Improving the chances of success in security for your Software development

Daniela Soares Cruzes

Espen Johansen

Who are we?

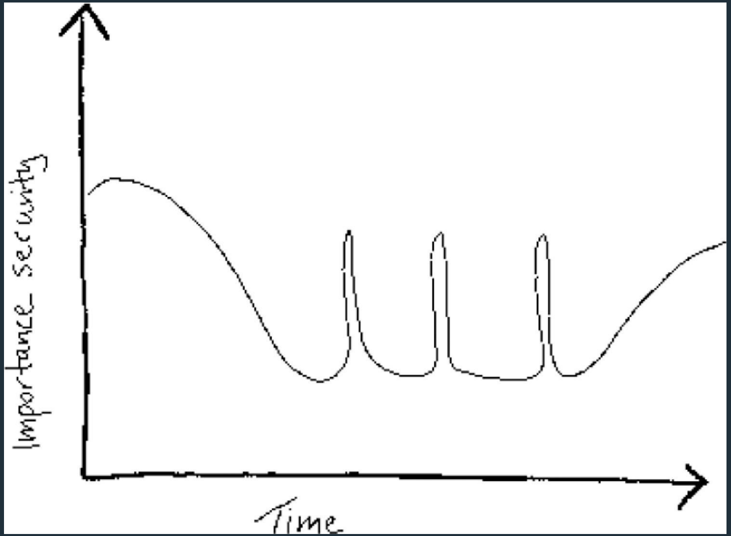
Daniela Cruzes

Prof. in Software Security and Software Engineering, NTNU
Lead Security Researcher - VISMA
daniela.soares.cruzes@visma.com

Espen Johansen

Chief Security Officer - Visma
espen.johansen@visma.com

Security Prioritisation?



Prioritisation among security requirements and activities

Prioritisation of security vs. other aspects such as functionality

The priority and attention given to security in the day-to-day work

Figure from: Inger Anne Tøndel, Daniela Soares Cruzes, Martin Gilje Jaatun, Guttorm Sindre, **Influencing the security prioritisation of an agile software development project,** Computers & Security, Volume 118, 2022, https://doi.org/10.1016/j.cose.2022.102744

Inger Anne Tøndel

Doctoral thesis

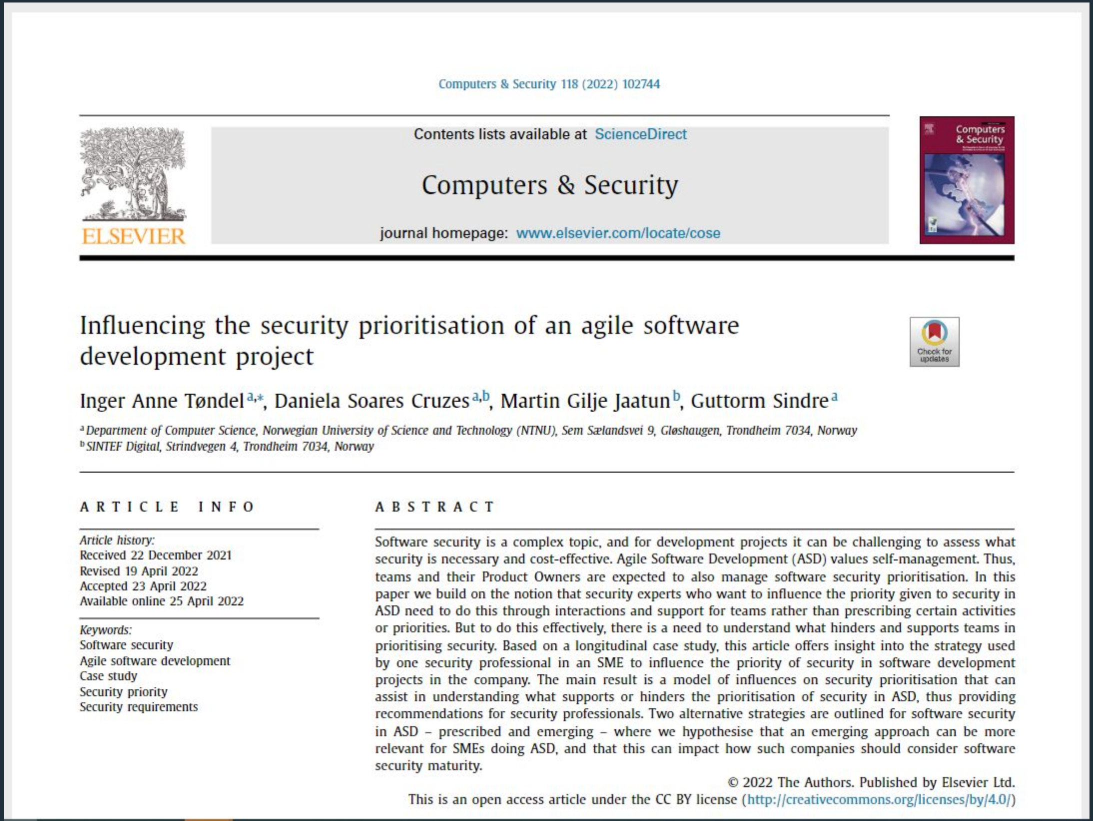
Doctoral theses at NTNU, 2022:285

Inger Anne Tøndel

Prioritisation of security in agile software development projects

https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3022462 t

Case study



Computers & Security 118 (2022) 102744

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Influencing the security prioritisation of an agile software development project

Inger Anne Tøndel[a,*], Daniela Soares Cruzes[a,b], Martin Gilje Jaatun[b], Guttorm Sindre[a]

[a] Department of Computer Science, Norwegian University of Science and Technology (NTNU), Sem Sælandsvei 9, Gløshaugen, Trondheim 7034, Norway
[b] SINTEF Digital, Strindvegen 4, Trondheim 7034, Norway

ARTICLE INFO

Article history:
Received 22 December 2021
Revised 19 April 2022
Accepted 23 April 2022
Available online 25 April 2022

Keywords:
Software security
Agile software development
Case study
Security priority
Security requirements

