Visma Idella B.V.

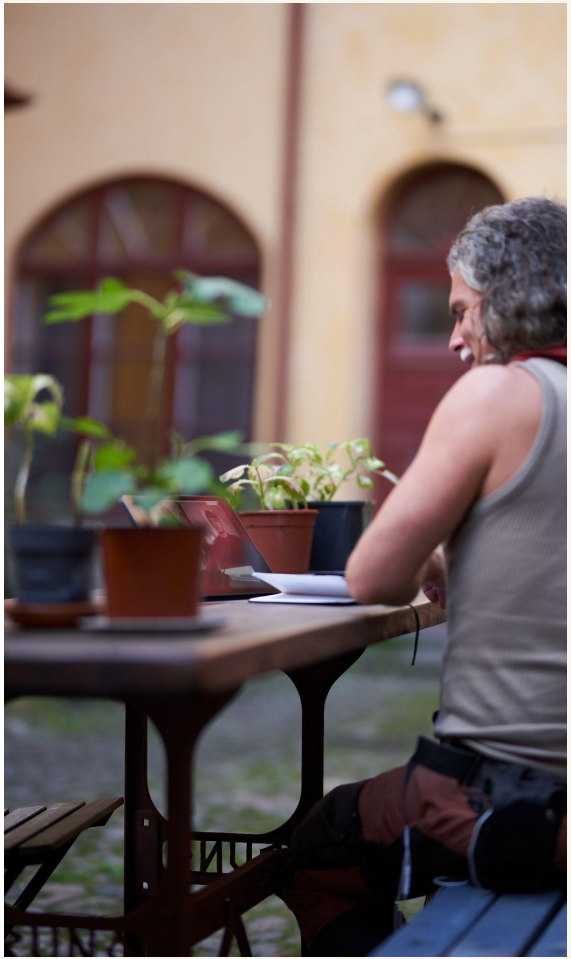
In Control met DORA

Dit webinar wordt opgenomen!

26 juni 2024

Lilian Rolefes *Risk Manager*
Corinna Angel *sr. Legal Counsel & Data Protection Manager*
Gerwin Dirkzwager, *Security Manager*

VISMA | idella



Corinna ANGEL
corinna.angel@visma.com

Gerwin DIRKZWAGER
gerwin.dirkzwager@visma.com

Lilian ROLEFES
lilian.rolefes@visma.com

Inhoud

1. Introductie
2. *Nieuw*: contractering
3. Fit/gap-analyse
4. ICT Risicobeheer: deepdive
    a. Protection & Prevention
    b. Detection
    c. Response & Recovery
5. Vooruitblik
6. Afsluiting

1. Introductie

3 blokken

- Blok 1: Contractering en Fit/gap-analyse
- Blok 2: Protection & Prevention
- Blok 3: Detection, Response & Recovery

Na elk blok behandelen we binnengekomen vragen.

1. Introductie

Corinna Angel

- Sr. Legal Counsel
- Data Protection Manager
- Lid Regulatory Guild
- Lid Information Security Board

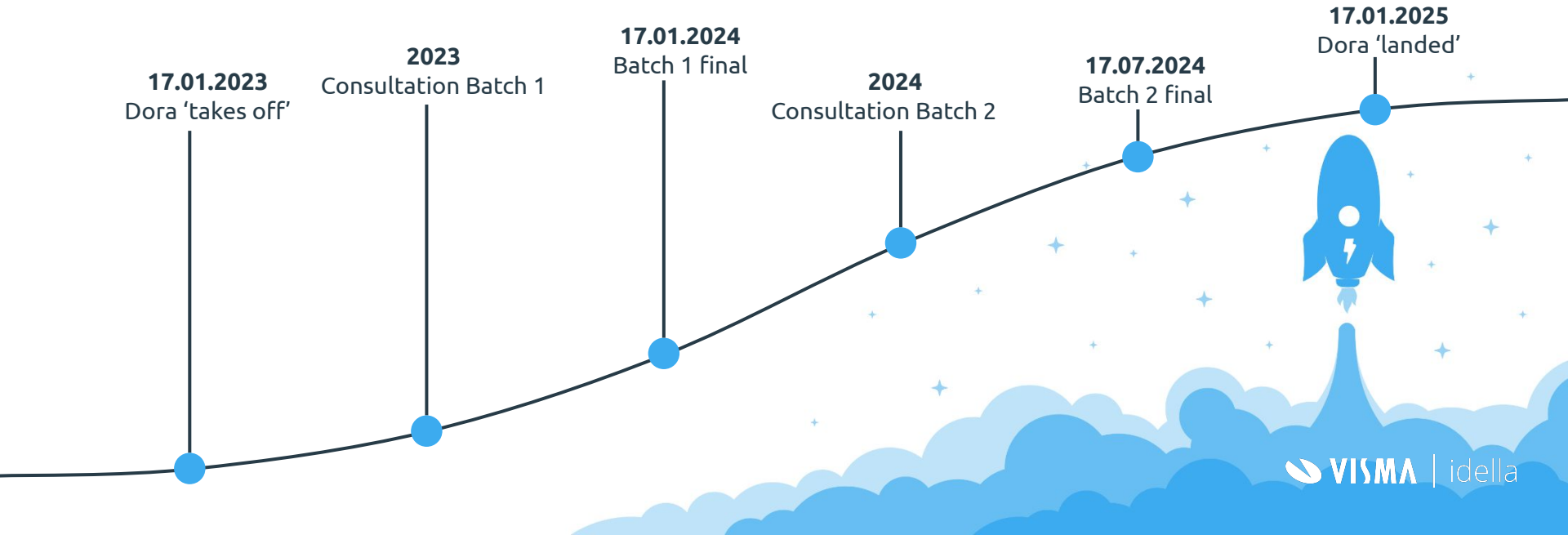
Lilian Rolefes

- Risk Manager
- Voorzitter Regulatory Guild

Gerwin Dirkzwager

- Security Manager
- Voorzitter Information Security Board

1. Introductie



2. Contractering (amendement)

Pensioenfederatie amendement

Auteur *Loyens & Loeff*

Betrokken partijen

1. Verbond van Verzekeraars
2. Pensioenfederatie
3. Dutch Fund and Asset Management Association (DUFAS)
4. Vereniging van Vermogensbeheerders & Adviseurs

