questions to ask are: how can the existing security (management) approach be transformed into an Information Security Management System; and how long will such a transformation take?

To address the first of these, Figure 1 presents the important activities as derived from ISO/IEC 27001. Our experience is that most attention and effort must be given to risk management, measuring and operational security management. The other activities are still critical, but are frequently already in place or need only modification to accommodate any new requirements derived from the necessary modifications in risk management, measuring and operational security management.

To the question of how long such a transformation may take and how many resources it will require, the answer naturally depends on what already exists. However, in our experience it takes 6 to 12 months to introduce an ISMS and about double that time, another 12-24 month, until the necessary controls are implemented and fine-tuned. With respect to resource requirements, we find that, under the assumption that: (a) a competent team is available; and (b) a basic security program exists, around 3 – 5 man years (about 3300 – 5500 hours) are necessary. These factors together imply that, although the legislation has not yet been issued, it may already be time for an organization to consider how to become ready.

Planning	Operation	Control	Improvement
• Scope Definition	• Control Implementation, Operation and Maintenance	• Measuring	• Continuous Improvement
• Policy	• Reporting	• Internal Control	• Compliance Management
• Risk Analysis & Control Definition	• Continuous Risk Management	• Management Review	

Figure 1 ISMS activities

Deloitte’s ISMS approach

Our view is that for a comprehensive approach (outlined in Figure 2) it is important to consider the business sector, the culture and the environmental context of the organization to determine what security is necessary. Further, our approach considers the need for responsiveness in mitigating modern cybersecurity risks, the importance of integrating an ISMS into existing organizational structures and routines, and the ongoing need to demonstrate the business benefits of information security investments.

Due to its broad acceptance, and the fact that it will (most likely) be prescribed by regulative power, we base our approach on ISO 27001 and extend it where necessary. Initially the ISO standard is concerned with identifying interested parties which we complement with the internal processes, organizational structure and the information system landscape. Based on the needs of the identified stakeholders, an ambition level and the resulting scope for the ISMS should be set and amendments to the policy and governance framework should be implemented (see Fig. 2 - Deter).

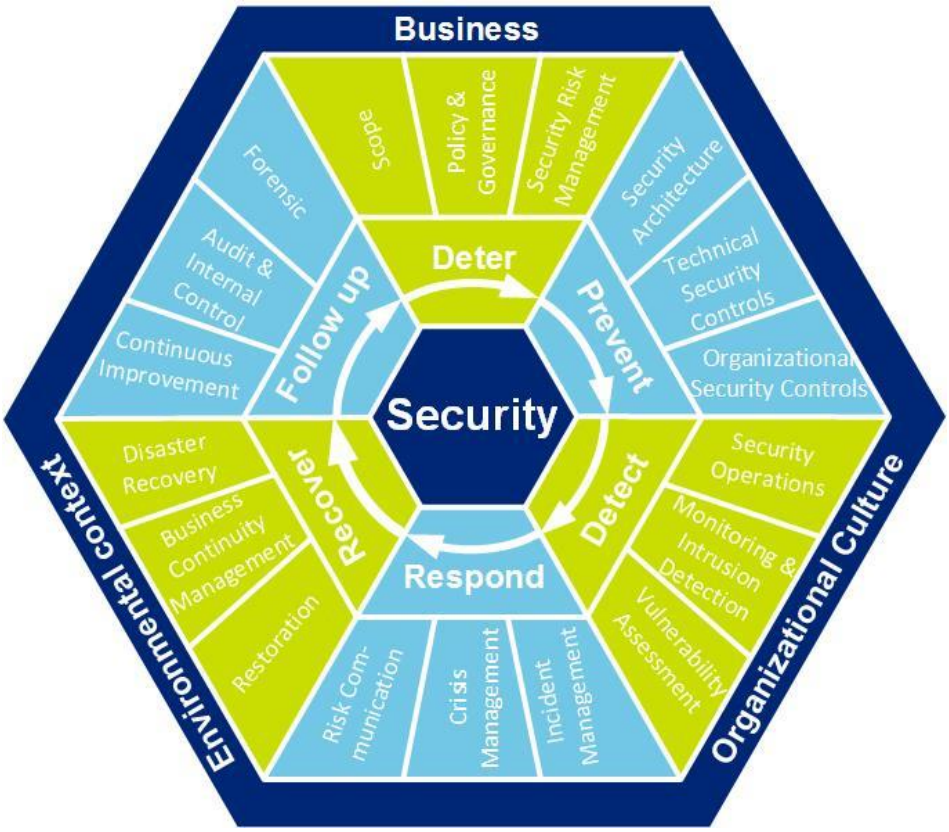


Figure 2 Deloitte’s ISMS approach

Subsequently the security architecture has to link risk assessment with security controls, while also being observant to the organization's business needs, rather than to abstract threats. The challenge is to employ risk assessment in a holistic and multi-layered manner that simultaneously considers organizational, economic and technical aspects for the security controls. Our experience shows that it may be more effective to implement detection and response capabilities instead of preventive security controls (i.e. a balance must be struck between Prevent, Detect, Respond and Recover in Fig. 2). Modern cyber risks require organizations to be aware, prepared and responsive. We believe that the interdependency between these aspects must be addressed on strategic, tactic and operational levels. We find the integration of organizational and technical controls a key success factor, particularly at the operational level.