ABSTRACT

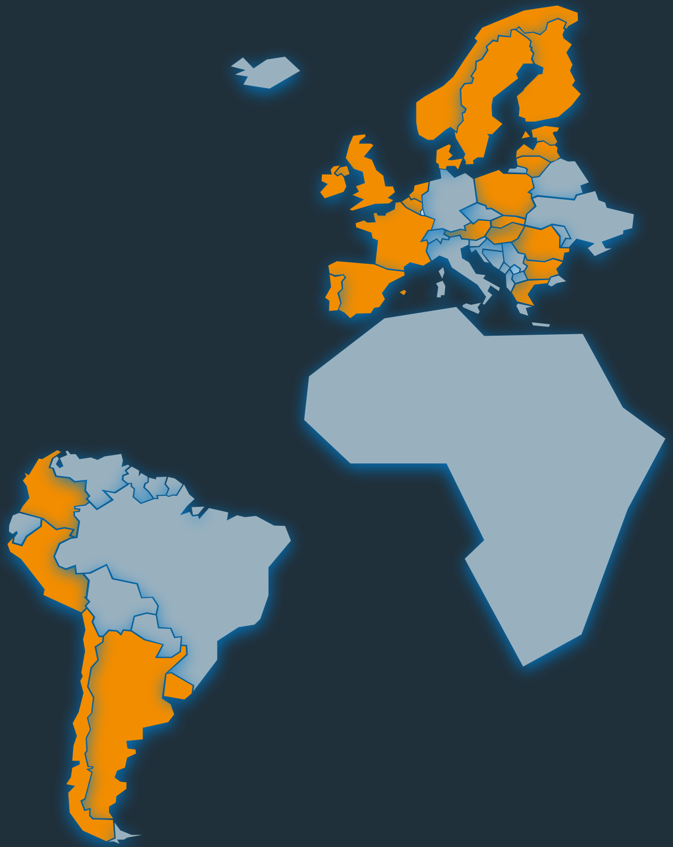
Software security is a complex topic, and for development projects it can be challenging to assess what security is necessary and cost-effective. Agile Software Development (ASD) values self-management. Thus, teams and their Product Owners are expected to also manage software security prioritisation. In this paper we build on the notion that security experts who want to influence the priority given to security in ASD need to do this through interactions and support for teams rather than prescribing certain activities or priorities. But to do this effectively, there is a need to understand what hinders and supports teams in prioritising security. Based on a longitudinal case study, this article offers insight into the strategy used by one security professional in an SME to influence the priority of security in software development projects in the company. The main result is a model of influences on security prioritisation that can assist in understanding what supports or hinders the prioritisation of security in ASD, thus providing recommendations for security professionals. Two alternative strategies are outlined for software security in ASD – prescribed and emerging – where we hypothesise that an emerging approach can be more relevant for SMEs doing ASD, and that this can impact how such companies should consider software security maturity.

What influences the security prioritisation throughout an agile sw development project?

www.sciencedirect.com/science/article/pii/S0167404822001390

Visma Context

- ~300 self managed companies
- 700 + development teams
- 50+ Acquisitions/year
- We have a **large and diversified** technology stack
- **Wide network** of distributors and partners



Visma Security Program **(VSP)**

empowers software teams in Visma to autonomously manage security

“Help others make good security decisions every day”

Influences to the priority given to security

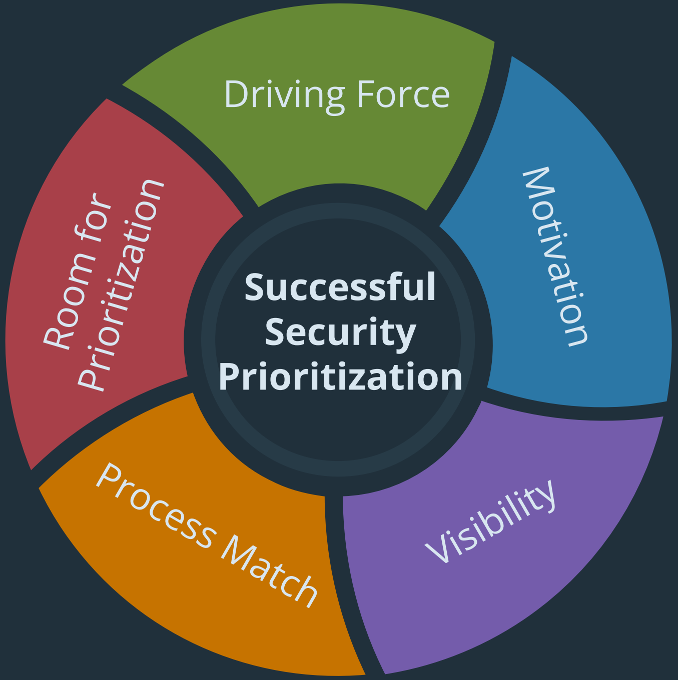
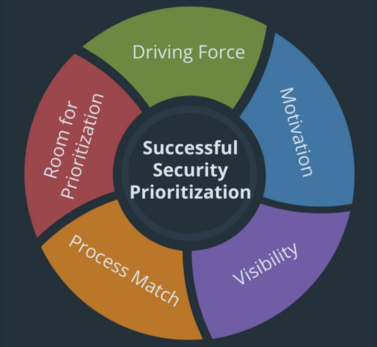


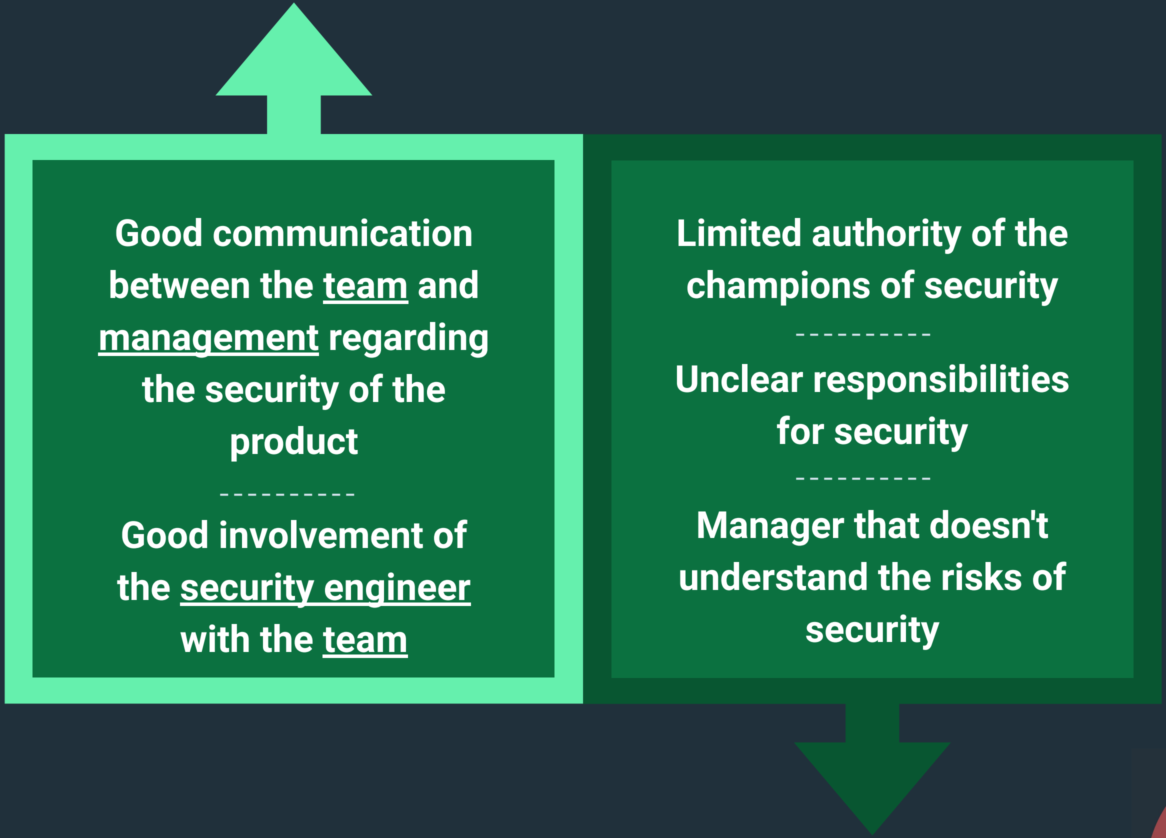
Figure from: Inger Anne Tøndel, Daniela Soares Cruzes, Martin Gilje Jaatun, Guttorm Sindre, **Influencing the security prioritisation of an agile software development project,** Computers & Security, Volume 118, 2022, https://doi.org/10.1016/j.cose.2022.102744

