CREATING IT SECURITY SPECIFICATIONS

Solving Business IT Problems

Version	:	0.3
Date	:	5-8-2015
Status	:	DRAFT
Author	:	Maikel Mardjan

Growth
No Complexity

IMPORTANCE OF SPECIFICATIONS

Every organisation is different. However when you are faced with the challenge to create a new (IT) product or service having requirements before you start will help. Always.

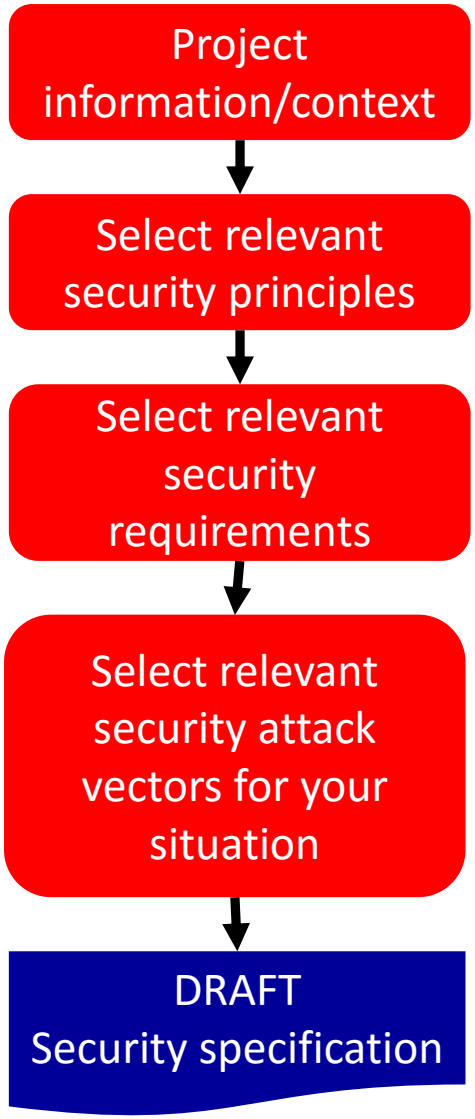
Creating security specifications is ***complex.*** IT Security is knowledge intensive and many stakeholders and government regulations can be involved.

We have simplified this complex but crucial step in every project.

Growth
No Complexity

How does it work

We create 80% of the document for you! (Based on your selections)



Every step is optional! Even the first.

No email address is required to use the tool

Knowing in advanced exact all your requirement is not agile. Principles will guide your development all the way!

Some security requirements are always the same. Choose which will apply for you.

Attack vectors mean you know what you do. The most used attack vectors are pre-selected. You just have to select which apply for your situation.

The DRAFT security specification is directly delivered online. You can also download the html export to add more requirements later in the text editor of your choice!

Requirements prioritisation

Since security is always in the end risk based we recommend that you prioritise your chosen requirements. We use the de-facto standard: the acronym MoSCoW.

This stands for:

M – MUST: have this.

S – SHOULD: have this if at all possible.

C – COULD: have this if it does not effect anything else.

