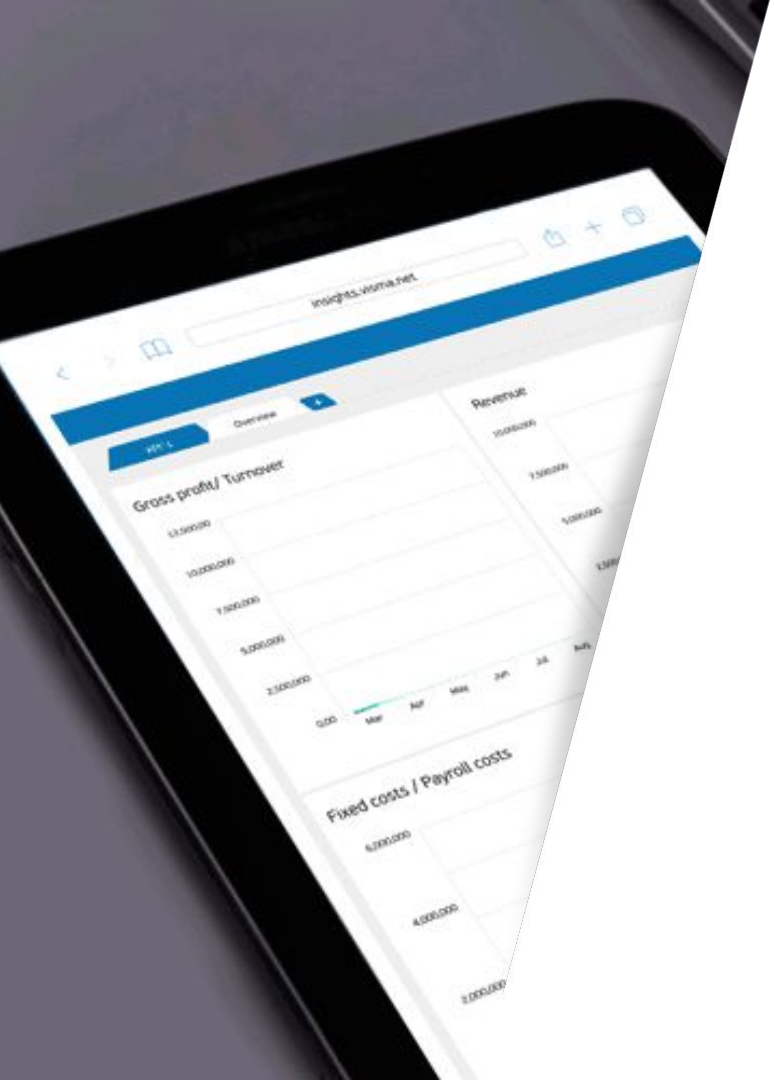


Informasjonssikkerhet i Visma

2020

VISMA

Visma structure - Teamwork

- Many teams are highly self-managed
- High pace of development and deployment
- Environment constantly changing
- High amount of integrations
- Highly skilled and capable team members
- Teams want to do what is “right” based on accurate information
- Responsibility are accepted with necessary support

VISMA

Decentralized security

- Team is responsible for security of their service with support from Product Security
  - Owns the complete experience (design, develop, test, deploy, operate) - Holistic view
  - Knows the end users
  - Aware of the context the service exists in

- With support from Product Security
  - Standardized security services
  - Security services are not exclusive, other tools are highly welcome and encouraged
  - Teams are encouraged to take own initiative into ways to improve the security of their service
  - Understand and acknowledge continuous improvement in the security area

TP - Target Portfolio

- The Target Portfolio is a database of assets developed or used by Visma.