Driving Force

“someone who takes initiative and responsibility for making software security happen”



Driving Force



Good communication between the team and management regarding the security of the product

----

Good involvement of the security engineer with the team

Limited authority of the champions of security

Unclear responsibilities for security

Manager that doesn't understand the risks of security

Driving Force
Motivation
Visibility
Process Match
Room for Prioritization
Successful Security Prioritization

“Great things in businesses are never done by one person. They’re done by a team of people.” – Steve Jobs

VSP roles

VSP
Program Owner

Security
Engineer

VSP
Partner

Infrastructure
Engineer

VSP
Service Owner

Security
Manager

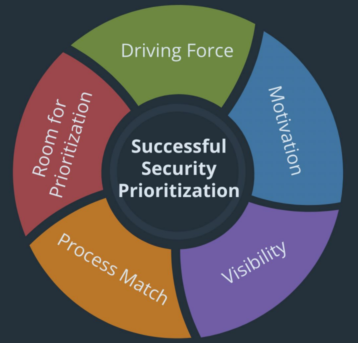
Asset Owner

(Product / Solution / Infrastructure / HR)

Data Protection
Manager

Motivation

“the willingness to focus on software security, as well as the aspects that cause such willingness.”



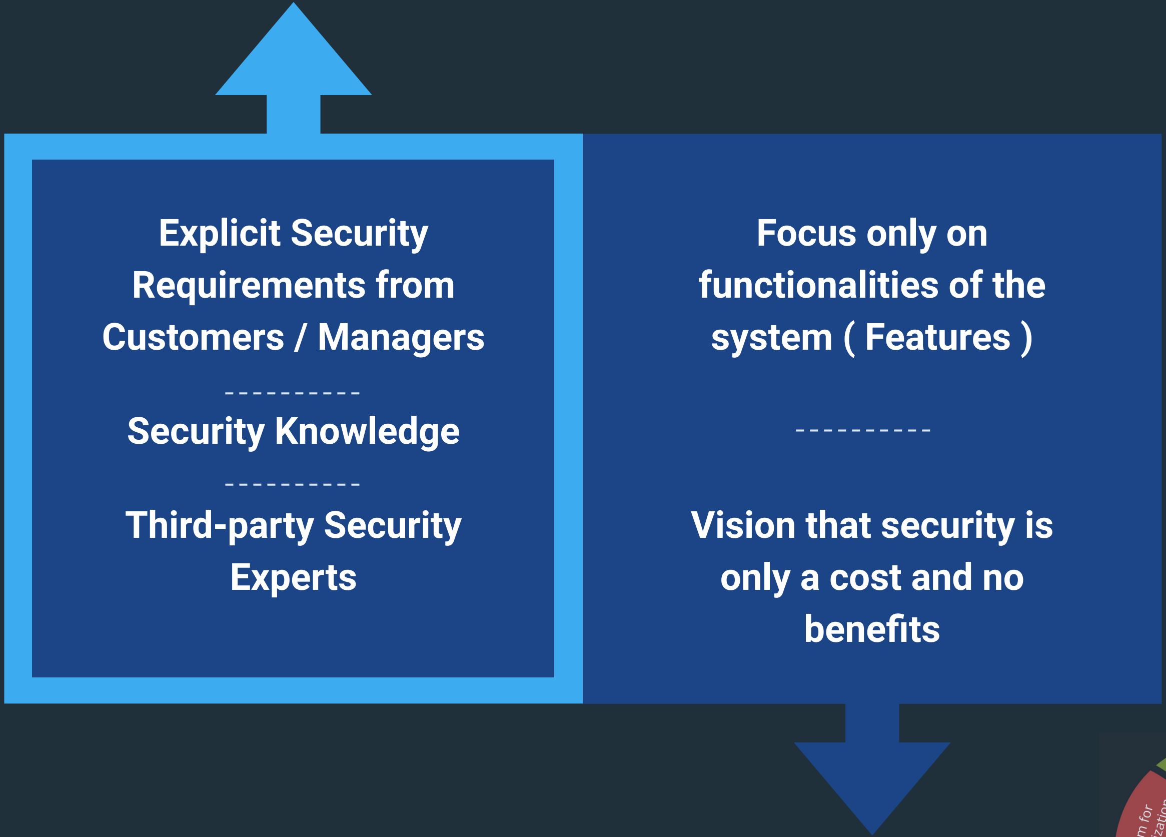
Motivation

Build projects around motivated individuals. Give them the environment and support they need, and trust them to get the job done.

Agile Principle #5

Driving Force
Motivation
Visibility
Process Match
Room for Prioritization
Successful Security Prioritization

Motivation



Explicit Security Requirements from Customers / Managers

Security Knowledge

Third-party Security Experts

Focus only on functionalities of the system (Features)

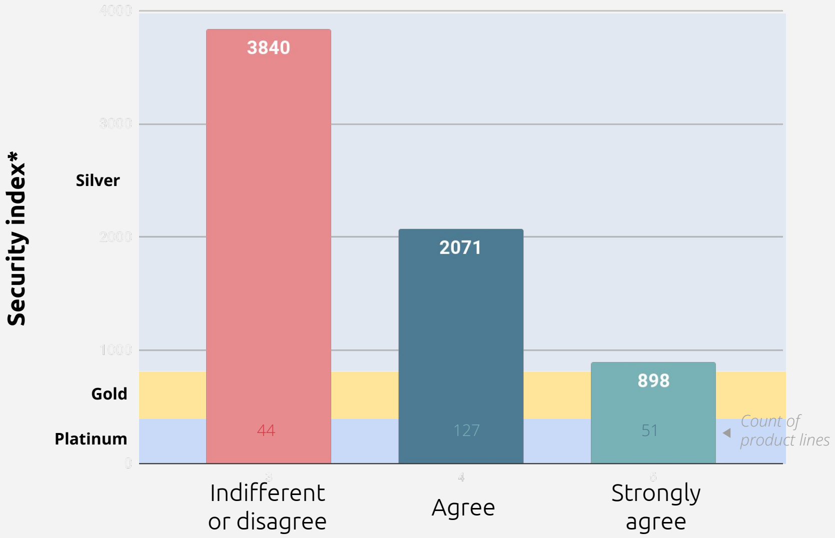
Vision that security is only a cost and no benefits

Driving Force
Motivation
Visibility
Process Match
Room for Prioritization
Successful Security Prioritization

Teams with **good security practices** report that they have more autonomy to innovate.

