Continuous Security

Value creation through Continuous Security.
By Bart de Best

Context:
This blog was written based on an experience with designing an Information Security Value System (ISVS) at a supplier of a streaming service organisation.

Challenge:
The challenge of this assignment was that there was no awareness for information security, and this was experienced as a delaying factor and also had a cost-increasing effect on the total cost of ownership.

Solution:
The solution to this challenge has been found in the concept of Continuous Security. This blog discusses this approach in broad terms based on the following steps:

1. Translate from ISMS to ISVS
2. Determining the ISVS security practices
3. Determining the ISVS
4. Determining the ISVS value streams
5. Implementation of the ISVS
6. The certification

1. Translate from ISMS to ISVS

The ISO 27001 standard consists of the description of the Information Security Management System (ISMS). This ISMS describes the method for operationalising information security. In addition, this standard describes a very extensive set of information security controls in the appendices. A control is a countermeasure to a risk.

The vision for applying information security at this organisation is based on the view that information security, just like service management, as defined within ITIL 4, must add value to the business value streams. That is why the name Information Security Value System (ISVS) was chosen instead of ISMS. This is in analogy to the renaming of Service Management System (SMS) to Service Value System (SVS). This seems like an arbitrary choice, but it has resulted in a fundamentally different interpretation of information security as described in this blog.

2. Determining ISVS security practices

The SVS of ITIL 4 is no longer based on processes but on value streams. Which value streams should be applied is not defined by ITIL 4.
However, management practices have been defined that can be used to define value streams yourself based on the need for this. In order to define the ISVS in analogy with the SVS, security practices have been defined as depicted in Figure 1.

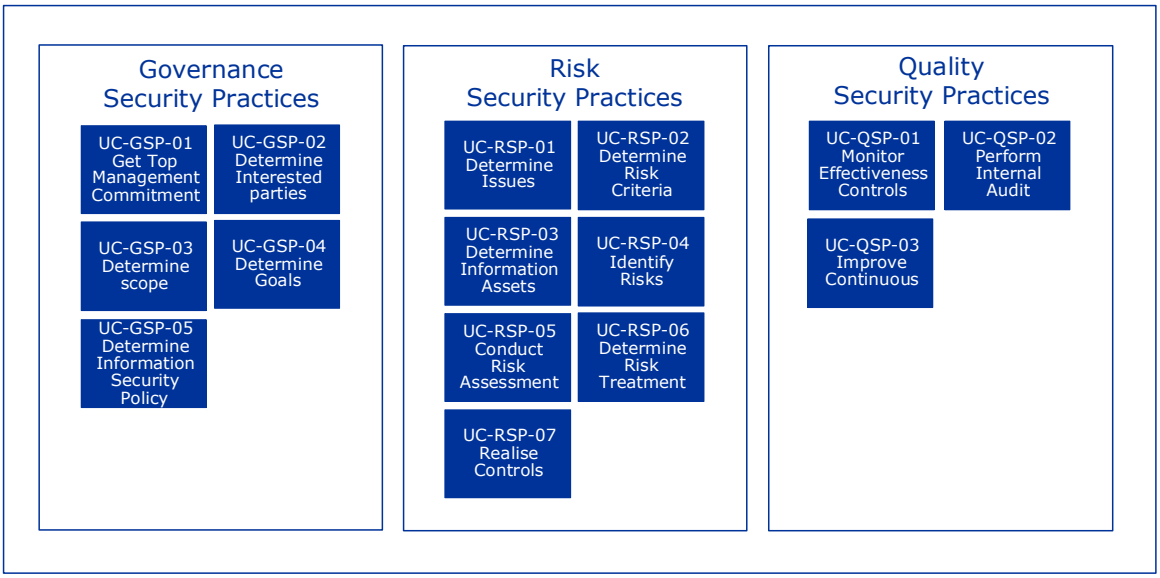


Figure 1, Information security practices.

The governance security practices are the guiding practices of the ISVS. The risk security practices fulfil the risk management aspect of the ISVS. The quality security practices provide substance to the ISVS measurement and control system. Together, these security practices implement all the methods mentioned in ISO 27001 to manage the lifecycle of information security controls.

3. Determining the ISVS

The ISVS is depicted in figure 2. The ISVS is based on the information security architecture that defines architectural models and principles for information security. The information security value chain is shown in the centre of figure 2.

