Security + Devops + Ambidexterity = FUN

Espen Agnalt Johansen

Security Director

Visma

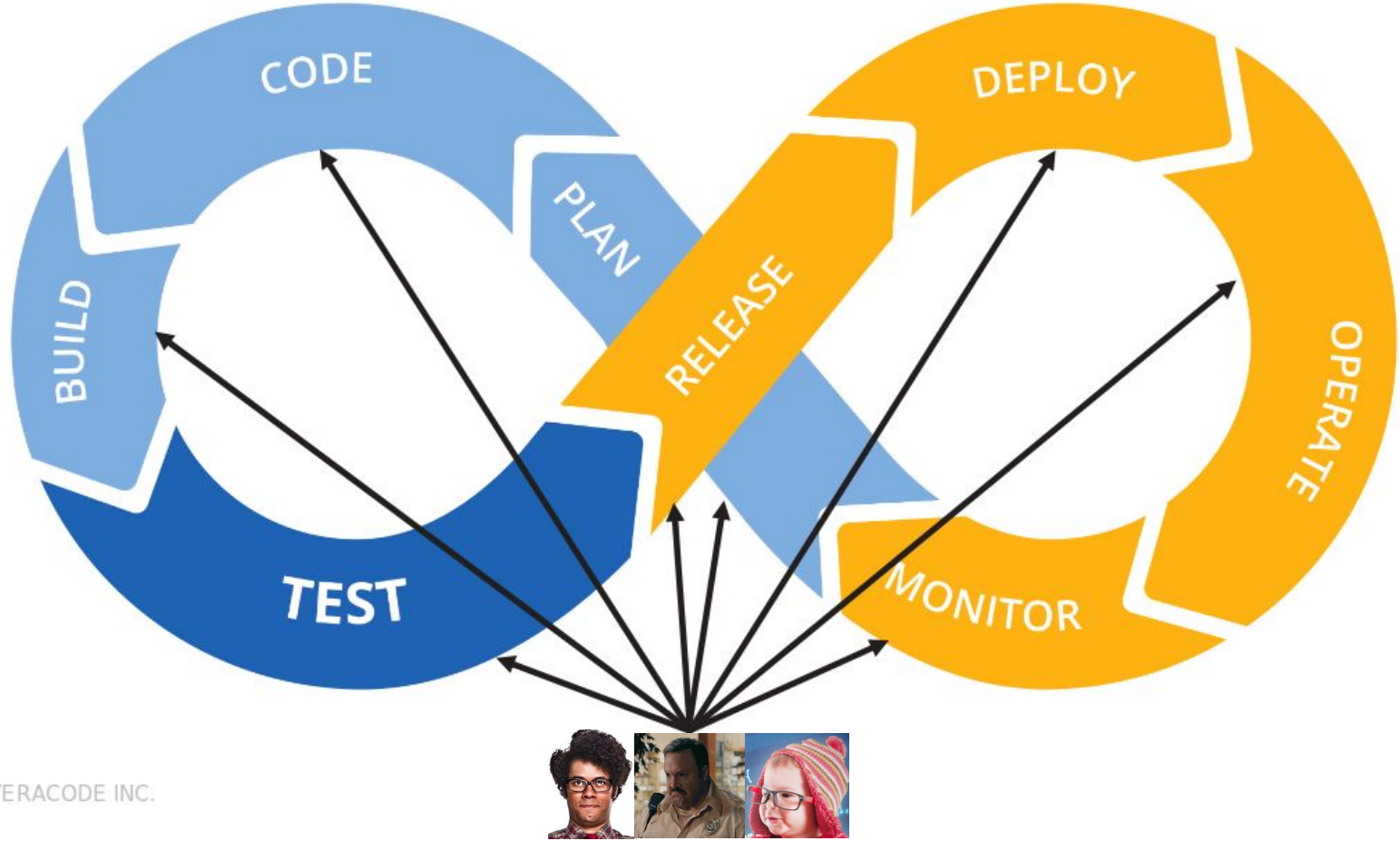
Security + Ambidexterity + DevOps = 💓

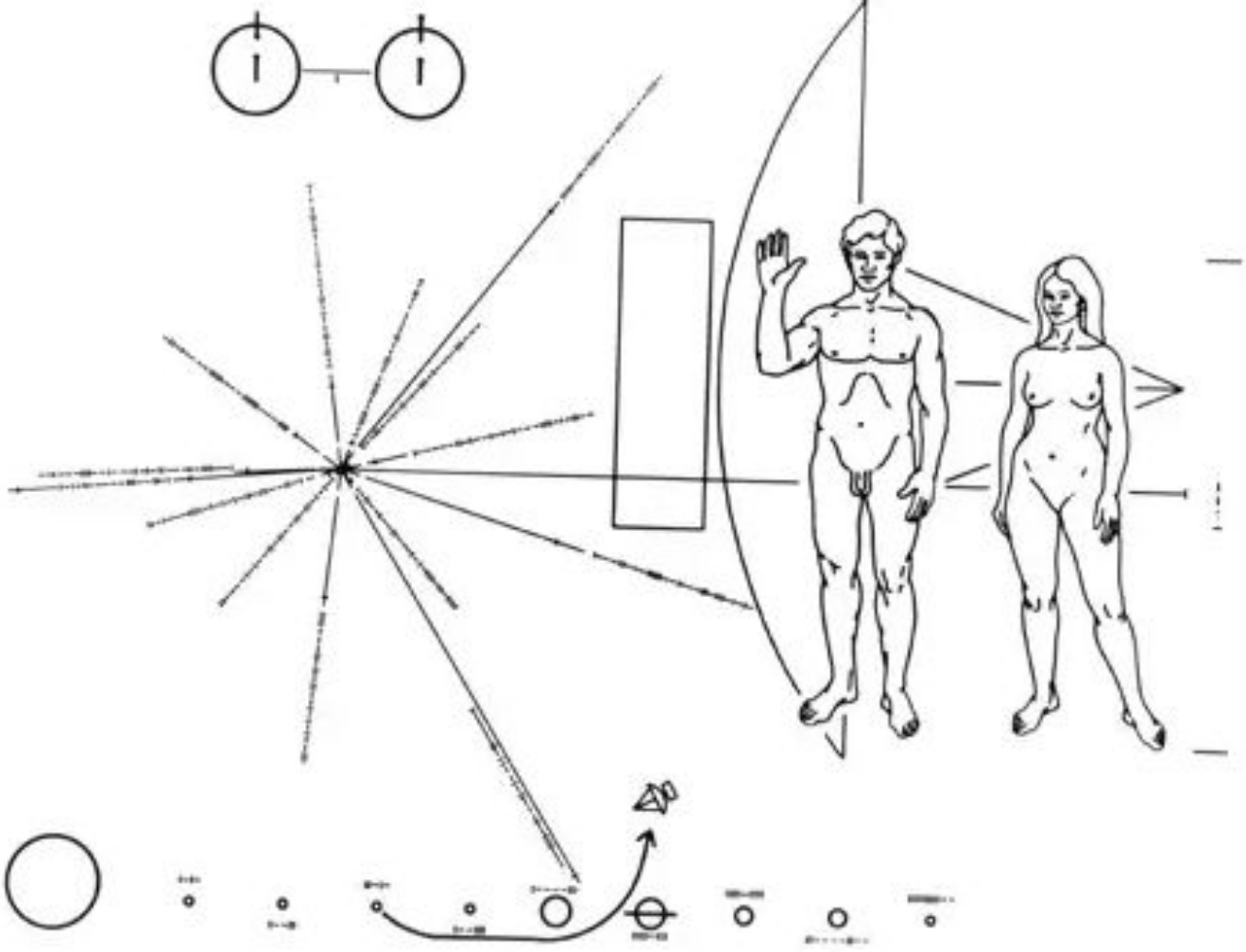
Empowerment of Security Engineers through Security Chartering in Visma