Flyt Barenhage:

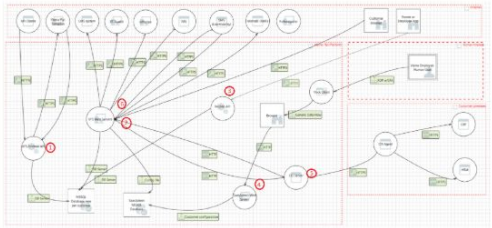
Assessment	Assessment date	Unresolved issues from assessment	SAST	ATVS	CTI	Bug Bounty	Latest manual test	Unresolved critical and severe issues	Unresolved recommended issues
APPROVED PRIVACY: PSA APPROVED	2019-07-31	0 saker	ENROLLED	ENROLLED	ENROLLED	ENROLLED	2019-12	0 saker	1-sak

SSA - Security Self Assessment

- Mandatory Security Review document

- Attack surface
- Input validation
- Session management
- Access control
- Privacy and data protection (PSA)
- Encryption
- Security monitoring
- Error handling
- Account and password management
- Operation

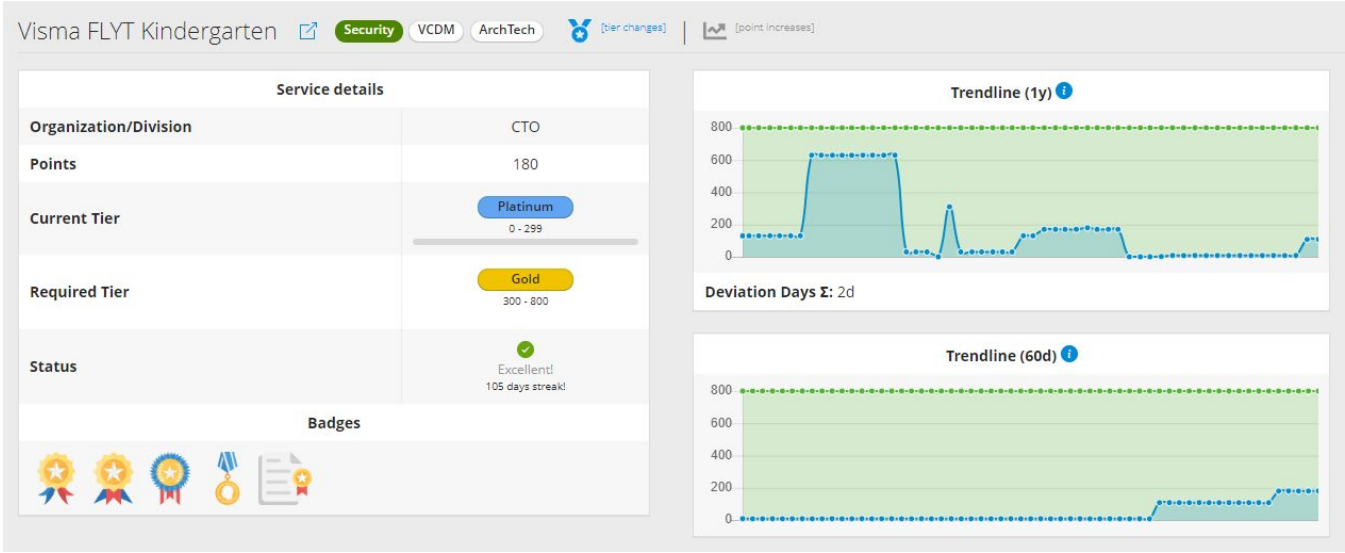
Visma Flyt Skole

› SA01 - Attack surface interface	REQUIRED GDPR		OK	 The Flow Diagram can be found here. The Threat Model File is also located there.

Title	Attack surface interface 1
Description	The external API is a REST/JSON based web API used for retrieving and manipulating information in the Visma Flyt Skole customer databases.