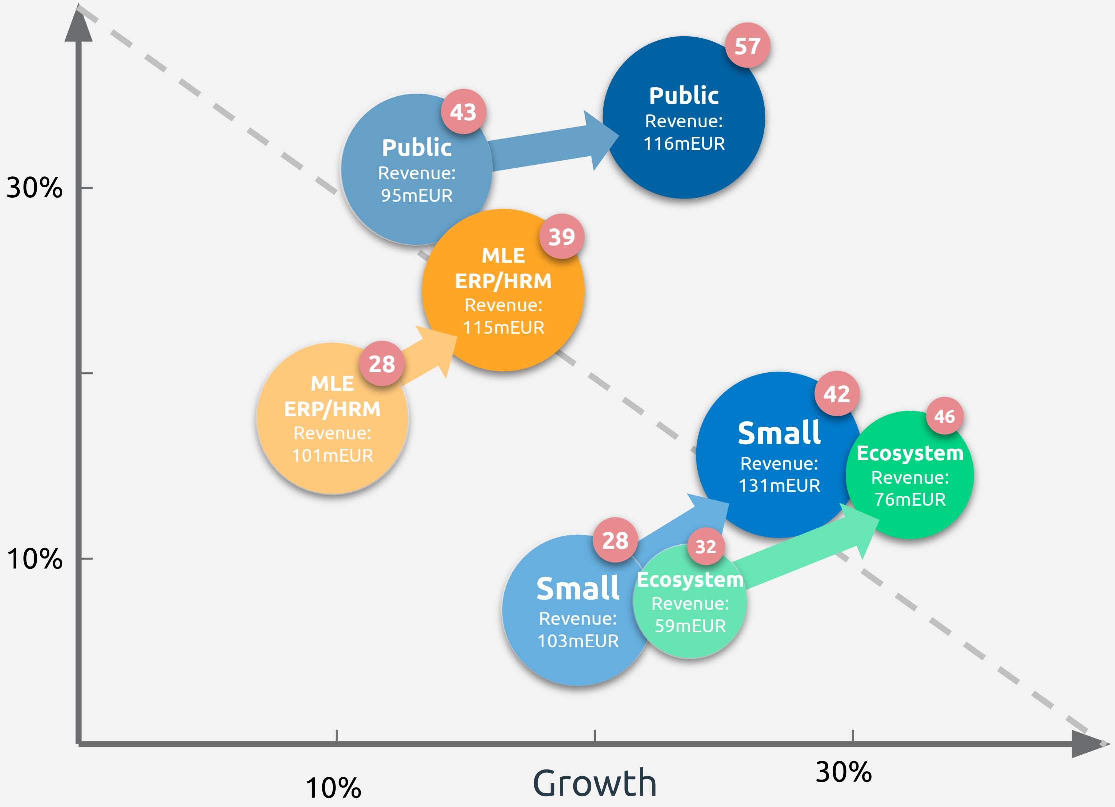
Innovation survey and Security index

*I am able to work on new ideas during the development process, without having to get permission from someone outside of my team**



*Having a low score for the security index indicates good security practices.

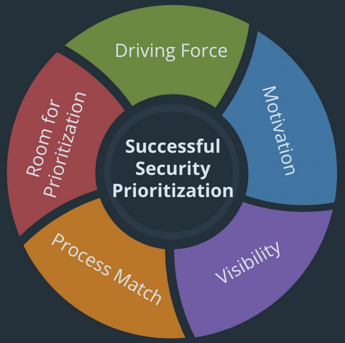
Part of the reasons for the growth of VISMA acquired companies can be attributed to better security practices



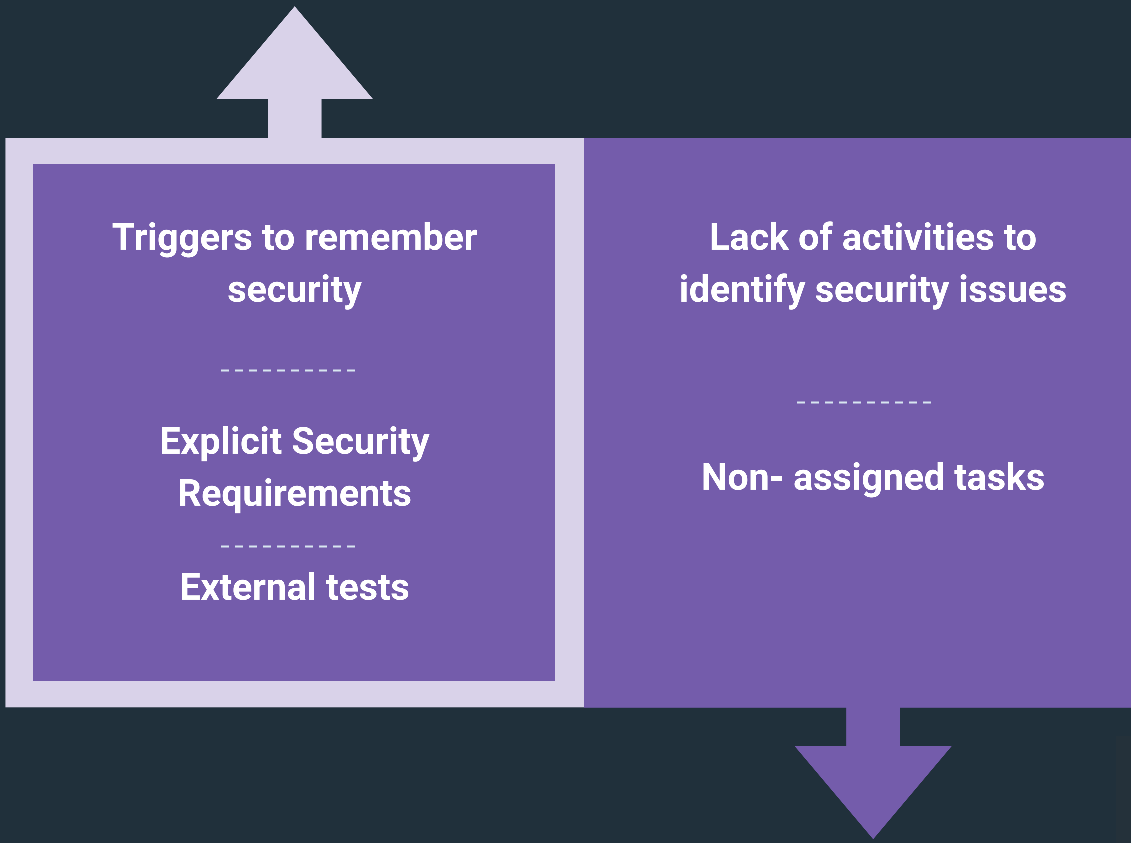
Aggregated financial data collected for the acquisition year (AY) and the year following the acquisition (AY + 1)

Visibility

“the degree to which security is visible (seen, identified …) to stakeholders of the project”