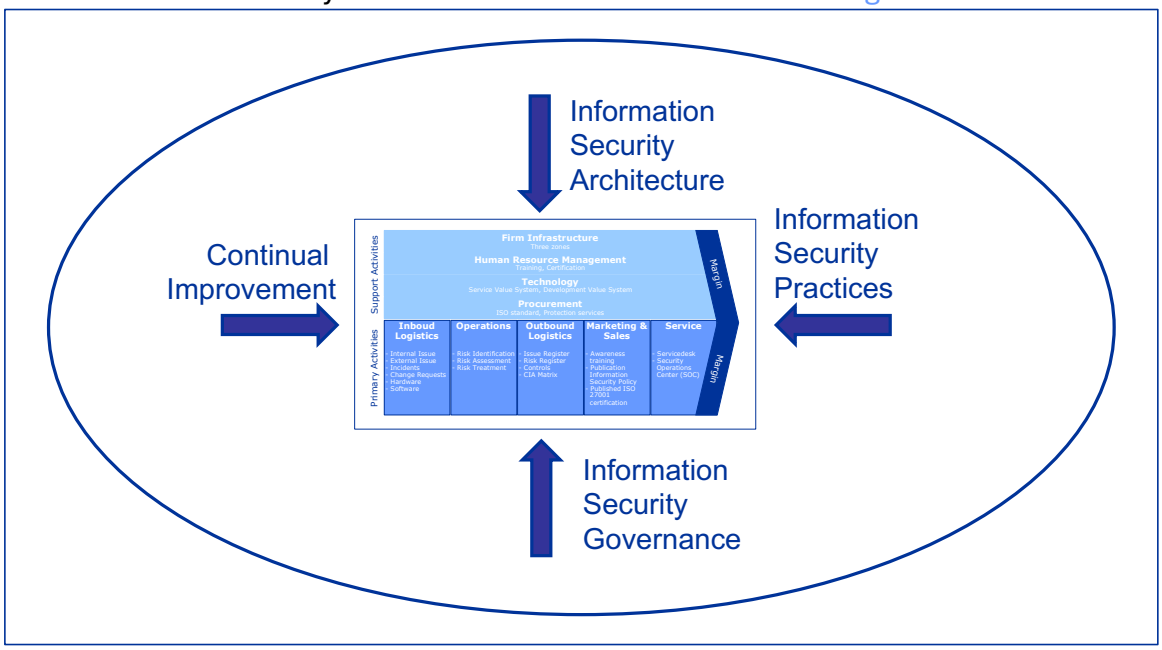


Figure 2. The Information Security Value System (ISVS).

4. Determining the ISVS value streams

Figure 3 shows examples of information security value streams.

