Continuous Security

Waardecreatie door Continuous Security.
Door Bart de Best

Context:
Deze blog is geschreven op basis van een ervaring met het vormgeven van een Information Security Value System (ISVS) bij een leverancier van een streaming service organisatie.

Uitdaging:
De uitdaging van deze opdracht was dat er geen awareness was voor information security en dit als een vertragende factor ervaren werd en daarenboven een kostenverhogende werking had op de total cost of ownership.

Oplossing:
De oplossing voor deze uitdaging is gevonden in het concept van Continuous Security. Deze blog bespreekt deze aanpak op hoofdlijnen aan de hand van de volgende stappen:

1. Vertalen van ISMS naar ISVS
2. Bepalen van de ISVS security practices
3. Bepalen van het ISVS
4. Bepalen van de ISVS value streams
5. Implementatie van het ISVS
6. De certificering

1. Vertalen van ISMS naar ISVS

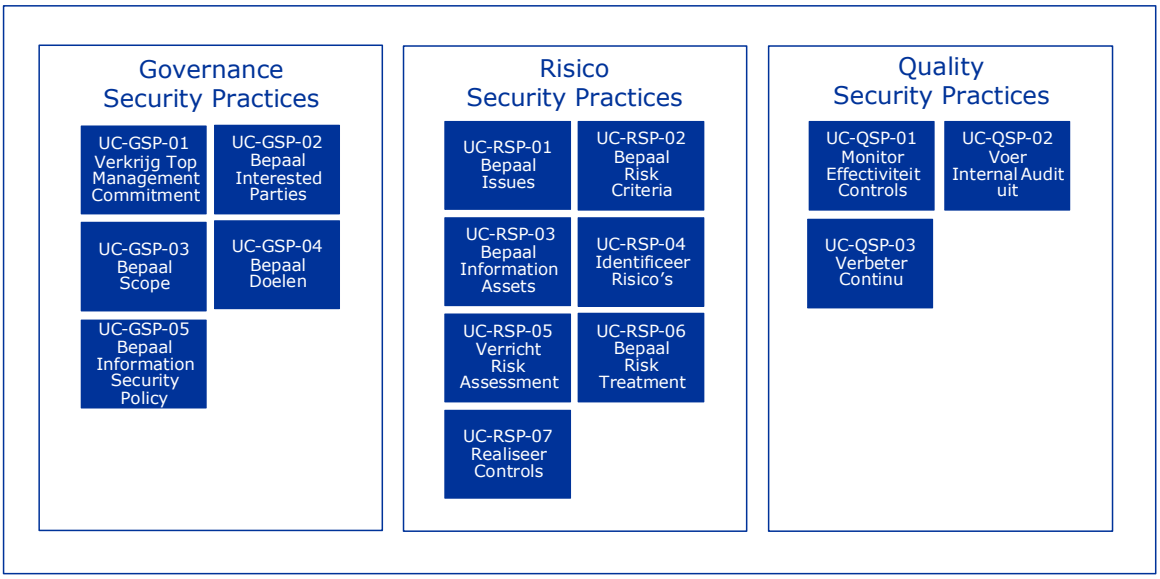
De ISO 27001 norm bestaat uit de beschrijving van het Information Security Management System (ISMS). Dit ISMS beschrijft de werkwijze om information security te operationaliseren. Daarnaast beschrijft deze norm in de bijlagen een zeer uitgebreide set van information security controls. Een control is een tegenmaatregel voor een risico.

De visie die voor het toepassen van information security bij deze organisatie is gebaseerd op de zienswijze dat information security net als service management, zoals gedefinieerd binnen ITIL 4, waarde moet toevoegen aan de business value streams. Daarom is gekozen voor de naam Information Security Value System (ISVS) in plaats van ISMS. Dit in analogie van het hernoemen van Service Management System (SMS) naar Service Value System (SVS). Dit lijkt een arbitraire keuze, maar heeft gezorgd voor een fundamentele andere invulling van information security zoals in deze blog is beschreven.

2. Bepalen van ISVS security practices

Het SVS van ITIL 4 is niet meer gebaseerd op processen maar op value streams. Welke value streams toegepast moeten worden is niet door ITIL 4 gedefinieerd. Wel zijn er management practices gedefinieerd die gebruikt kunnen worden om zelf value streams te definiëren op basis van de behoefte daartoe.

Om het ISVS in analogie met het SVS te kunnen definiëren zijn dan ook security practices gedefinieerd zoals afgebeeld in figuur 1.