Visibility



Triggers to remember security

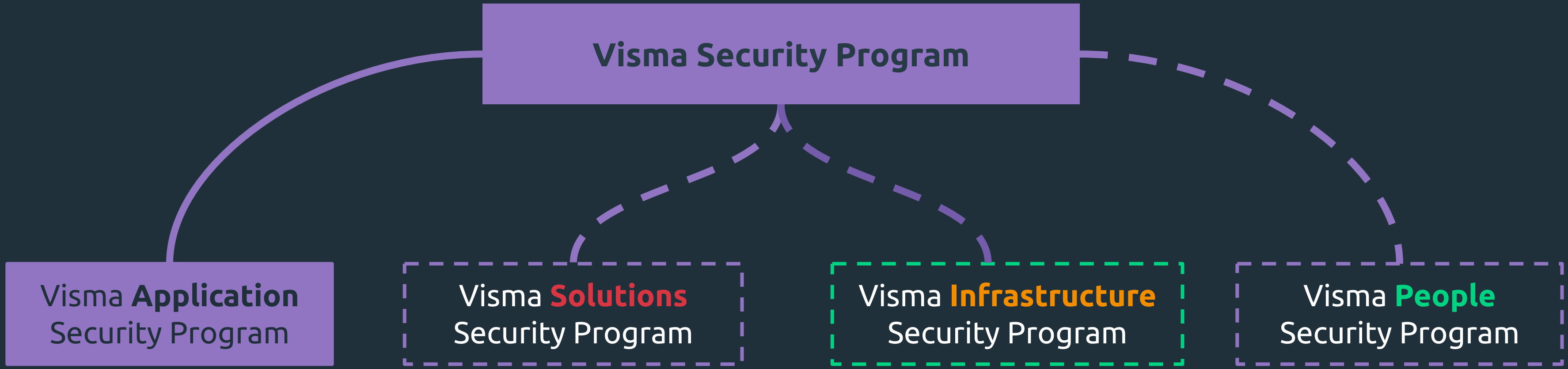
Explicit Security Requirements

External tests

Lack of activities to identify security issues

Non- assigned tasks

Driving Force
Motivation
Visibility
Process Match
Room for Prioritization
Successful Security Prioritization



Visma Security Program

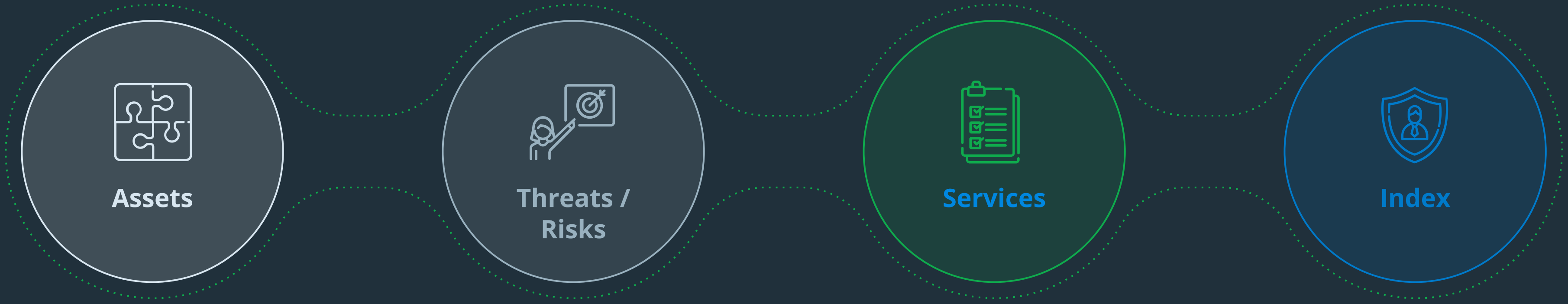
Visma **Application** Security Program

Visma **Solutions** Security Program

Visma **Infrastructure** Security Program

Visma **People** Security Program

Visma Application Security Program



Assets

Threats / Risks

Services

Index

Applications

Software application that we write and control

Risk of data breach due to potential code vulnerabilities

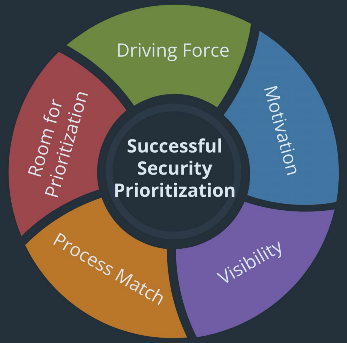
(SSA)	Security Self-Assessment
(DPSA)	Data Protection Self-Assessment
(SAST)	Static Application Security Test
(SCA)	Software Composition Analysis
(DAST)	Dynamic Application Security Test
(MAVA)	Manual Application Vulnerability Assessment
(CTI)	Cyber Threat Intelligence
(BB)	Bug Bounty
(RD)	Responsible Disclosure

What security tier should be in place?

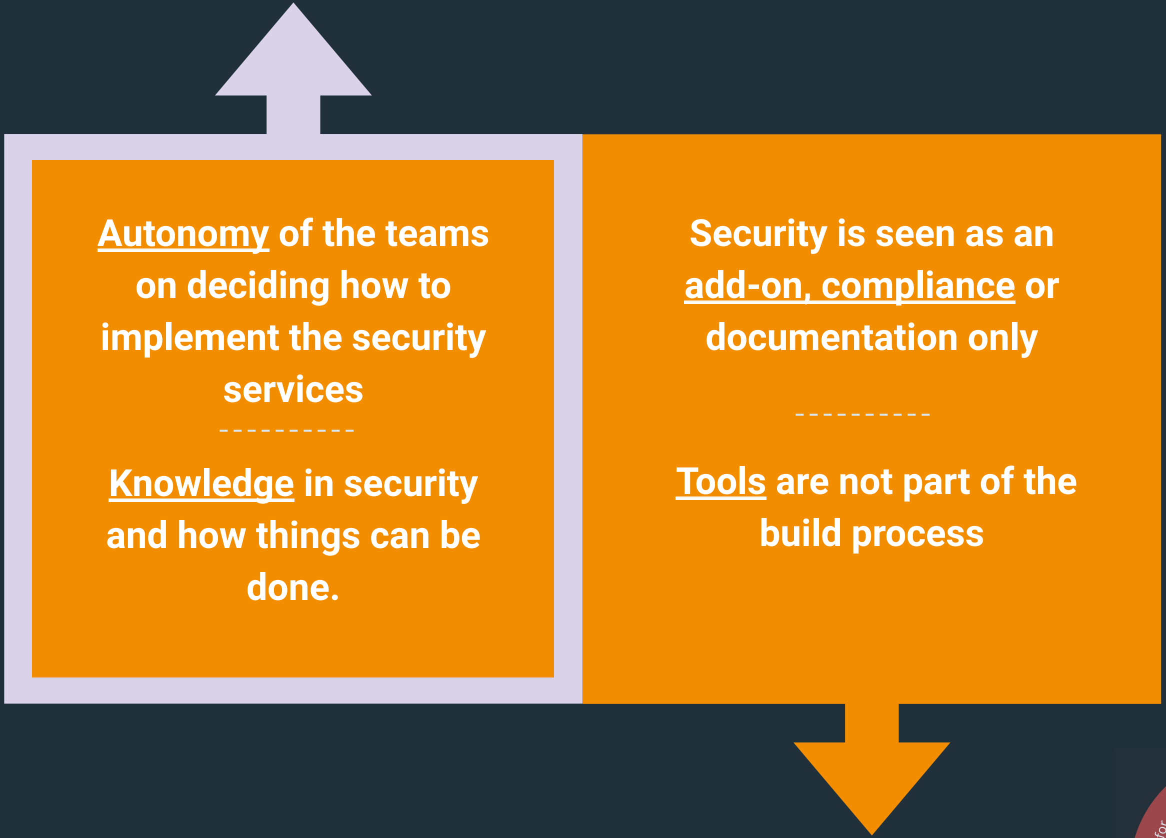
How well are we covered for the risks?