Feedback

5. AFM
6. DNB

2. Contractering (amendement)

Pensioenfederatie amendement*

1. Kritieke of belangrijke ICT-leveranciers
   a. https://www.pensioenfederatie.nl/website/themas/pensioenuitvoering/dora
   b. Opbouw

1. Definities en interpretatie 2. Amendement (toelichting) 3. Functiebeschrijving en uitbesteding 4. Locaties van Functies en gegevensverwerking 5. Dienstenniveau 6. Gegevensbescherming, toegang, herstel en teruggave 7. Assistentie bij incidenten 8. Samenwerking met autoriteiten	9. Beëindigingsrechten 10. Deelname aan training 11. Opzegtermijn en rapportageverplichting 12. Bedrijfscontinuïteit en ICT-beveiliging 13. Testen 14. Monitoring (audit) 15. Exit 16. Vertrouwelijkheid 17. Diverse 18. Jurisdictie

**Ontwikkeld voor diverse financiële entiteiten en vereisen daarom specifieke aanpassingen*

2. Contractering

Ontvangst en studie

Mei/ Juni '24

Vaststelling Visma Idella

Juni/ Juli '24

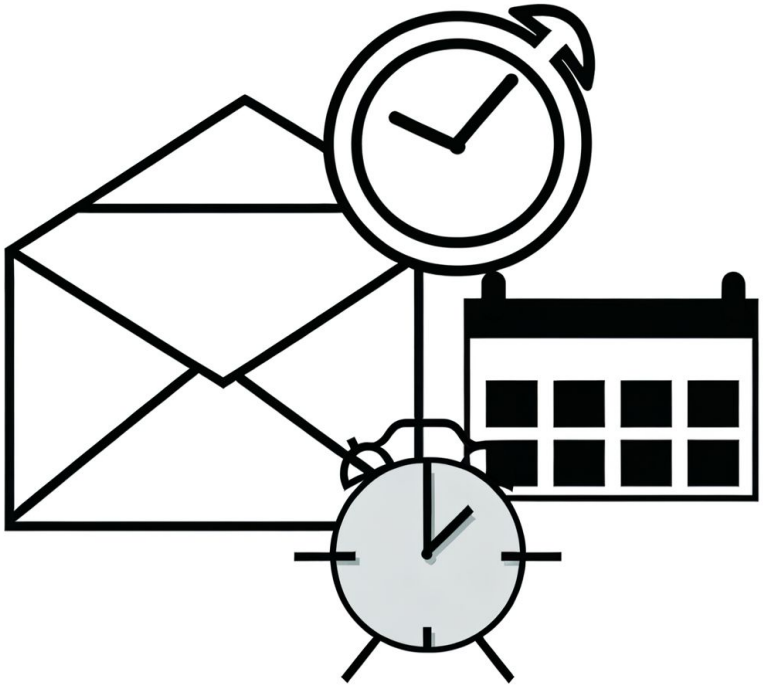
Overleg Klant

September/Oktober '24

Vaststelling

November '24

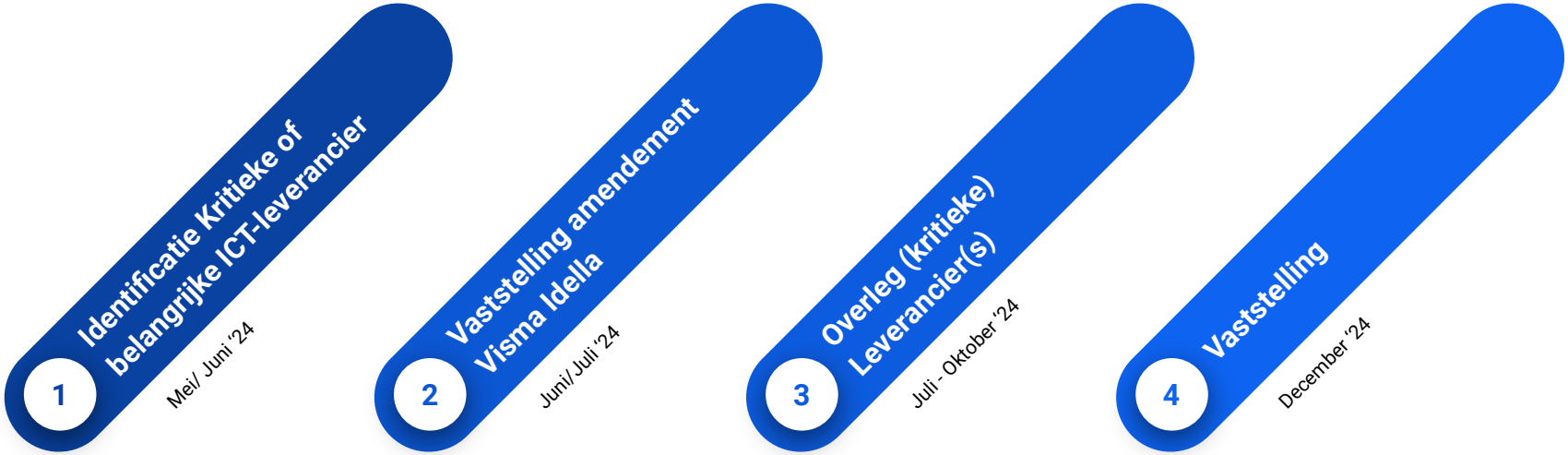
2. Contractering



Uitnodigingen om tot bespreking te komen volgen asap

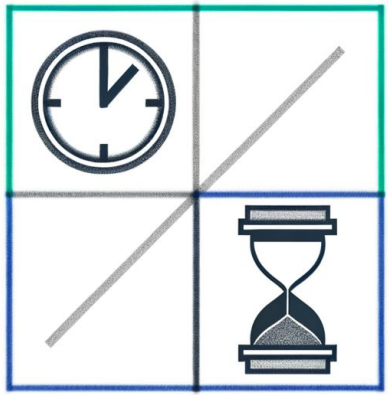
(***via uw CS-manager***)

2. Contractering



mei/juni = focus kritieke of belangrijke ICT-leveranciers

3. Fit/gap-analyse



PENDING

4. ICT Risicobeheer

Protection & Prevention

Protection & Prevention

(…) *continuously monitor and control the security and functioning of ICT systems and tools and shall minimise the impact of ICT risk on ICT systems through the deployment of appropriate* ***ICT security tools****, policies and procedures.*

- **Belangrijkste DORA-vereisten:**
  - ICT-risicobeheer,
  - Robuuste ‘governance frameworks’,
  - Grondig testen van ICT-systemen.

- Nadruk ligt op het belang van het beschermen van gevoelige gegevens en het waarborgen van de operationele integriteit.