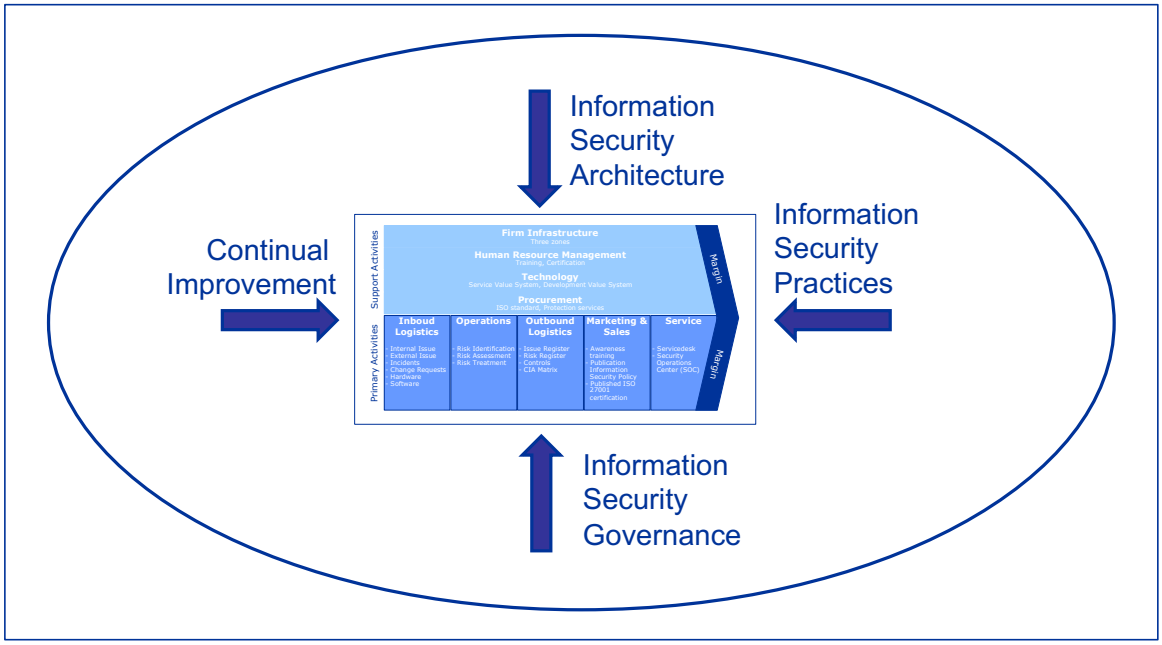


Figuur 1, Information security practices.

De governance security practices zijn de sturende practices van het ISVS. De risico security practices geven invullen aan het risicomanagement aspect van het ISVS. De quality security practices geven invulling aan het meet- en regelsysteem van het ISVS. Samen geven deze security practices invulling aan alle in de ISO 27001 genoemde werkwijze om de lifecycle van information security controls te managen.

3. Bepalen van het ISVS

Het ISVS is afgebeeld in figuur 2.