A good example would be incident management. We frequently observe that organizations have an incident reporting scheme as part of their operational IT management, which implies a heavy technical focus. This often results in security incidents not being correctly identified, and for those security incidents that are correctly identified, insufficient information is collected. This is a failure of the organizational control and has a twofold consequence. Firstly, we have found that while the immediate effect of an incident is handled there is rarely a follow up to investigate or correct the root cause. Secondly, a lack of information prevents the organization from continuously improving its ISMS. In future it is also likely that this will create problems with respect to the obligation to report to the national CERT.

To accommodate the need for responsiveness and to ensure the required continuous improvement, a critical capability is to be able to automatically monitor and measure the ISMS (linking detection activities to follow-up activities - see Fig. 2). This will provide the organization with improved response capabilities, as part of their operational security management, and with the necessary data to identify where the greatest improvement potential is. Naturally, the process to make use of this information is a must to keep the ISMS focused and well-tuned.

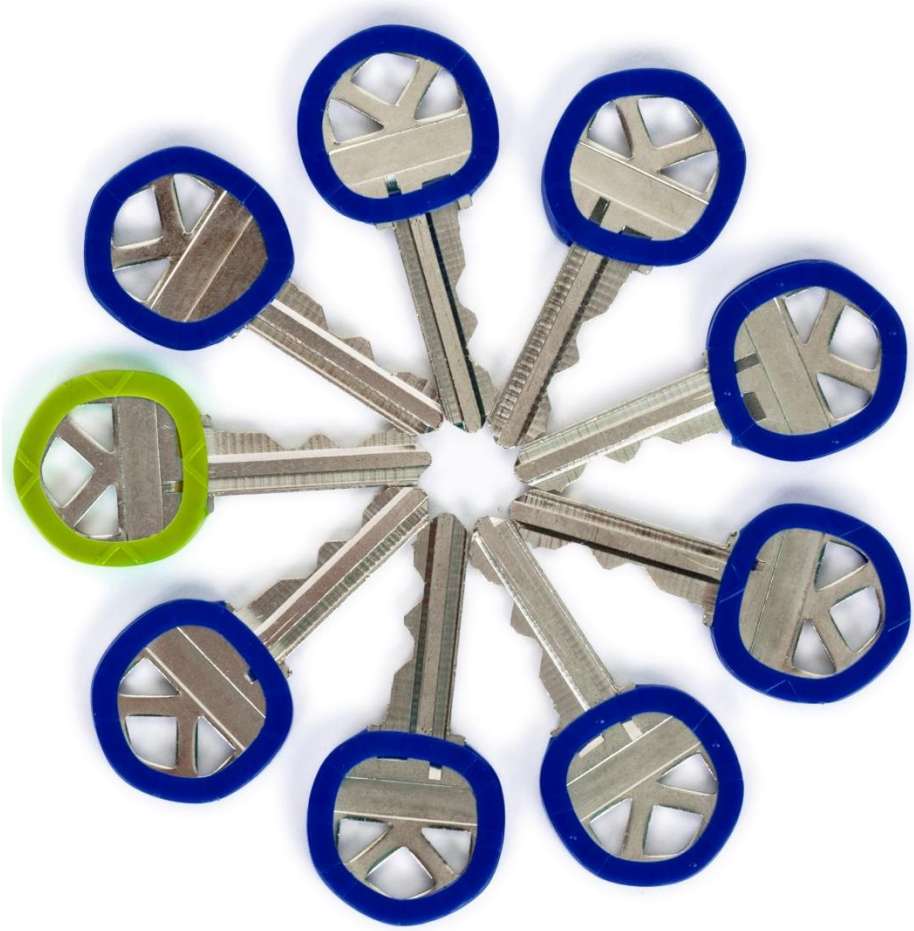
Furthermore, we believe that security must integrate easily with existing organizational structures and processes. To achieve this Deloitte has developed, tested and tuned tools and templates for the ISMS activities that provide reliable and well-tried solutions. Our templates and tools encompass, amongst others, the following key accelerators:

- Security and privacy policy, instruction and guideline templates;
- IT Risk Management Framework;
- Security control catalogues;
- Integrated security requirement libraries;
- Security tuned continuous improvement approaches;
- Internal control procedures; and
- Cultural change methods.

By adapting these tools and templates to the unique demands of the organization, the implementation activities are likely to be significantly accelerated.

Ultimately, the key for long term success is the capability to uphold an appropriate level of security. This is dependent on security investments providing constant benefits without introducing undue burdens. Information security therefore becomes a constant journey where the Information Security Management System describes, like a travel plan, how and by what means the journey is conducted.

If you have further questions or would like to discuss with us do not hesitate to contact us.



Contacts

Marcus Sörlander
Partner
Enterprise Risk Services
msoerlander@deloitte.se
+46 752 46 20 00

Dr. Albin Zuccato
Manager
Enterprise Risk Services
azuccato@deloitte.se
+46 752 46 23 40

Stefano Goudarzi
Manager
Enterprise Risk Services
sgoudarzi@deloitte.se
+46 752 46 30 13

Ronny Lundvall
Manager
Enterprise Risk Services
rlundvall@deloitte.se
+46 752 46 33 43