The Security Maturity Index

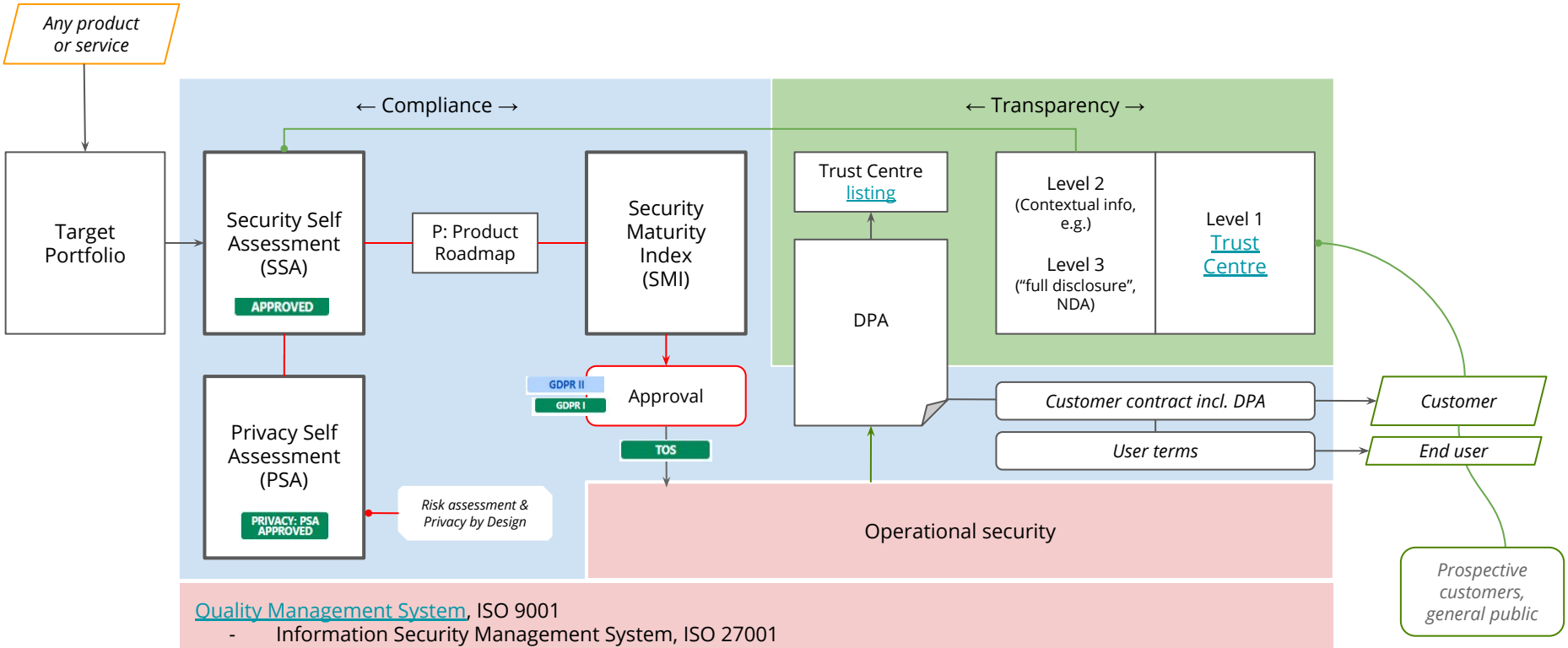
- Custom application ingesting data from different sources (Jira, Coverity, …)
- Gamified compliance and governance, required tiers are assigned to each product.
- **Powerful tool for stakeholders.**



Checklist

- Procedures & processes: incident management, subcontractors, data requests etc.
- All services in Visma are listed and followed up in our internal Target Portfolio
- Will get assistance from the Visma Security team and SecOps/SOC (Incidents and Intelligence)
- All teams has a Security Engineer
- All teams attend mandatory Training program
    - Additional Competence sharing in SecEng Guild and On-site training for different roles (devs, mgmt, PO, SO, BA, QA)
- All teams perform a Security Self Assessment, including embedded Privacy Self Assessment
- All services set up automated and manual tests (Security + Quality)
    - Manual Application Vulnerability Assessment (Pentest)
    - Automated Static Application Security Test (SAST)
    - Automated Third-party Vulnerability Service (ATVS)
    - Bug Bounty
    - Cyber Threat Intelligence

Privacy Framework:



Quality Management System, ISO 9001
- Information Security Management System, ISO 27001

Key privacy procedures:
- P: Handle data requests
- P: Update Trust Centre and Terms of Service
- P: Validate new or changed third party data processor

VISMA

Respect

Reliability

Innovation

Competence

Team spirit

VISMA