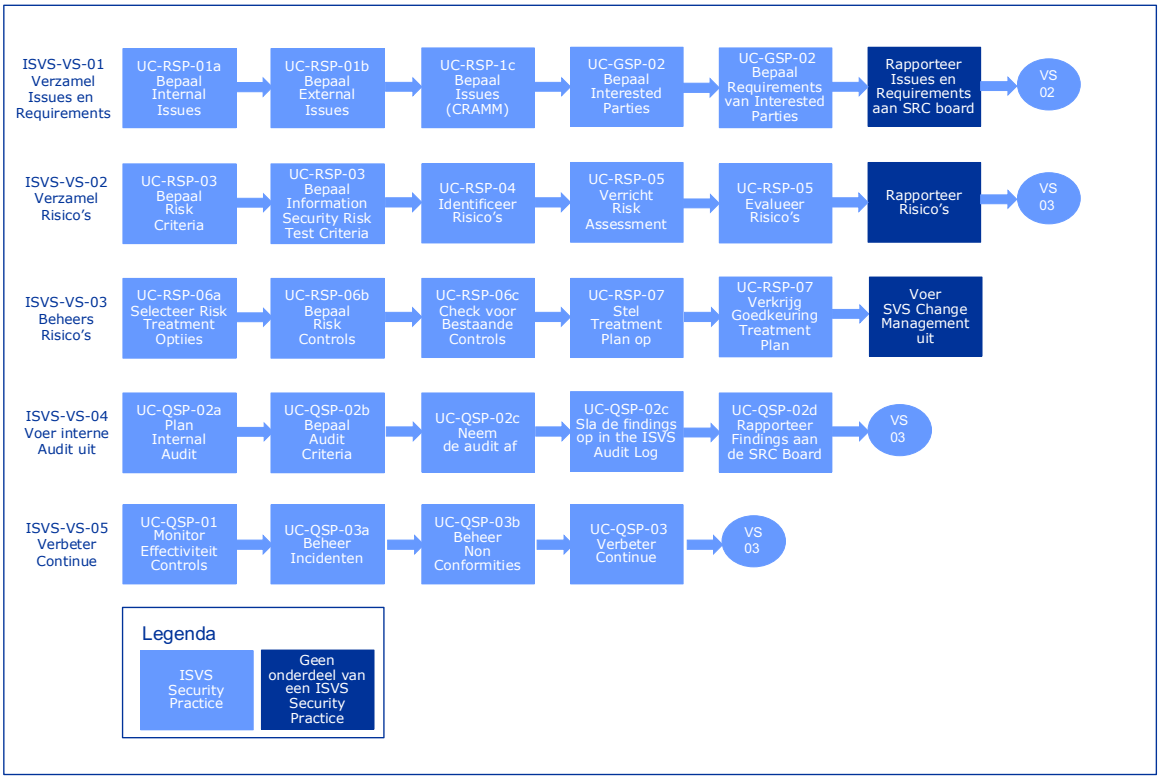


Figuur 2. Het Information Security Value System (ISVS).

Het ISVS is gebaseerd op de information security architectuur die architectuur-modellen en -principes voor information security definieert. De information security value chain is in het centrum van het figuur 2 weergegeven.

4. Bepalen van de ISVS value streams

Figuur 3 geeft voorbeelden van information security value streams.



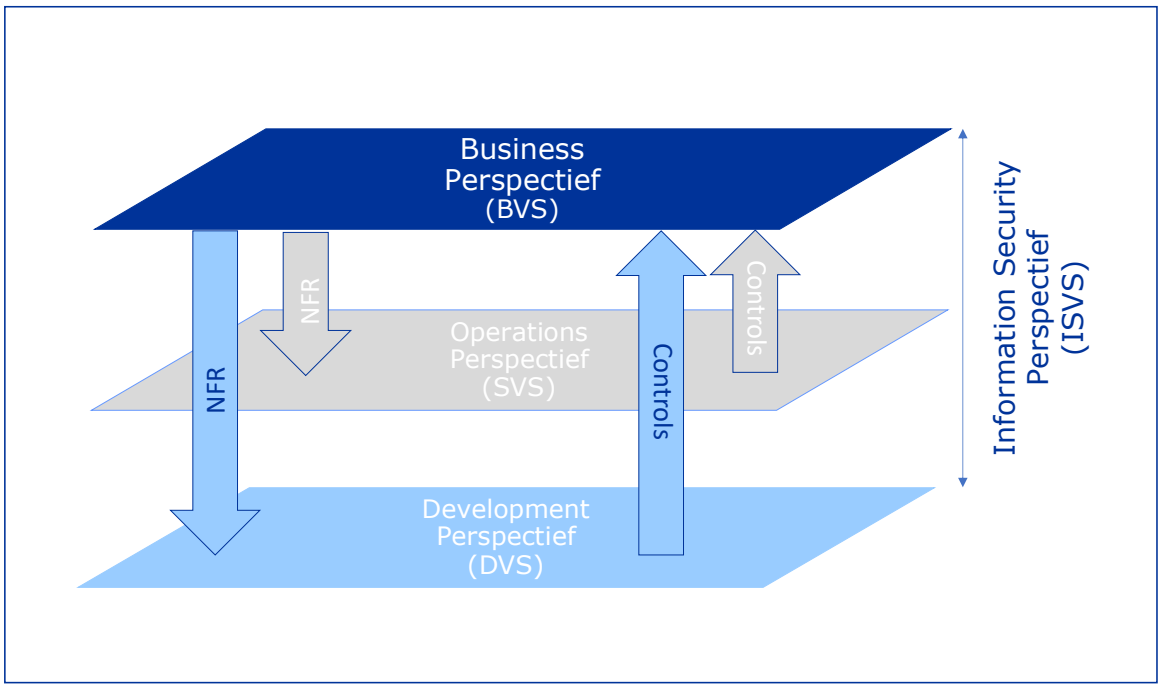
Figuur 3. Voorbeelden van information security value streams.

Deze information security value streams kunnen gekozen worden op basis van de security practices. Samen vormen deze security value streams de information security value chain. Het ISVS en het SVS zijn door deze information security architectuur goed op elkaar af te stemmen dan wel te integreren.