SECURITY
GUARD


if(p
hq
}
if
h
}
tains("age")){
ge = :age";
query = em
Person.cla
));


DEFEND BLOGGERS RIGHTS

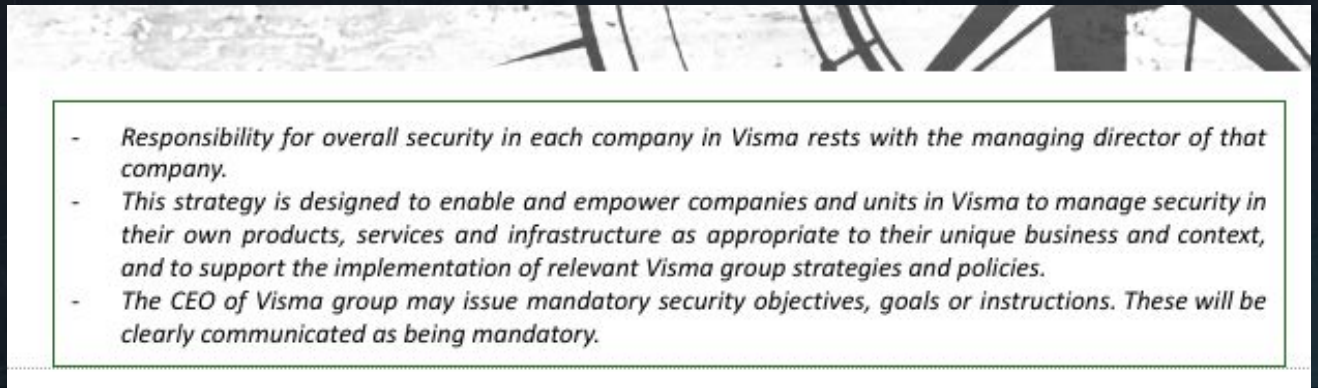




Are your people Empowered?

Are your people enabled?

Have YOU embedded and Ensured the 2 above?