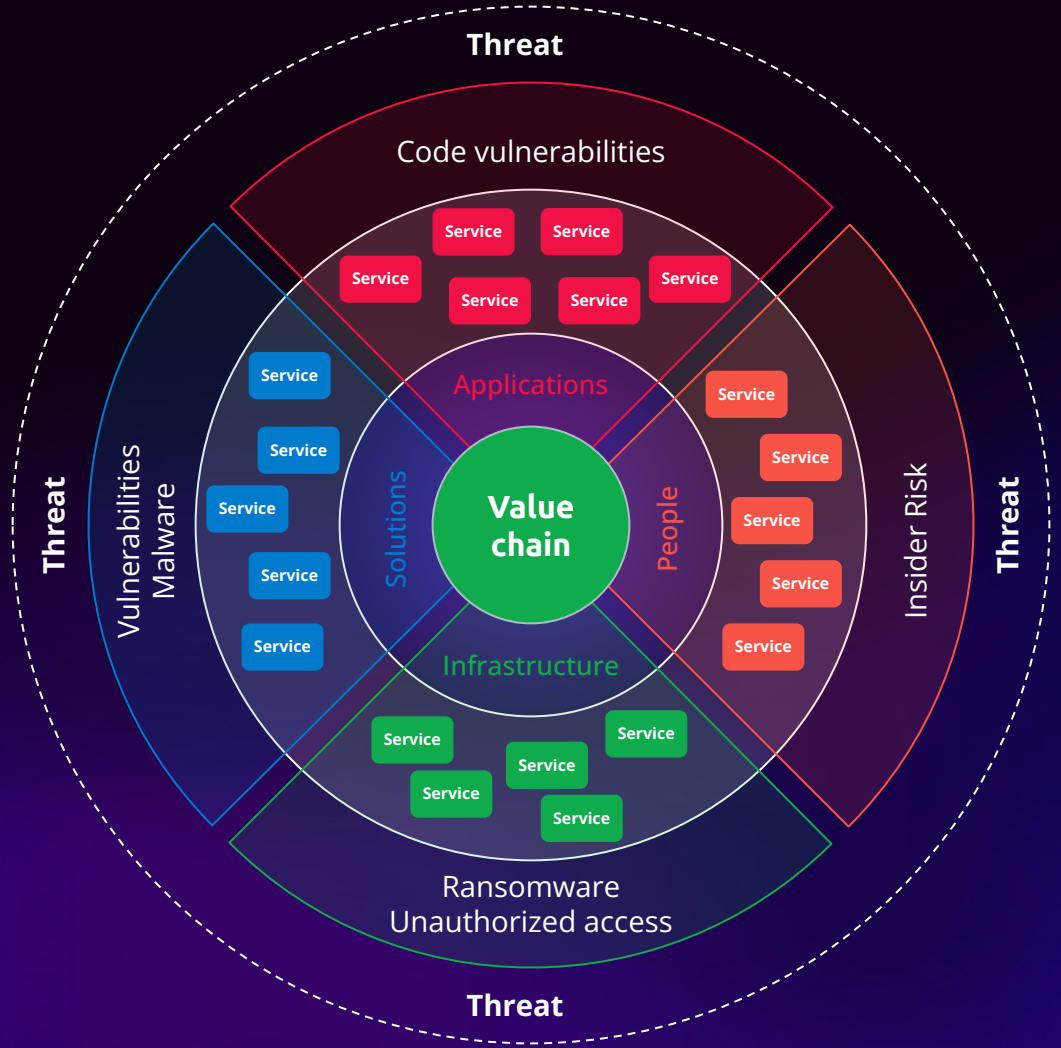
Protection & Prevention: Implicaties

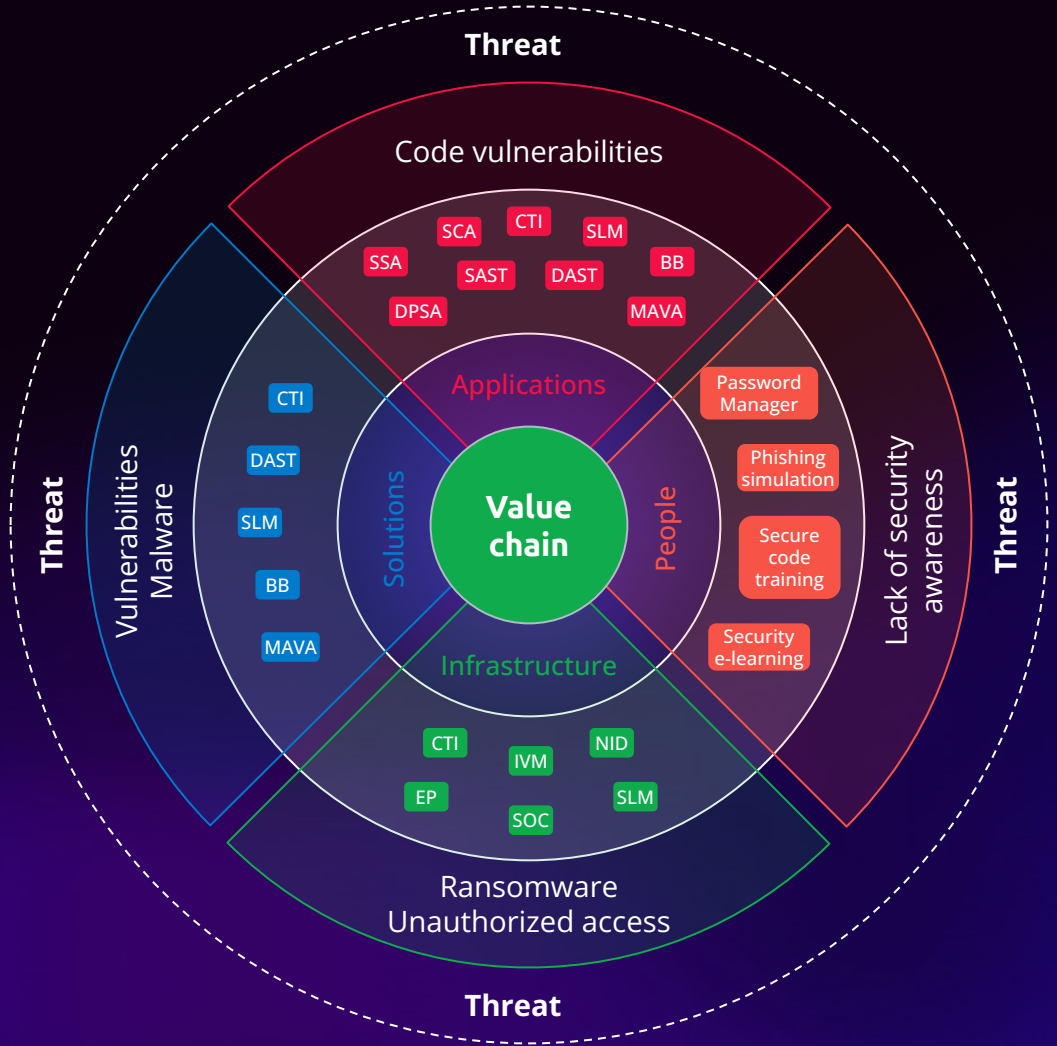
- **Compliance betekent:**
  - Het aanpassen van beleid, processen en technologieën om te voldoen aan de strenge eisen van DORA.
    - Momenteel worden alle beleidsstukken onder de loep genomen
    - Als onderdeel van migratie naar ISO/IEC 27001:2022
    - Ook beleidsstukken en procesbeschrijvingen die niet direct onder ISO27001 verplicht zijn worden meegenomen.
  - Het aanpakken van de uitdagingen en kansen bij het vergroten van de ICT-veerkracht.
  - Alle producten geregistreerd binnen **Visma Application Security Program (VASP)**
    - Alle producten ‘in production’ op niveau **‘Platinum’**

Visma Application
Security Program

VISMA | idella

Visma
Security Program




Threat
Code vulnerabilities
SCA
CTI
SLM
SSA
SAST
DAST
BB
DPSA
MAVA
Applications
Threat
Vulnerabilities
Malware
CTI
DAST
SLM
BB
MAVA
Solutions
Value chain
People
Password Manager
Phishing simulation
Secure code training
Security e-learning
Lack of security awareness
Threat
Infrastructure
CTI
IVM
NID
EP
SLM
SOC
Ransomware
Unauthorized access
Threat

Visma **Application** Security Program

Or just simply VASP

Protection & Prevention: Build in Quality

Security testen: Alle software componenten worden continue getest en gemonitored op security.