5. Implementatie van het ISVS

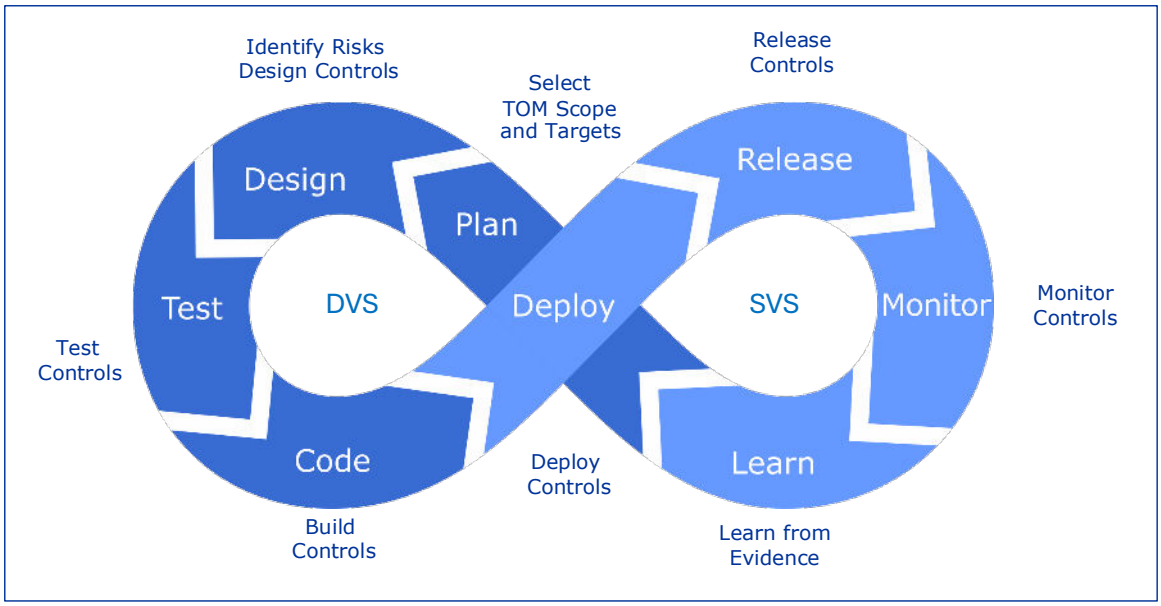
De business value streams zijn ook te beschouwen als een value system en wel het Business Value System (BVS), zoals weergegeven in figuur 4. Ook dit value system bestaat uit een value chain waarin business value streams gedefinieerd zijn. Dit BVS geeft de sturing aan de invulling van het ISVS en wel door de Non-Functional Requirements (NFR) te definiëren. Deze zijn op te delen in Confidentiality, Integrity en Accessibility (CIA) eisen.

Deze CIA eisen moeten vertaald worden naar het Development Value System (DVS) dat de informatiesystemen ontwikkelt en het SVS van ITIL dat de informatiesystemen beheert. Het ISVS borgt dat deze CIA requirement analyse plaatsvindt en dat het DVS en SVS deze vertalen naar security controls voor de informatiesystemen. Het DVS moet deze controls bouwen en het SVS moet deze beheersen.



Figuur 4, ISVS als integrator van het BVS, het SVS en DVS.

Een voorbeeld van deze integratie van value systems is in figuur 5 afgebeeld. In deze figuur is het DevOps Lemniscaat weergegeven. Aan de linkerkant is het DVS afgebeeld en aan de rechter kant het SVS. Bij elke van de stappen in het DevOps Lemniscaat is aangegeven wat de rol is om de information security controls, zoals gedefinieerd door het ISVS, moeten worden gerealiseerd en geoperationaliseerd.



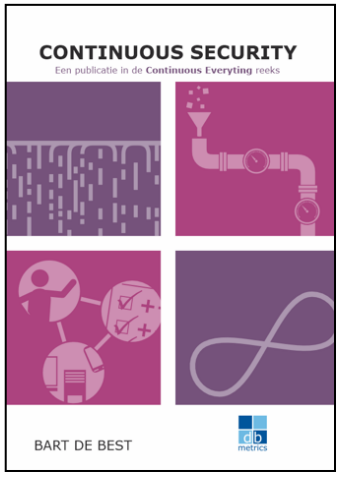
Figuur 5, Information security control lifecycle management.

6. *De certificering*

De aanpak om information security controls af te leiden van de doelen van de business value streams in het BVS heeft ertoe geleid dat het voor de bestuurders van de leverancier direct inzicht heeft gekregen in het belang van de information security controls. Vooral de verantwoordelijkheid van het in bezit zijn van de informatie assets van de streaming service klant en de information security controls die nodig zijn om deze te beschermen maakte diepe indruk en gaf de doorslag om te investeren in de information security controls. Deze investering wordt nu gezien als een mogelijkheid om outcome te verhogen voor de eigen organisatie en klanten.

Door de information security controls vanuit het ISVS te borgen in de value streams van het DVS en SVS van de DevOps teams is invulling gegeven aan het Continuous Security concept. Dit omdat er nu niet meer jaarlijks aandacht is voor het ISVS vanwege een audit maar in elke DevOps sprint zowel vanuit development als operations monitoring plaatsvindt van het in control zijn. Het ISVS is in 6 maanden gebouwd en in 3 maanden live gegaan. De auditors waren verbaasd over deze unieke aanpak en waren trots op het ondertekenen van het certificaat.

Door Bart de Best
DutchNordic.Group



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