Process Match

“the ability to fit the security approach into the existing software development process, so that they align well”



Process Match



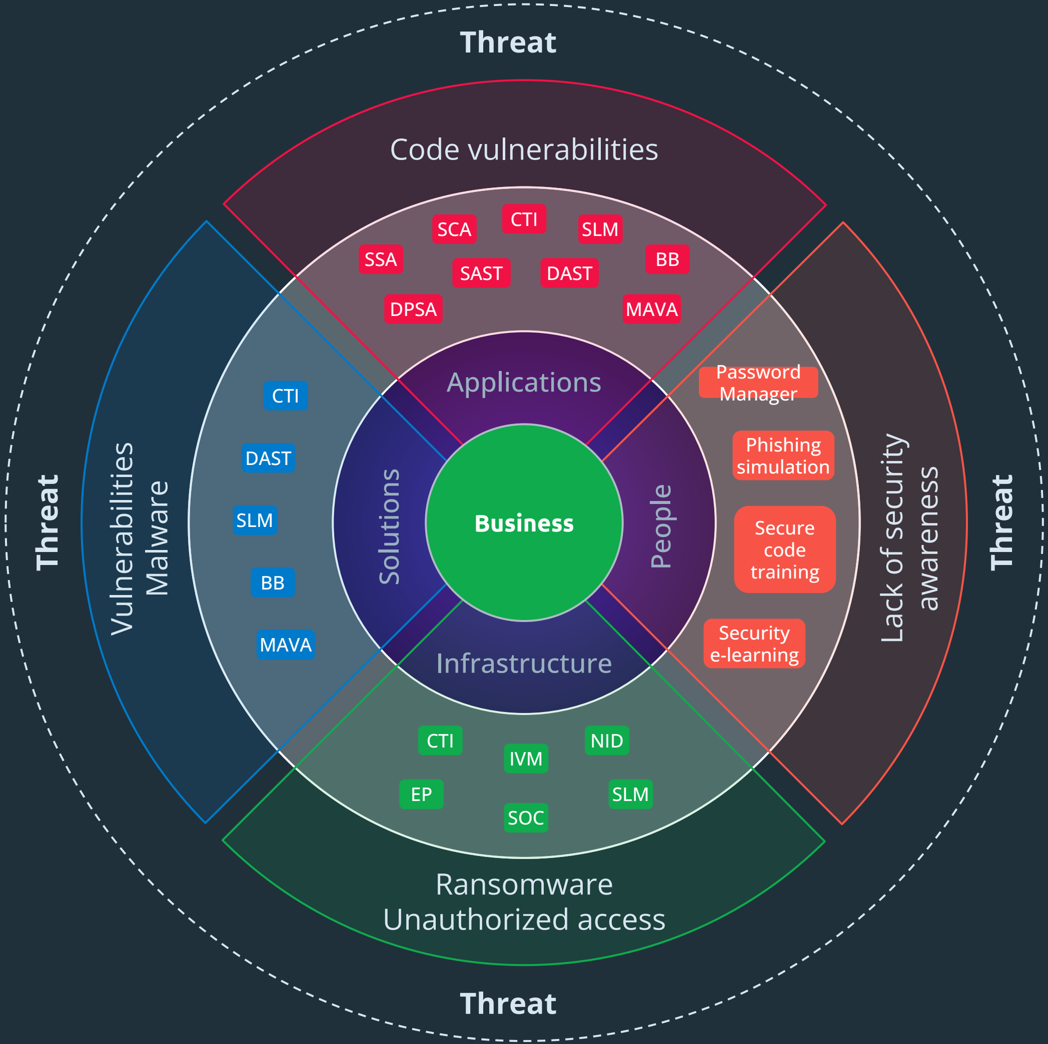
Autonomy of the teams on deciding how to implement the security services

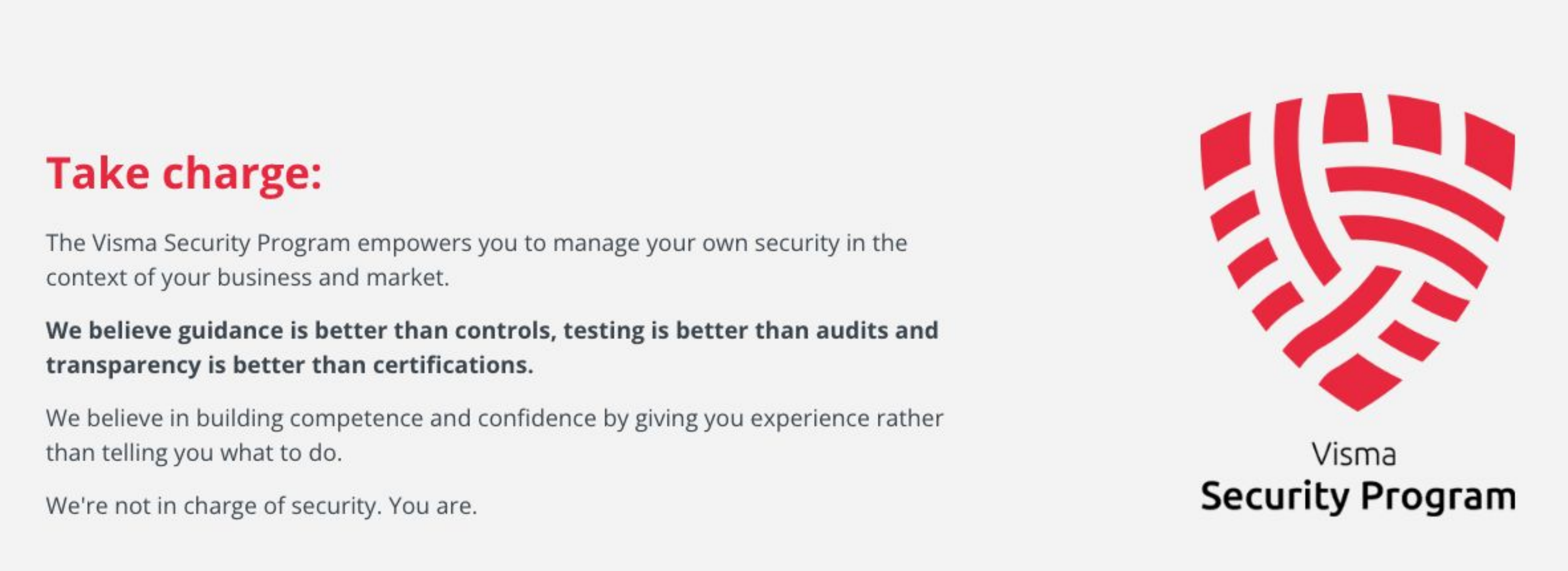
Knowledge in security and how things can be done.