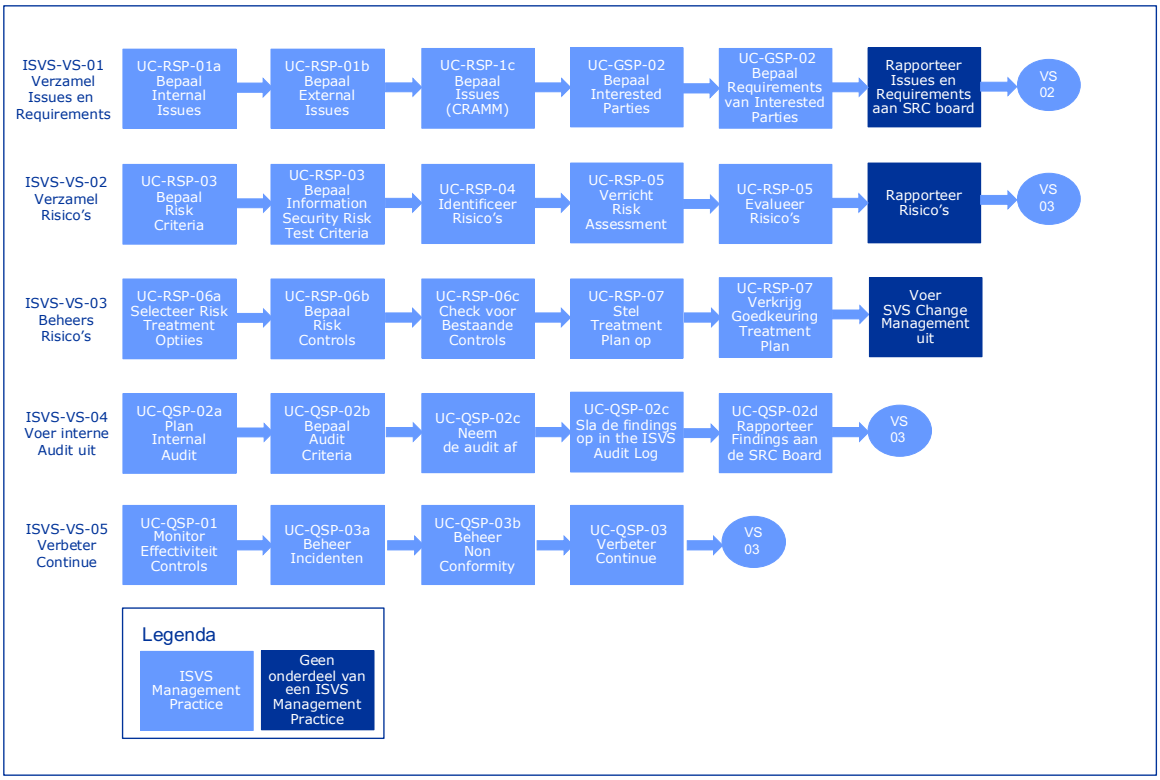


Figure 3. Examples of information security value streams.

These information security value streams can be chosen based on the security practices. Together, these security value streams form the information security value chain. The ISVS and the SVS can be properly coordinated or integrated with each other thanks to this information security architecture.

5. Implementation of the ISVS

The business value streams can also be regarded as a value system, namely the Business Value System (BVS), as shown in figure 4. This value system also consists of a value chain in which business value streams are defined. This BVS guides the implementation of the ISVS by defining the Non-Functional Requirements (NFR). These can be divided into Confidentiality, Integrity, and Accessibility (CIA) requirements.

These CIA requirements must be translated into the Development Value System (DVS) that develops the information systems and the SVS of ITIL that manages the information systems. The ISVS ensures that this CIA requirement analysis takes place and that the DVS and SVS translate this into security controls for the information systems. The DVS must build these controls and the SVS must manage them.

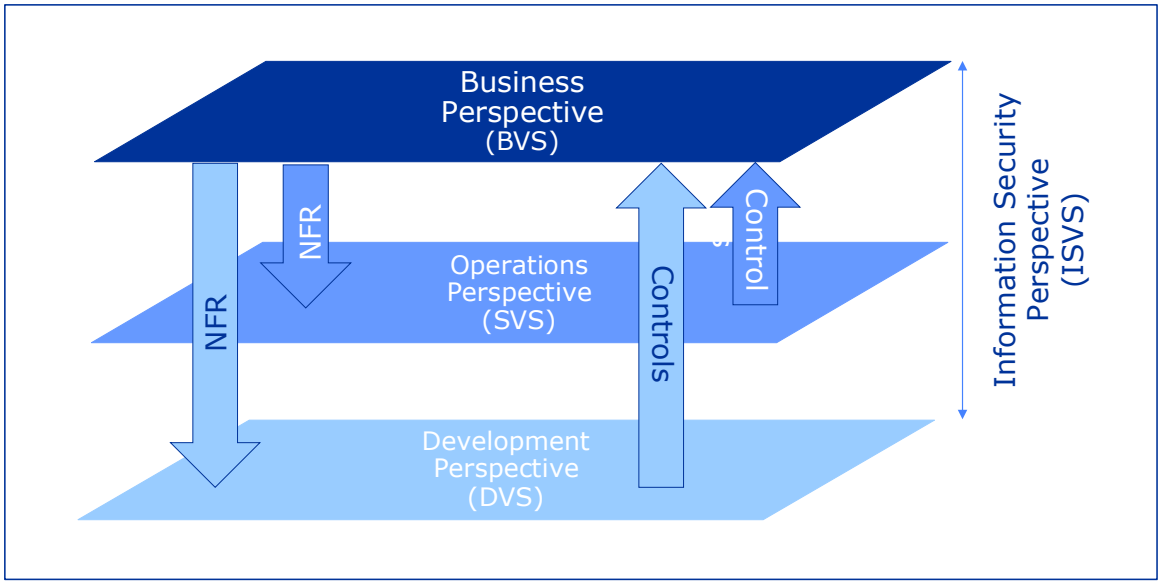


Figure 4, ISVS as integrator of the BVS, SVS and DVS.