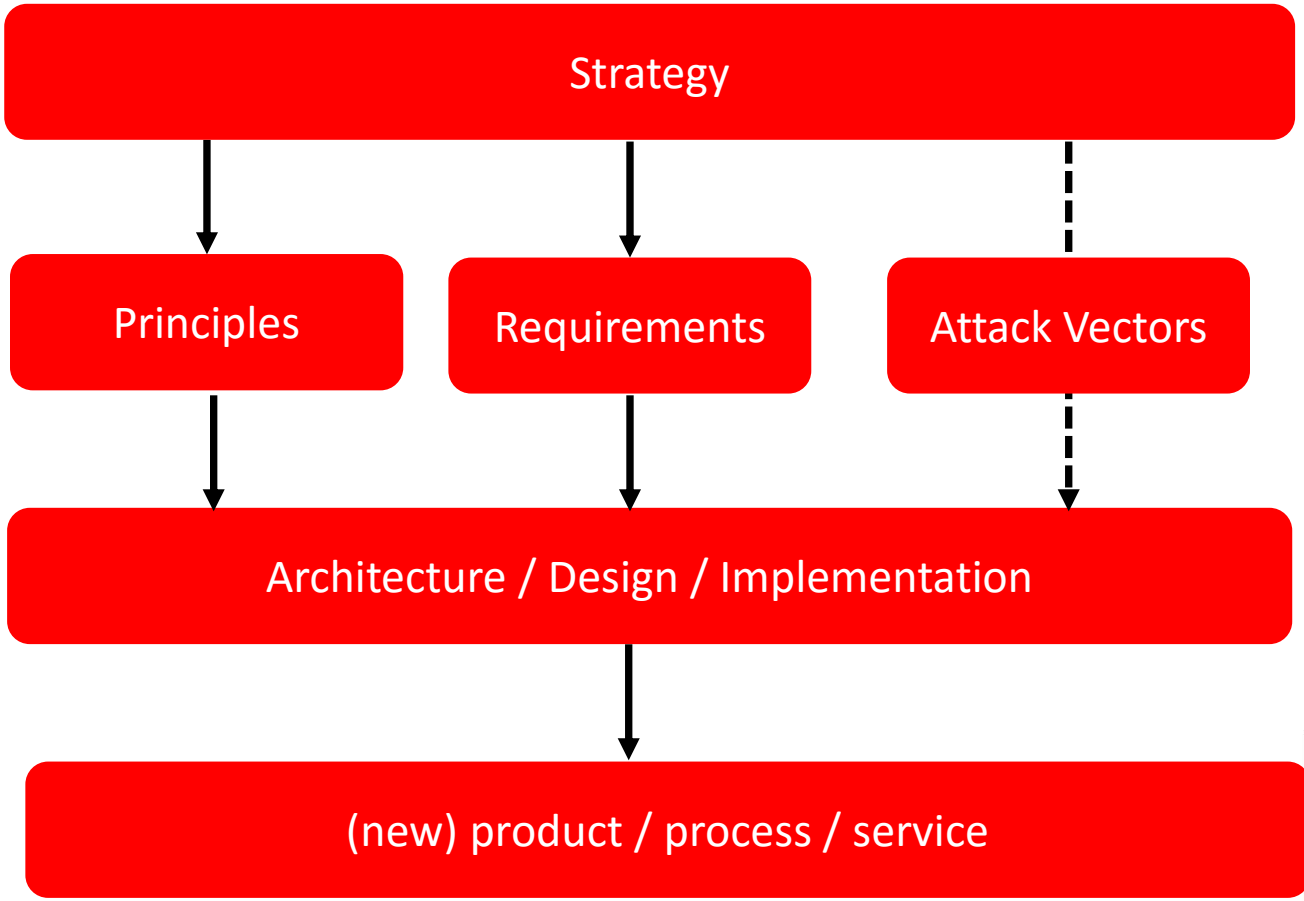
W - WON'T: have this not now, but would like this in the future.

Requirements marked as "Won't" are potentially as important as the "Must" category. Classifying something as "Won't" acknowledges that it is important, but can be left for a future release. In fact a great deal of time might be spent in trying to produce a good "Won't" list. This has three important advantages:

1. Stakeholders/Users do not have to fight to get something onto a requirements list.
2. Thinking about what will be required later, affects what is asked for now.
3. The designers seeing the future trend can produce solutions that can accommodate these requirements in a future release.

What are security principles?

Security Principles are statements of direction that govern selections and implementations. Security principles provide a foundation for decision making and are a fundament for the project.



Growth
No Complexity

Attack Vectors

The attack vectors for you to reuse are:

- Quality factors based on OWASP-top 10: Select what is relevant in your case and make sure testing/inspection takes place!
- Security personas: Security personas identify the user motivations, expectations and goals responsible for driving bad behaviour. See: https://nocomplexity.com/security-personas/
- Security attack vectors: See https://nocomplexity.com/attack-vectors/ for a in depth explanation.

About the tool

The goal of the tool is to simplify the complex task of creating security specifications. Security is complex. So instead of being busy of the easy things, we created this tool so you can focus on the 20% real challenges when creating security specifications. The easy 80% is now just to select what has been proven right the last 50 years!

Currently the tool is in beta stage. The software used to create the tool is 100% GPL licensed.

Please contact us (see next slide) if you want to join this project.

The ***real challenge*** is to create working solutions based on your requirements. We love IT design challenges, so if you need assistance to create a solution architecture of IT design based on your security specifications: **Contact Us!**

We also can provide consultancy services and organize workshops to create good security requirements for your project!

Growth
No Complexity

CONTACT?

Call : +31 [0] 6 22869536 or
mail : info@nocomplexity.com

' No man is wise enough by himself'

Plautus

THE Open GROUP
TOGAF™ 9 Certified

CISSP

OWASP
Open Web Application Security Project

Growth
No Complexity