Security is seen as an add-on, compliance or documentation only

Tools are not part of the build process

«If it is not in Jira it does not exist for the development team»





Take charge:

The Visma Security Program empowers you to manage your own security in the context of your business and market.

We believe guidance is better than controls, testing is better than audits and transparency is better than certifications.

We believe in building competence and confidence by giving you experience rather than telling you what to do.

We're not in charge of security. You are.

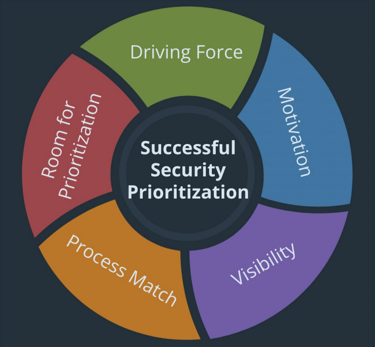
Visma
Security Program

«Get the certification with changing only one policy»

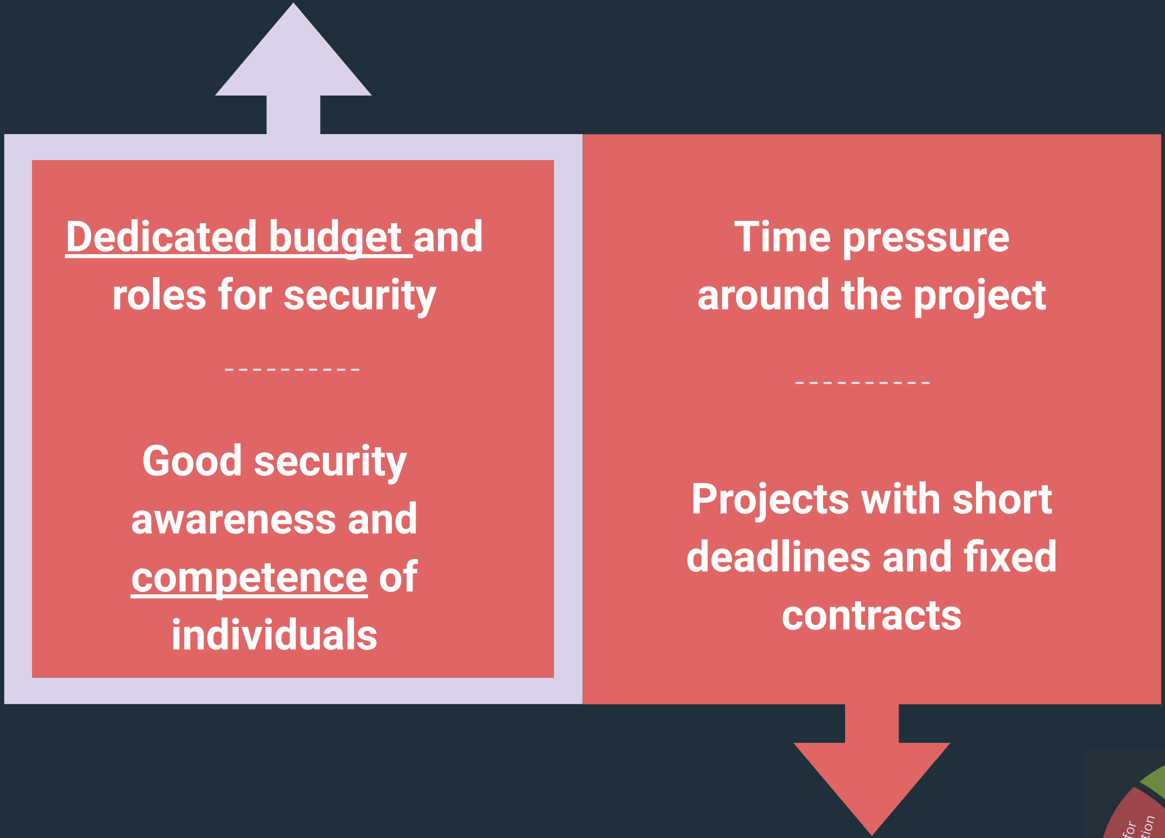
ISO 27001 Certification

Room for Prioritisation (maneuvre)

“resources (time, budget, competence) to prioritise software security, and to act accordingly.



Room for Prioritisation



Dedicated budget and roles for security

- - - - - - - - - - -

Good security awareness and competence of individuals

Time pressure around the project

- - - - - - - - - - -

Projects with short deadlines and fixed contracts

Driving Force
Motivation
Visibility
Process Match
Room for Prioritization
Successful Security Prioritization

Security Level - **Recommended Guidelines**

Platinum

Lowest level of risk appetite

This tier requires
all risk mitigation controls available in VASP.

Expected security work
Daily basis

Product type
SaaS with sensitive data

Gold

Medium level of risk appetite.

This tier requires
most of the risk mitigation controls available in VASP.

Expected security work
Weekly basis

Product type
SaaS with some sensitive data

Silver

High level of risk appetite.

This tier has
a lot of acceptance of deviations of the risk mitigation controls available in VASP.