An example of this integration of value systems is shown in Figure 5. This figure shows the DevOps Lemniscate. The DVS is depicted on the left and the SVS on the right. Each of the steps in the DevOps Lemniscate indicates what the role is in realising and operationalising the information security controls, as defined by the ISVS.

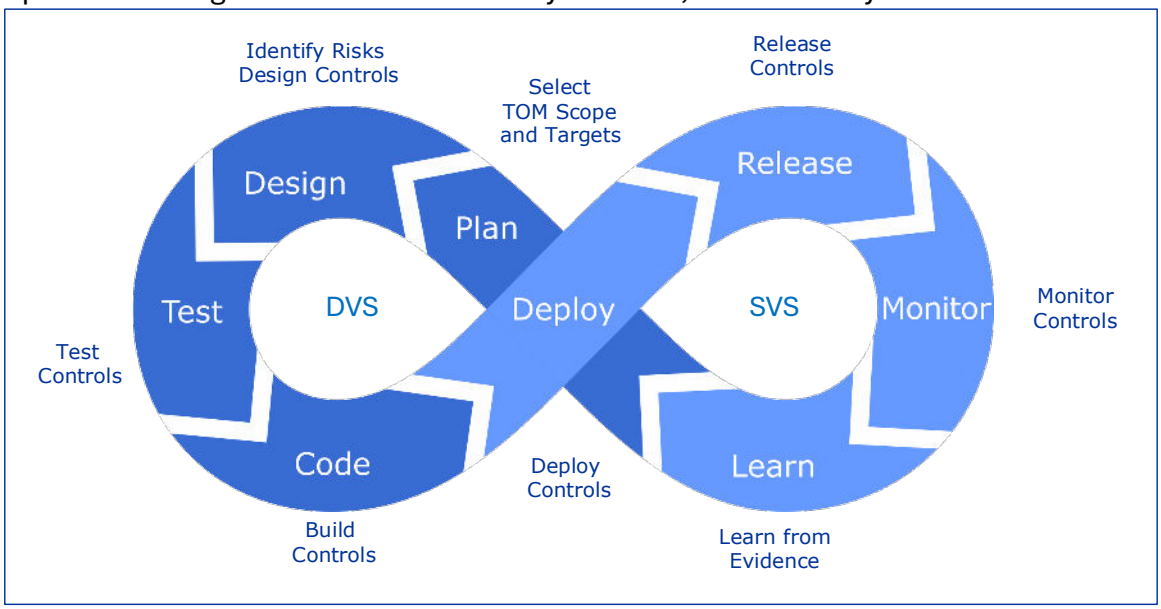


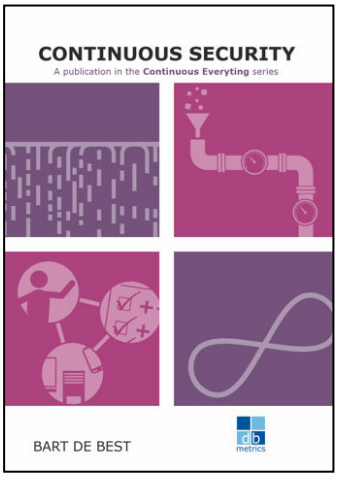
Figure 5, Information security control lifecycle management.

6. The certification

The approach to derive information security controls from the goals of the business value streams in the BVS has led to the supplier's directors gaining direct insight into the importance of the information security controls. In particular, the responsibility of being in possession of the streaming service customer's information assets and the information security controls needed to protect them made a deep impression and was the deciding factor to invest in the information security controls. This investment is now seen as an opportunity to increase outcomes for your own organisation and customers.

By securing the information security controls from the ISVS in the value streams of the DVS and SVS of the DevOps teams, the Continuous Security concept has been implemented. This is because there is no longer annual attention to the ISVS due to an audit, but monitoring of being in control takes place in every DevOps sprint from both development and operations. The ISVS was built in 6 months and went live in 3 months. The auditors were amased by this unique approach and were proud to sign the certificate.

By Bart de Best
DutchNordic.Group



https://www.dbmetrics.nl/ce-en/continuous-security-en/