VismaIdella.Vips.DocumentManagement

6 total issues | Configure | Azure DevOps | master

Start scan

Issues | Checks

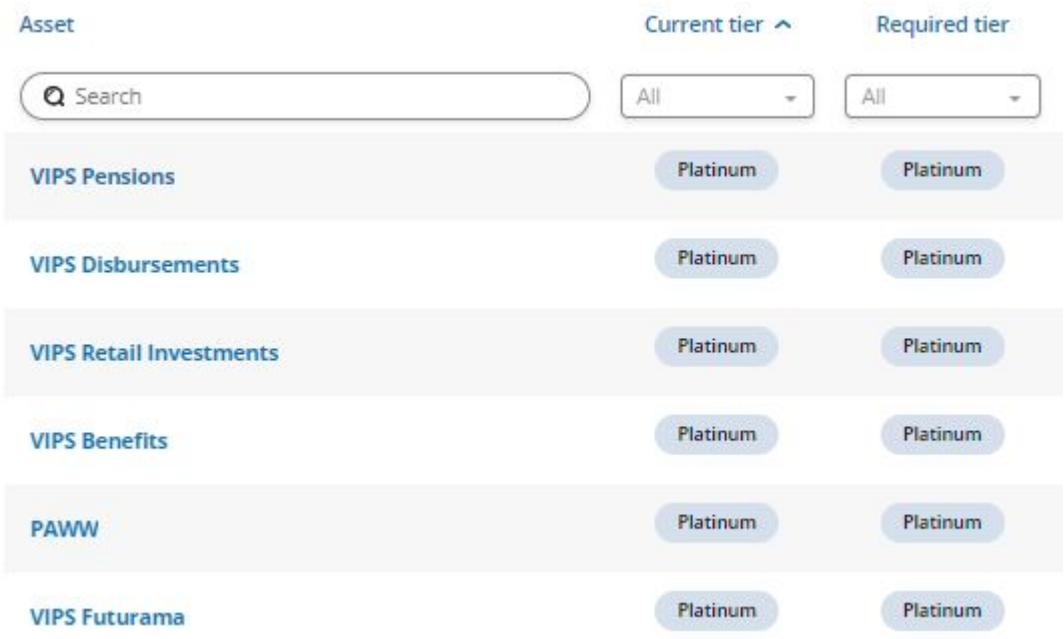
Last scan 17 hours ago

Type	Checks	Description	Compliance	Issues
	Open source dependency monitoring — View monitored lockfiles	We monitor 3rd party dependencies you are using in your app for any known vulnerabilities.	Compliant	0
	Exposed secrets monitoring	We are monitoring your application for any secrets which have been accidentally exposed in your source code, currently or at one point in the past.	Compliant	0
	License management	Aikido checks the licenses of all your dependencies to make sure you are legally permitted to make use of them.	Compliant	0
	SAST — Create custom rule — View SAST rules	Static application security testing.	Compliant	0
	IaC — View IaC rules	Infrastructure as Code testing. Check which files we can monitor in your application.	Compliant	0
	Malware detection — View malware monitor	Aikido checks for dependencies which are actually containing malware.	Compliant	0
	Mobile issues — View mobile rules	Mobile manifest file monitoring.	Compliant	0

Protection & Prevention: ICT Security Tools

Onderdeel van VASP zijn de inzet van vele testen gebruik makend van diverse tools:

- CTI - Cyber Threat Intelligence
- Bug Bounty
- PENTEST
- SLM - Security Log Management (SIEM)
- SSA - Security Self-Assessment
- DPSA - Data Protection Self-Assessment (GDPR compliance)
- SCA - Software Composition Analysis (Aikido)
- SAST - Static Application Security Test (Polaris)



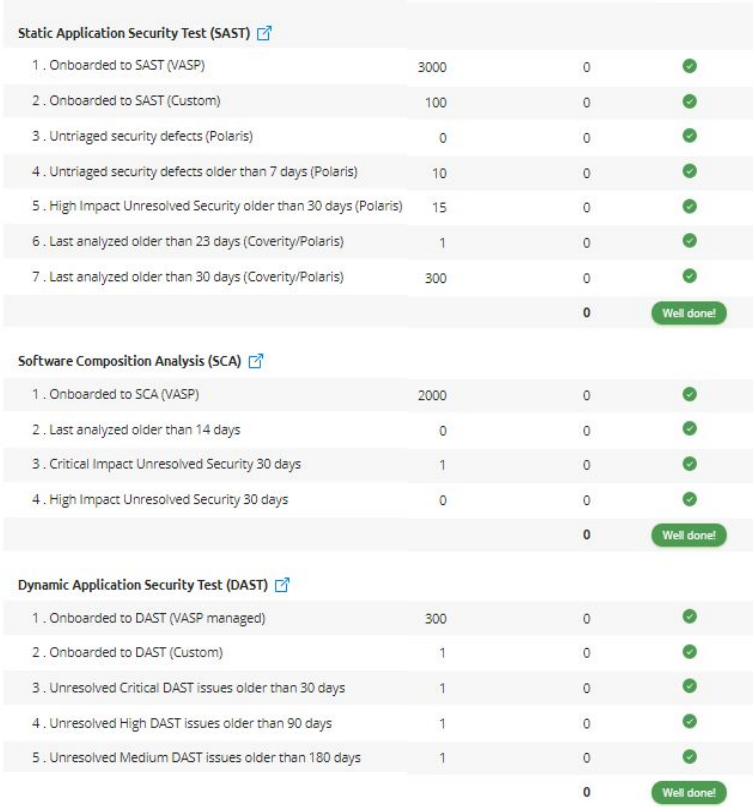
VISMA | idella

Build in Quality: Security testen

Static Application Security Test (SAST): De gebruikte tool heet Polaris en is een clouddienst van Synopsys. Deze tool wordt gebruikt om een codescan uit te voeren en analyse op beveiligingsfouten tijdens het ontwikkelproces.