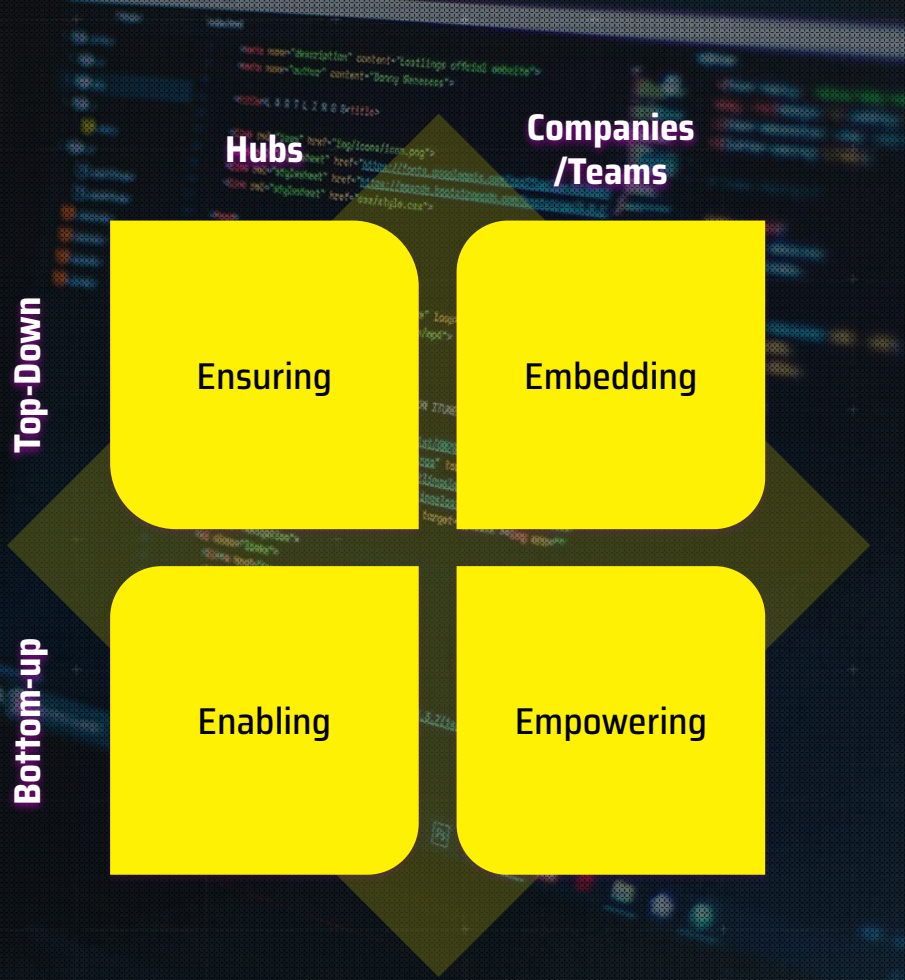
- *Responsibility for overall security in each company in Visma rests with the managing director of that company.*
- *This strategy is designed to enable and empower companies and units in Visma to manage security in their own products, services and infrastructure as appropriate to their unique business and context, and to support the implementation of relevant Visma group strategies and policies.*
- *The CEO of Visma group may issue mandatory security objectives, goals or instructions. These will be clearly communicated as being mandatory.*

“Ambidexterity is the ability to use both the **right** and **left** hand equally well”

—Wikipedia

An Ambidextrous Governance Model

Top-down or bottom-up

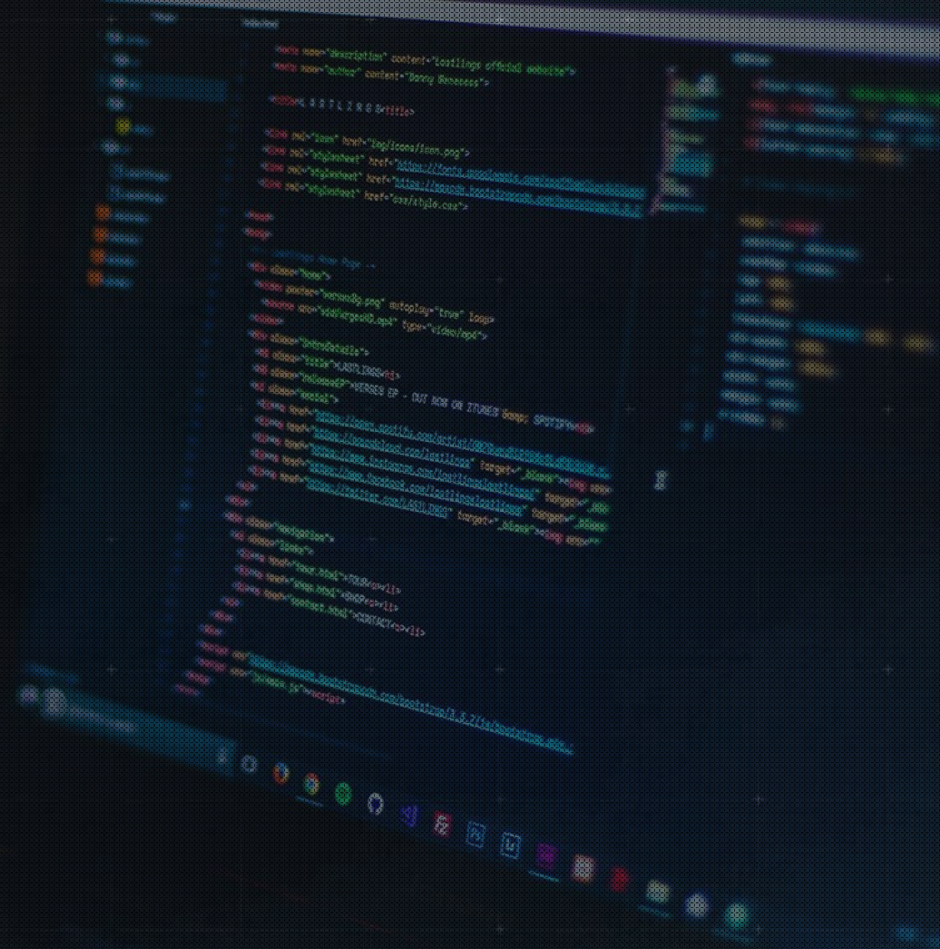


Adapted from: McDermott, Aoife & Hamel, Lauren & Steel, David & Flood, Patrick & McKee, Lorna. (2015). Hybrid Health Care Governance for Improvement? Combining Top-Down and Bottom-up Approaches to Public Sector Regulation, Public Administration. 93. 10.1111/padm.12118