Expected security work
Monthly basis

Product type
OnPrem/Saas with no sensitive data

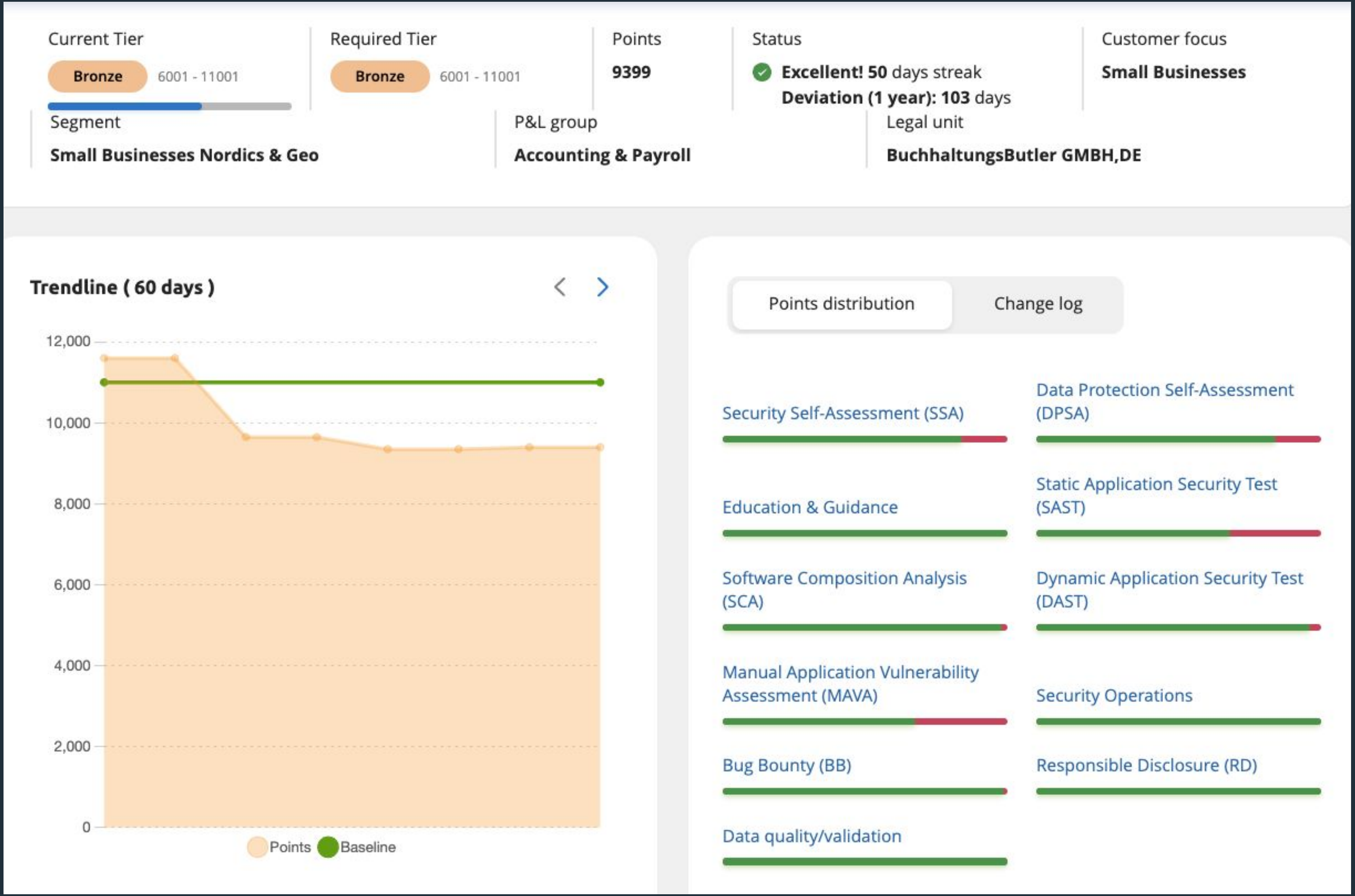
Bronze

Critical level of risk appetite.

This tier has
a high acceptance of deviations of the risk mitigation controls available in VASP.

Expected security work
Seldom basis

Product type
OnPrem



Current Tier

Bronze 6001 - 11001

Required Tier

Bronze 6001 - 11001

Points

9399

Status

✓ **Excellent! 50** days streak

Deviation (1 year): 103 days

Customer focus

Small Businesses

Segment

Small Businesses Nordics & Geo

P&L group

Accounting & Payroll

Legal unit

BuchhaltungsButler GMBH,DE

Trendline (60 days)

Points distribution | Change log

Security Self-Assessment (SSA)

Data Protection Self-Assessment (DPSA)

Education & Guidance

Static Application Security Test (SAST)

Software Composition Analysis (SCA)

Dynamic Application Security Test (DAST)

Manual Application Vulnerability Assessment (MAVA)

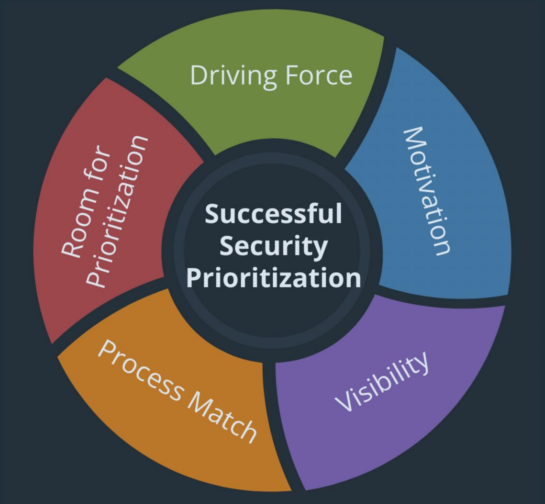
Security Operations

Bug Bounty (BB)

Responsible Disclosure (RD)

Data quality/validation

Influences to the priority given to security



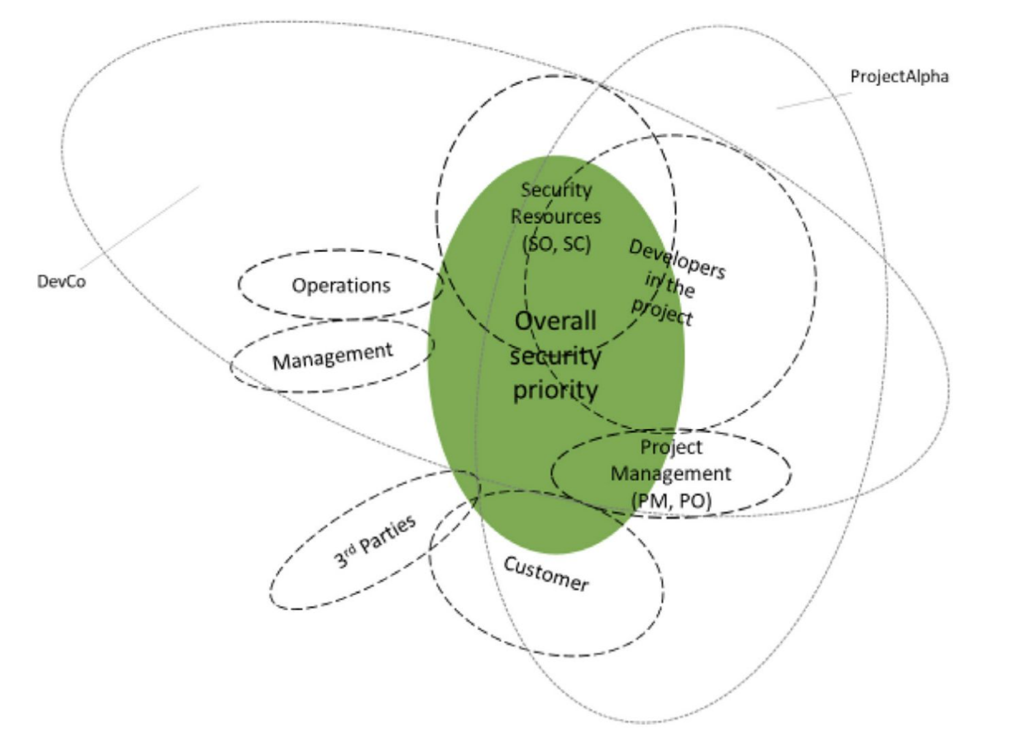

ProjectAlpha
DevCo
Security Resources (SO, SC)
Developers in the project
Operations
Management
Overall security priority
Project Management (PM, PO)
3rd Parties
Customer

Fig. 5. Overview of the stages of the Security Requirements Initiative.

One Size Fits doesn’t fit All

There is more than only hard core activities.

Image By AWeith - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=51789188