Software Composition Analysis (SCA): Aikido is een Software Composition Analysis-tool waarmee de ontwikkelaars kwetsbaarheden en licentie- problemen in Open Source-componenten kunnen identificeren.

Dynamic Application Security Test (DAST): DAST is een proces waarbij een applicatie of software- product in een werkende staat wordt getest. Deze tests zijn nuttig voor naleving van de industrie- standaarden en om te controleren of de algemene beveiligingsmaatregelen aanwezig zijn.



Static Application Security Test (SAST)			
1 . Onboarded to SAST (VASP)	3000	0	✓
2 . Onboarded to SAST (Custom)	100	0	✓
3 . Untriaged security defects (Polaris)	0	0	✓
4 . Untriaged security defects older than 7 days (Polaris)	10	0	✓
5 . High Impact Unresolved Security older than 30 days (Polaris)	15	0	✓
6 . Last analyzed older than 23 days (Coverity/Polaris)	1	0	✓
7 . Last analyzed older than 30 days (Coverity/Polaris)	300	0	✓
		0	Well done!
Software Composition Analysis (SCA)			
1 . Onboarded to SCA (VASP)	2000	0	✓
2 . Last analyzed older than 14 days	0	0	✓
3 . Critical Impact Unresolved Security 30 days	1	0	✓
4 . High Impact Unresolved Security 30 days	0	0	✓
		0	Well done!
Dynamic Application Security Test (DAST)			
1 . Onboarded to DAST (VASP managed)	300	0	✓
2 . Onboarded to DAST (Custom)	1	0	✓
3 . Unresolved Critical DAST issues older than 30 days	1	0	✓
4 . Unresolved High DAST issues older than 90 days	1	0	✓
5 . Unresolved Medium DAST issues older than 180 days	1	0	✓
		0	Well done!

VISMA | idella

Build in Quality: Security testen

Penetration Testing (PENTEST):
Penetratietesten is een handmatige testservice. Uitgevoerd door een gespecialiseerd pentest-team binnen Visma.

Security Log Management (SLM): Om ervoor te zorgen dat Visma zich in de best mogelijke positie bevindt om cybercriminaliteit waarbij onze diensten en klanten betrokken zijn, te onderzoeken en te voorkomen. Dit is een binnen Visma gestandaardiseerd proces voor het beheer van beveiligingslogboeken. 24/7 monitoring vindt plaats zowel geautomatiseerd als handmatige opvolging van geconstateerde 'security events'.

Penetration Testing (PENTEST)				
1 . PENTEST never performed (VASP)	0	3000	0	✓
2 . PENTEST older than 16 months	0	1	0	✓
3 . PENTEST older than 18 months	0	500	0	✓
4 . PENTEST older than 24 months	0	1	0	✓
5 . Unresolved critical PENTEST issues older than 30 days	0	3000	0	✓
6 . Unresolved severe PENTEST issues older than 90 days	0	1000	0	✓
7 . Unresolved recommended PENTEST issues older 180 days	0	100	0	✓
			0	Well done!
Security Operations				
1 . Onboarded to Cyber Threat Intelligence Service (CTI) (VASP)	0	300	0	✓
2 . Onboarded to Infrastructure Security Log Management (SLM) - Non-	0	0	0	✓
			0	Well done!

VISMA | idella

Build in Quality: Security testen

Bug Bounty (BB)				
1 . Onboarded to Bug Bounty (VASP)	1	1	1	!
2 . Unresolved Low, Medium and High Bug Bounty issues older than 94 days	0	1000	0	✓
3 . Unresolved Critical Bug Bounty issues older than 9 days	0	3000	0	✓
			1	

Bug Bounty (BB): Is een manier om de veiligheid van een dienst te testen met ethische hackers over de hele wereld die betaald zullen worden om beveiligingskwetsbaarheden aan ons te melden. De kracht van een Bug Bounty-programma zit hem in het aantal ogen en de expertise, het continu testen en de diversiteit tussen hackers – de hackers zijn gespecialiseerd in verschillende technologieën en dit leidt tot een zeer goede kwaliteit van de meldingen.

Meer onderzoekers = Meer bevindingen = Betere beveiliging.

Het Bug Bounty-programma vormt een aanvulling op alle andere beveiligingsdiensten die we leveren op het gebied van beveiligingstests. Alleen specifieke assets vallen binnen de scope en als zodanig accepteert Visma alleen meldingen daarvoor.

VISMA | idella

4. ICT Risicobeheer

Detection

ICT-related incident detection and response

(...) have in place mechanisms to promptly detect anomalous activities, in accordance with Article 17, including ICT network performance issues and ICT-related incidents, and to identify potential material single points of failure.

- **"Detection" in de context van DORA:** het identificeren van potentiële ICT-gerelateerde verstoringen voordat deze gevolgen hebben voor de bedrijfsvoering.
- Het belang van het ontwikkelen van robuuste detectiemogelijkheden als onderdeel van ICT-risicobeheer

VISMA | idella

Detection

- **Definitie van ICT-Related incidents (DORA):** één enkele gebeurtenis of een reeks onderling verbonden gebeurtenissen die niet door de financiële entiteit zijn gepland en die de veiligheid van het netwerk en de informatiesystemen in gevaar brengen en een negatief effect hebben op de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens, of op de diensten die door de financiële entiteit worden geleverd.