Ensuring

The adoption of evidence-based best practice

Strategy



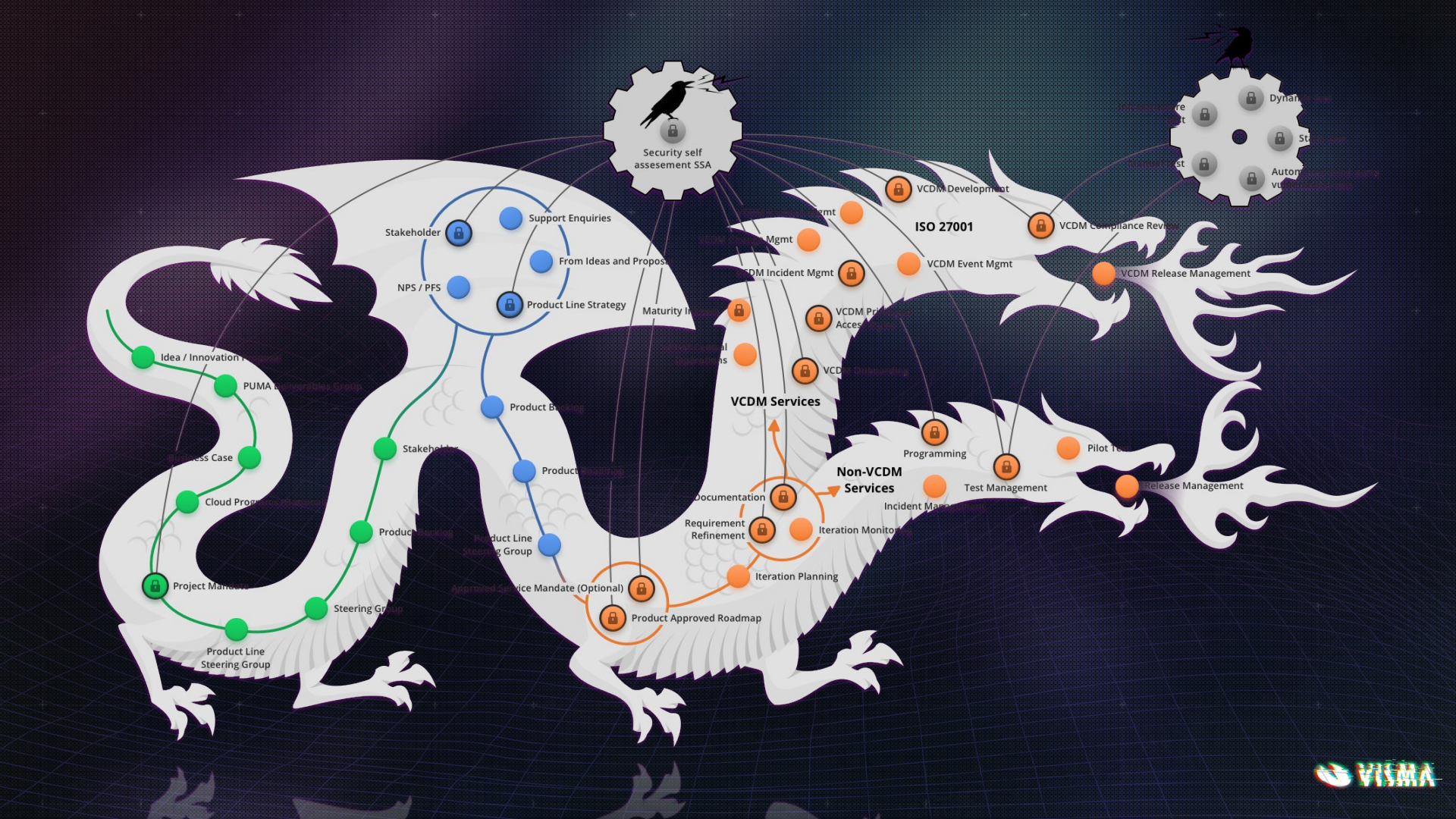
Enabling

Giving someone the
means to do something

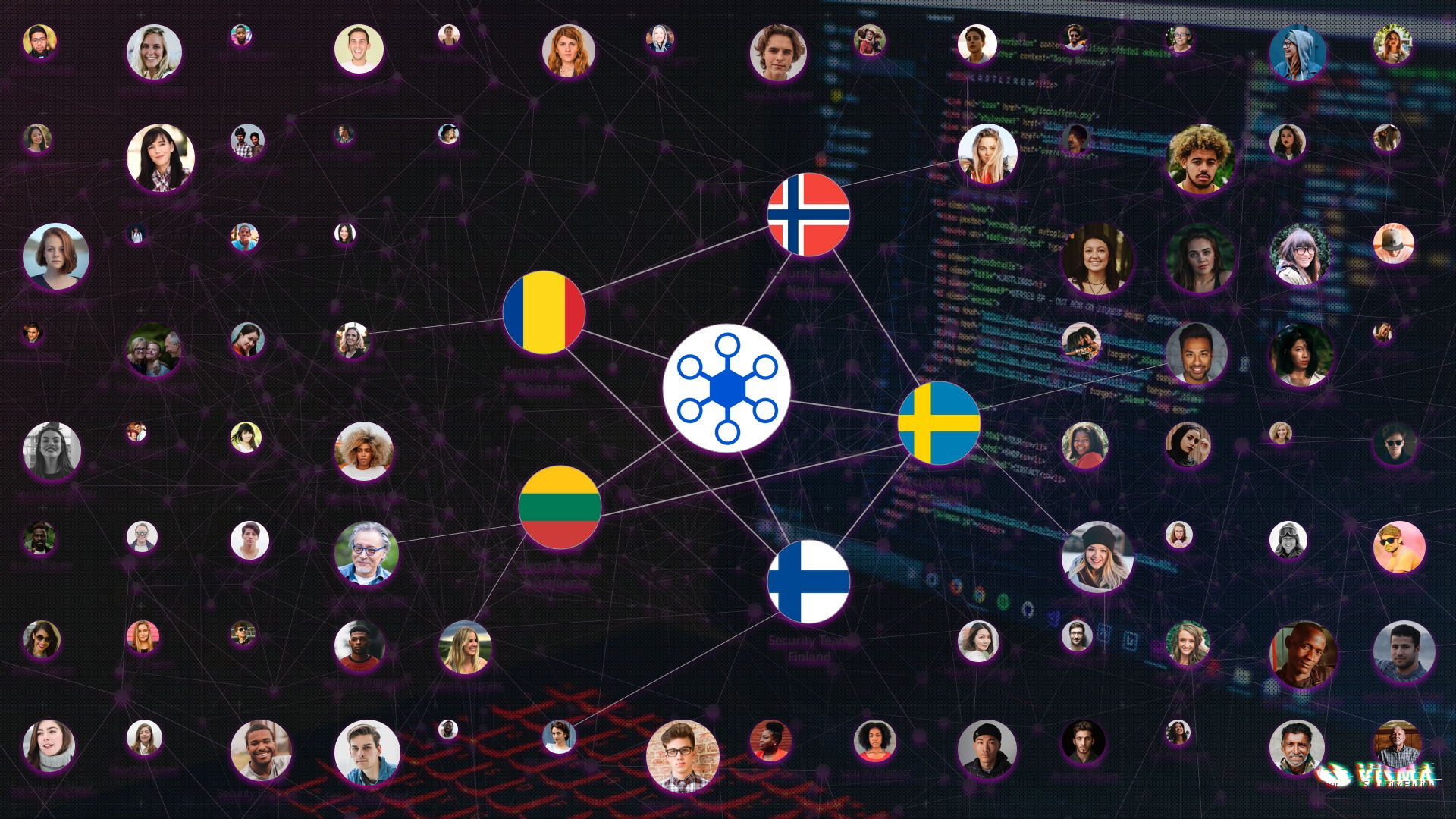

Train Hard.
Fight Easy.

Embedding

To incorporate as an essential part or characteristic


Security self assesement SSA
Stakeholder
Support Enquiries
From Ideas and Proposa
NPS / PFS
Product Line Strategy
Maturity In
Idea / Innovation
PUMA
Product B
Stakeholder
Product
Cloud Prog
Product
Project Manage
Steering Gr
Product Line Steering Group
Product Line
g Group
Approval Service Mandate (Optional)
Product Approved Roadmap
VCDM Development
ISO 27001
VCDM Compliance Revi
Mgmt
Mgmt
VCDM Incident Mgmt
VCDM Event Mgmt
VCDM Release Management
VCDM Pri
Acces
VCDM
VCDM Services
Programming
Pilot Te
Non-VCDM Services
Test Management
Release Management
Incident Mana
Documentation
Requirement Refinement
Iteration Monitor
Iteration Planning
Dynam
St
Autom
vu


Empowering
Creating a supportive climate for service improvement



SAST

ATVS

M&A

Influencing

ATVS

CTI

DAST

SecretSauce

Monitoring

Analysis

MAVA

Publications

SecretSauce

Research

SLM

Incident

Index

Detection

RedTeaming

Endpoint Monitoring

SecretSauce

Police Liaisoning

SecretSauce

Books

Coaching

BugBounty

Training

VISMA

Advisor Period & Year-end Closing - Financial Statement and Reconciliation

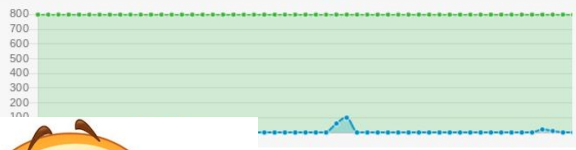
Security | VCDM | ArchTech | No notifcations [tier changes] | [point increases]