Implementatie van detectiestrategieën

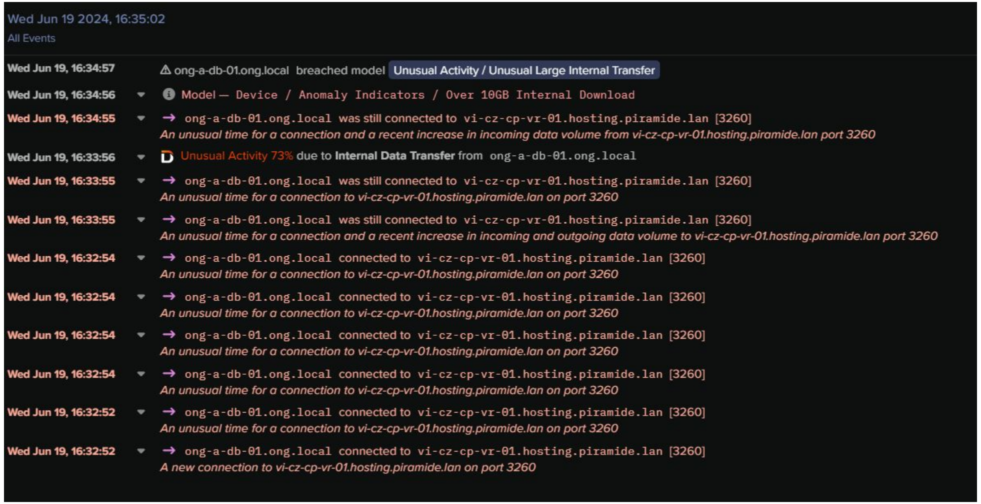
- Specifieke strategieën en technologieën die Visma Idella gebruikt voor effectieve detectie:
  - Anomaliedetectie bij systeembewerkingen.
  - Realtime monitoringtools voor vroege waarschuwingssignalen.
  - Geautomatiseerde mechanismen voor waarschuwingen en incidentrapportage.

Detection: Verbetering van de detectiemogelijkheden

Versterking van detectiekaders

Stappen om de detectiemechanismen binnen de infrastructuur van Visma Idella te verbeteren:

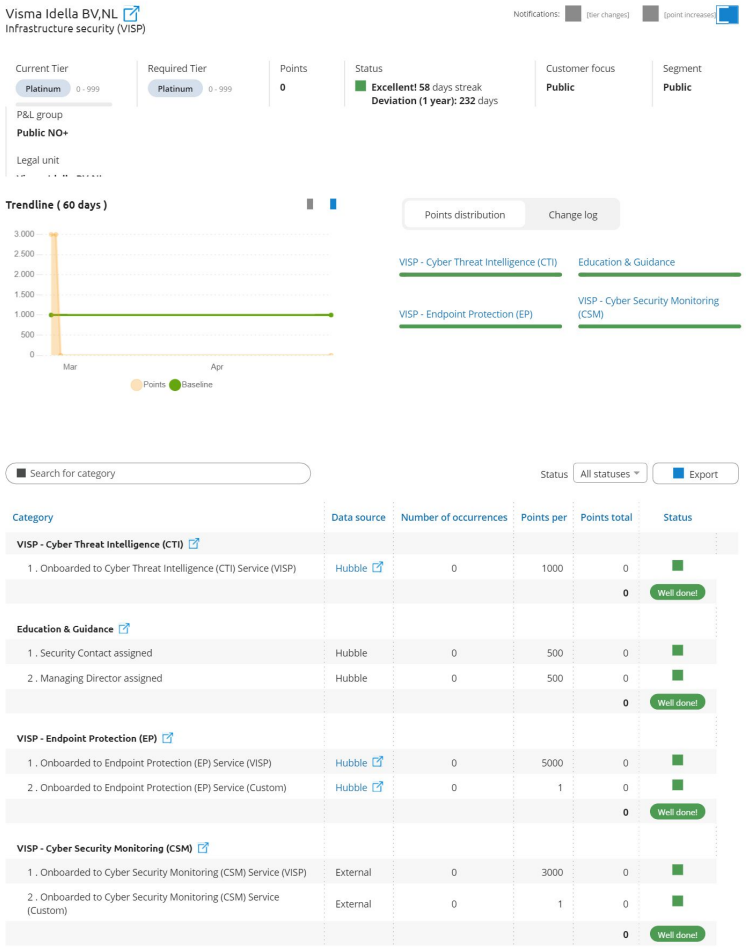
- Continue verbetering van data-analyse en monitoring.
- Implementatie van AI en machine learning voor voorspellende analyses.
- Regelmatige trainingen en simulaties voor IT-personeel en belanghebbenden.



Detection: Verbetering van de detectiemogelijkheden

Stappen om de detectiemechanismen binnen de infrastructuur van Visma Idella te verbeteren:

- Inzet van Infrastructure Security (VISP).
- Implementatie van AI en machine learning voor voorspellende analyses (Darktrace).
- Endpoint protection met AI-gestuurde cyberbeveiliging (SentinelOne).



Detection: Verbetering van de detectiemogelijkheden

Cyber Threat Intelligence (CTI):
De CTI-monitoringservice is een geweldige en beproefde manier om de vermeldingen van onze en de klants assets in verdachte context te detecteren en controleren.
Het biedt context voor een proactieve aanpak, waardoor wij een kijkje kunt nemen in wie onze middelen heeft genoemd en mogelijke indicatoren van een aanval die naar hen toe leidt, wat hun motivatie en capaciteiten zijn, en naar welke indicatoren van compromissen wij in onze services moet zoeken . Het platform helpt bij het nemen van beslissingen over de voortgang van onze beveiligingsgerelateerde acties.