Service details

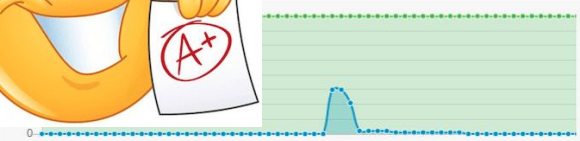
Organization/Division	VSI
Points	0
Current Tier	Platinum 0 - 299
Required Tier	Gold 300 - 800
Status	Overperforming 365 days streak! (from 2019-12-10)

Badges

Trendline (1y)



ıdline (60d)



Change log

Question	Points	Timestamp
Unresolved third party vulnerabilities (frontend+backend)	0 ▼10	2021-02-24
Untriaged security defects	0 ▼10	2021-02-16
Untriaged security defects older than 7 days	0	2021-02-12
Untriaged security defects	10 ▼190	2021-02-12
Untriaged security defects older than 7 days	0	2021-02-11
Last analyzed older than 30 days	0 ▼300	2021-02-11
Unresolved third party vulnerabilities (frontend+backend)	10 ▲10	2021-02-11
Untriaged security defects	200 ▲200	2021-02-11

Points distribution by category

Security Self-Assessment (SSA)	Education & Guidance
Static Application Security Test (SAST)	Automated Third-party Vulnerability Service (ATVS)
Dynamic Application Security Test (DAST)	Manual Application Vulnerability Assessment (MAVA)
Security Operations	Bug Bounty (BB)
Responsible Disclosure (RD)	Data quality/validation

[redacted] Security | VCDM | ArchTech | No notifcations [tier changes] | [point increases]

Service details

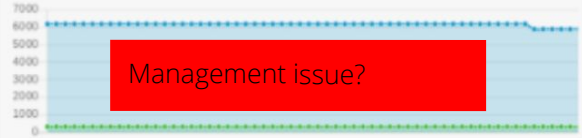
Organization/Division	[redacted]
Points	5891
Current Tier	Silver 801 - 6000
Required Tier	Platinum 0 - 299
Status	Action required 365 days deviation

Badges

Trendline (1y)

Management issue?

rendline (60d)



Management issue?

Change log

Question	Points	Timestamp
Security Engineer assigned	0 ▼300	2021-03-02
Valid Division (non-legacy)	0 ▼1	2021-03-02
Migrated to Product Security Catalog (PSC)	0 ▼1	2021-03-02
Product Owner assigned	0	2021-03-02
Onboarded to SAST (Custom)		
Valid Division (non-legacy)		
Migrated to Product Security Catalog (PSC)		
Unresolved recommended issues older 180 days	0 ▼700	2020-10-06

Funding issue?

Skill issue?

Points distribution by category

Security Self-Assessment (SSA) | Education & Guidance

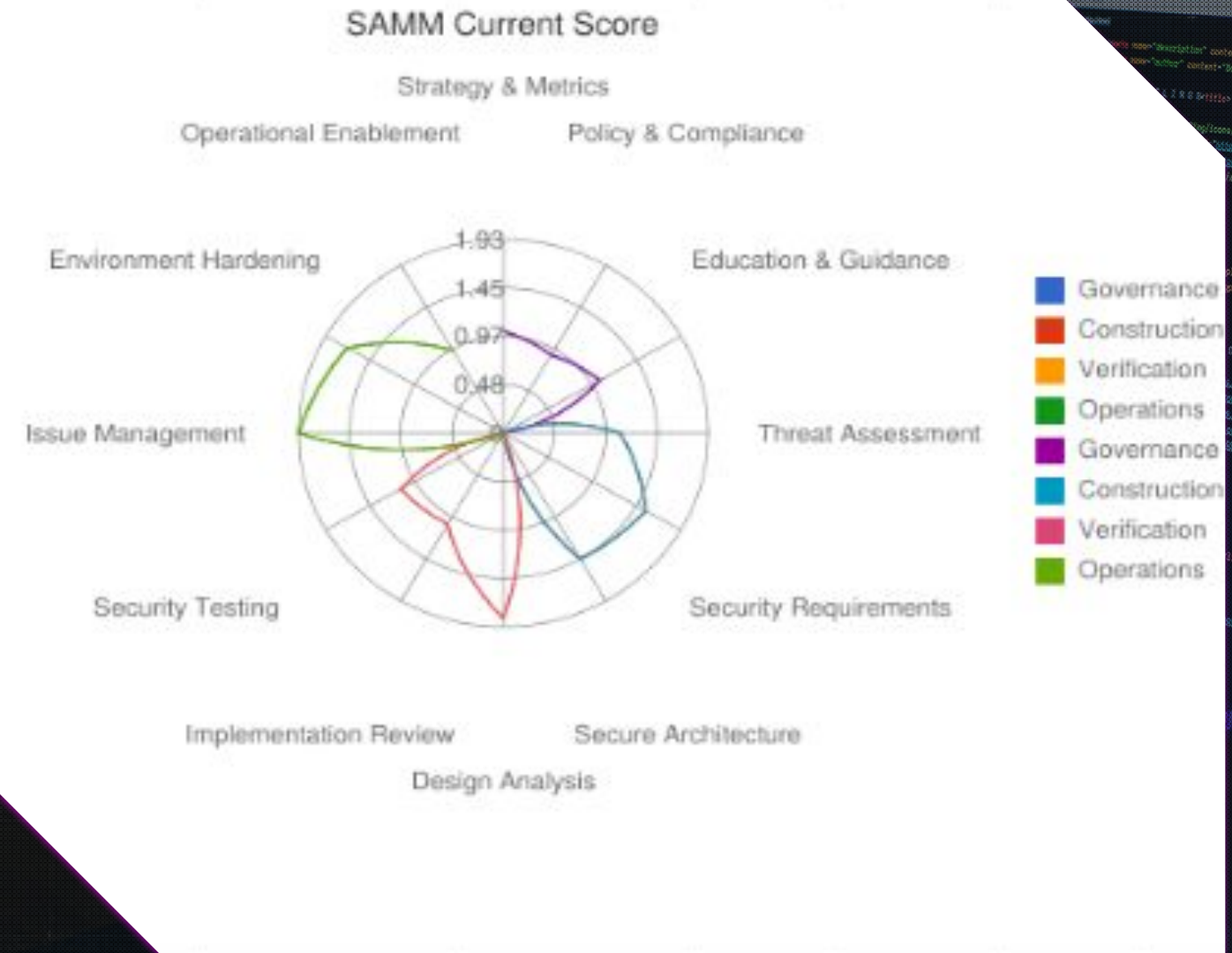
Static Application Security Test (SAST)

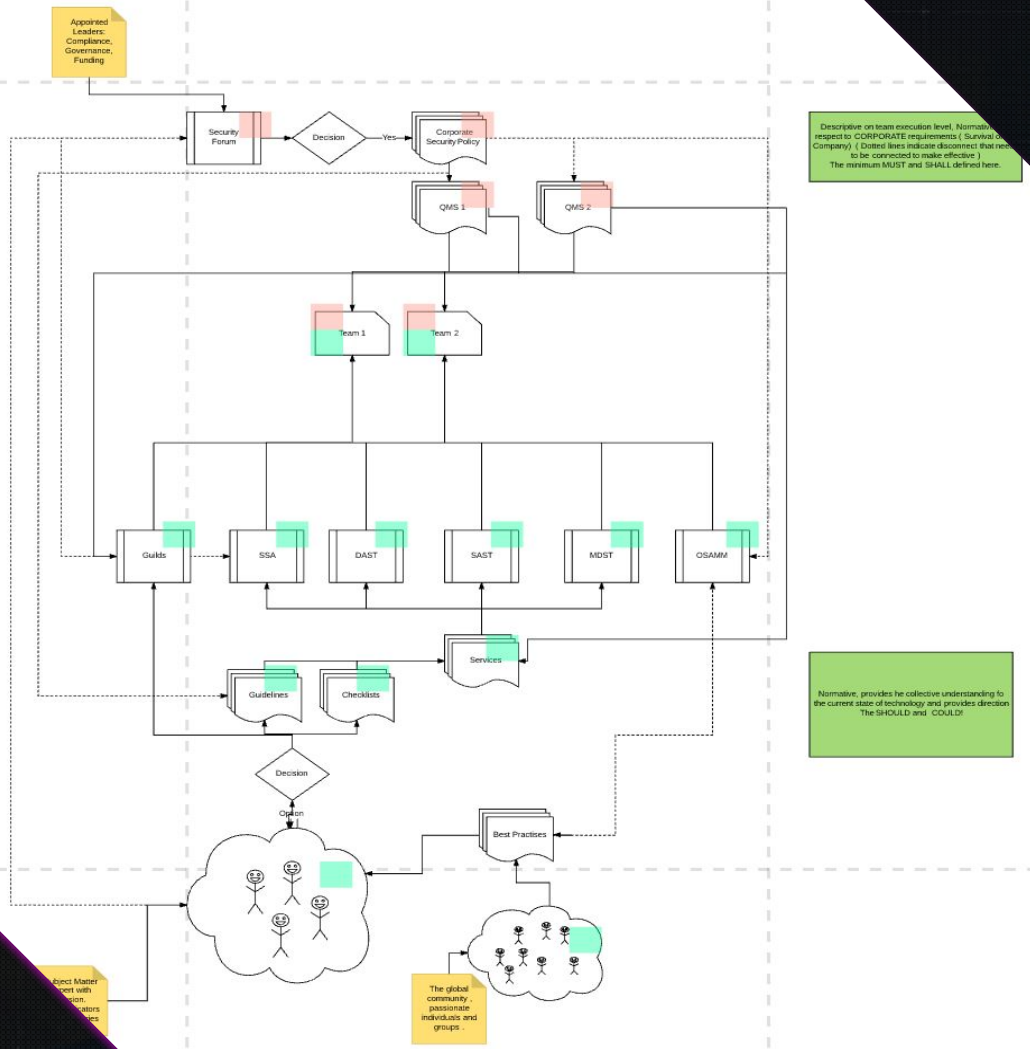
Dynamic Application Security Test (DAST)

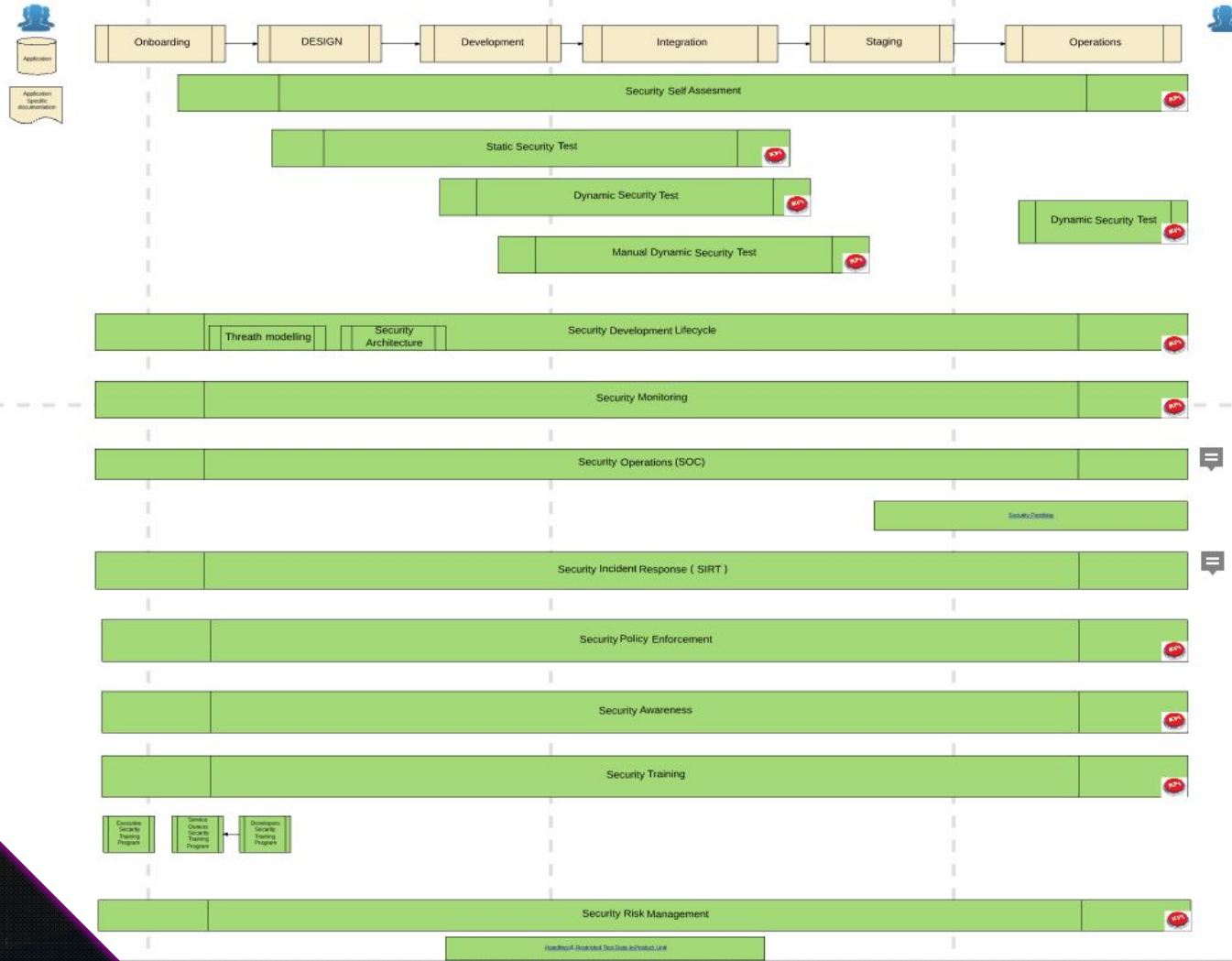
Security Operations

Data quality/validation

Management issue?


SAMM Current Score
Strategy & Metrics
Policy & Compliance
Education & Guidance
Threat Assessment
Security Requirements
Secure Architecture
Design Analysis
Implementation Review
Security Testing
Issue Management
Environment Hardening
1.93
1.45
0.97
0.48
Governance
Construction
Verification
Operations
Governance
Construction
Verification
Operations

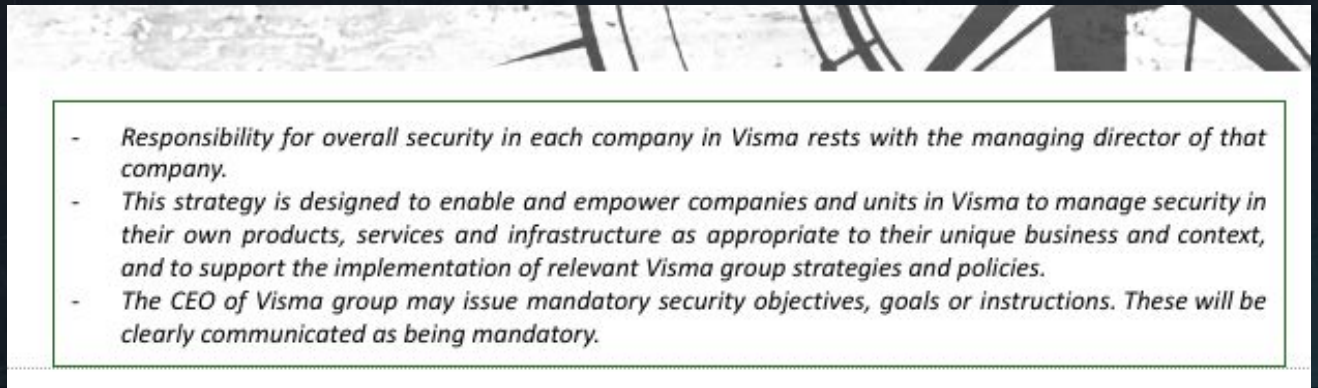

Appointed Leaders: Compliance, Governance, Funding
Security Forum
Decision
Yes
Corporate Security Policy
QMS 1
QMS 2
Team 1
Team 2
Guilds
SSA
DAST
SAST
MDST
OSAMM
Services
Guidelines
Checklists
Decision
Option
Best Practises
The global community , passionate individuals and groups .
Descriptive on team execution level, Normative respect to CORPORATE requirements (Survival Company) (Dotted lines indicate disconnect that need to be connected to make effective) The minimum MUST and SHALL defined here.
Normative, provides he collective understanding to the current state of technology and provides direction The SHOULD and COULD!


Onboarding
DESIGN
Development
Integration
Staging
Operations
Application
Application Specific documentation
Security Self Assesment
Static Security Test
Dynamic Security Test
Dynamic Security Test
Manual Dynamic Security Test
Threath modelling
Security Architecture
Security Development Lifecycle
Security Monitoring
Security Operations (SOC)
Security Incident Response (SIRT)
Security Policy Enforcement
Security Awareness
Security Training
Security Risk Management

Are your people Empowered?

Are your people enabled?

Have YOU embedded and Ensured the 2 above?



- *Responsibility for overall security in each company in Visma rests with the managing director of that company.*
- *This strategy is designed to enable and empower companies and units in Visma to manage security in their own products, services and infrastructure as appropriate to their unique business and context, and to support the implementation of relevant Visma group strategies and policies.*
- *The CEO of Visma group may issue mandatory security objectives, goals or instructions. These will be clearly communicated as being mandatory.*

Still curious?

"The game of Attribution" by Martin Öberg
Research on Empowering
Book chapter in PhD level on Product Sec/VASP
More videos to understand the fundamental thinking behind VASP
Our way of doing BugBounty talks
Visma Security Conference talks.
Twitch Streams
Podcasts : VASP and Academia , On transparency ,
Contribs to OpenSource : https://github.com/visma-prodsec
Next research "Sustainable Security Program" COMING SOON

Quokka : https://twitter.com/quokkaeveryhour


https://twitter.com/quokkaeveryhour