Deze service controleert voortdurend op bedreigingen van de buitenwereld tegen onze activa/ domeinen/ infrastructuur/ branding.
De belangrijkste gebieden die zij monitoren zijn:

- Darkweb-marktplaatsen
- Dark/Deep Web-forums
- Github-opslagplaatsen
- Certificaattransparantie
- Domeinregistratie
- Typosquatting
- Sociale media

Detection: Verbetering van de detectiemogelijkheden

To be announced...

Continue verbeteren door nieuwe en aangepaste diensten en producten.

Binnenkort de introductie van **ORCA.** Een cloud-gebaseerde beveiligingsplatform dat is ontworpen breed en diep inzicht te bieden in beveiligingsrisico's binnen cloudomgevingen zonder de prestaties te beïnvloeden.

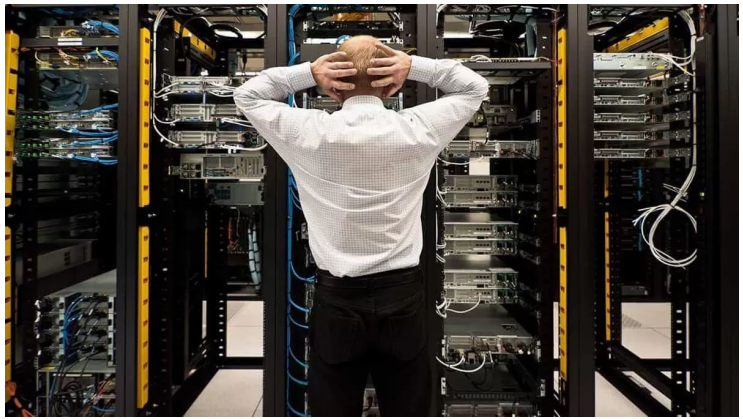
4. ICT Risicobeheer

Response & Recovery

Response & Recovery

(...) put in place a comprehensive ICT business continuity policy, which may be adopted as a dedicated specific policy, forming an integral part of the overall business continuity policy of the financial entity.

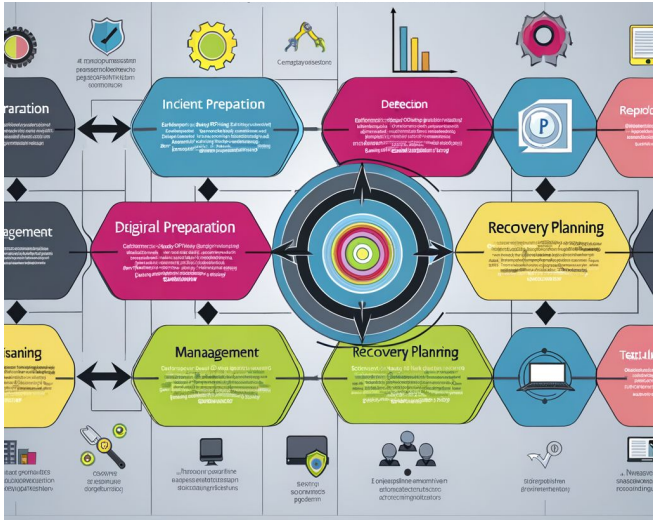
- Zorgen voor snel herstel



The Importance of Response & Recovery

Pijlers van veerkracht: respons en herstel

- Overzicht van de componenten "Response & Recovery" onder DORA.
- Tijdige en effectieve respons en herstel van cruciaal belang voor het behoud van de operationele continuïteit.



VISMA | idella

The Importance of Response & Recovery

Een beknopt overzicht van deze componenten:

1. **Incidentresponse**
   Voorbereiding
   Detectie en Analyse
2. **Incidentmanagement**
   Reactie
   Coördinatie en Communicatie
3. **Herstel en Continuïteit**
   Herstelplannen
   Geleerde Lessen
4. **Testen en Situatiebewustzijn**
   ICT Testen
   Threat Intelligence en Informatie Delen
5. **Regelgevende Vereisten**
   Rapportage
   Compliance

Continue verbetering en aanpassing

Wij zijn er nog niet. Onze producten en diensten evolueren.

Hier wordt rekening gehouden met:

- De aanpak voor het continu testen, leren en aanpassen van de respons- en herstelplannen.
- Bijjhouden van compliance
- Lessen uit eerdere incidenten
- Het identificeren van noodzakelijke technologische updates of procesverbeteringen

5. Vooruitblik

Planning (onder voorbehoud)

Voorjaar:
- Kennissessie 2 (juni*) ✅
- Mapping DNB GP Informatiebeveiliging 2023 ✅
- DNB Security Self Assessment ✖️
- ISO27001 (re-audit) ✅

Zomer:
- Kennissessie 3 (september*)
- Vaststelling beleid en processen **eerste** batch (1.0)
- Oplevering contractuele wijzigingen bestaande klanten
- Herijking afspraken kritieke leveranciers (0.7)
- ISO27001-2022 mapping/overige assurance
- ICT informatieregister (0.8)

Najaar:
- Kennissessie 4 (november*)
- 0.9 vaststelling beleid en processen **tweede** batch
- Afronding contractuele wijzigingen
- Herijking afspraken kritieke leveranciers (1.0)

Winter:
- Vaststelling beleid en processen **tweede** batch (1.0)
- Oplevering Informatieregister (1.0)

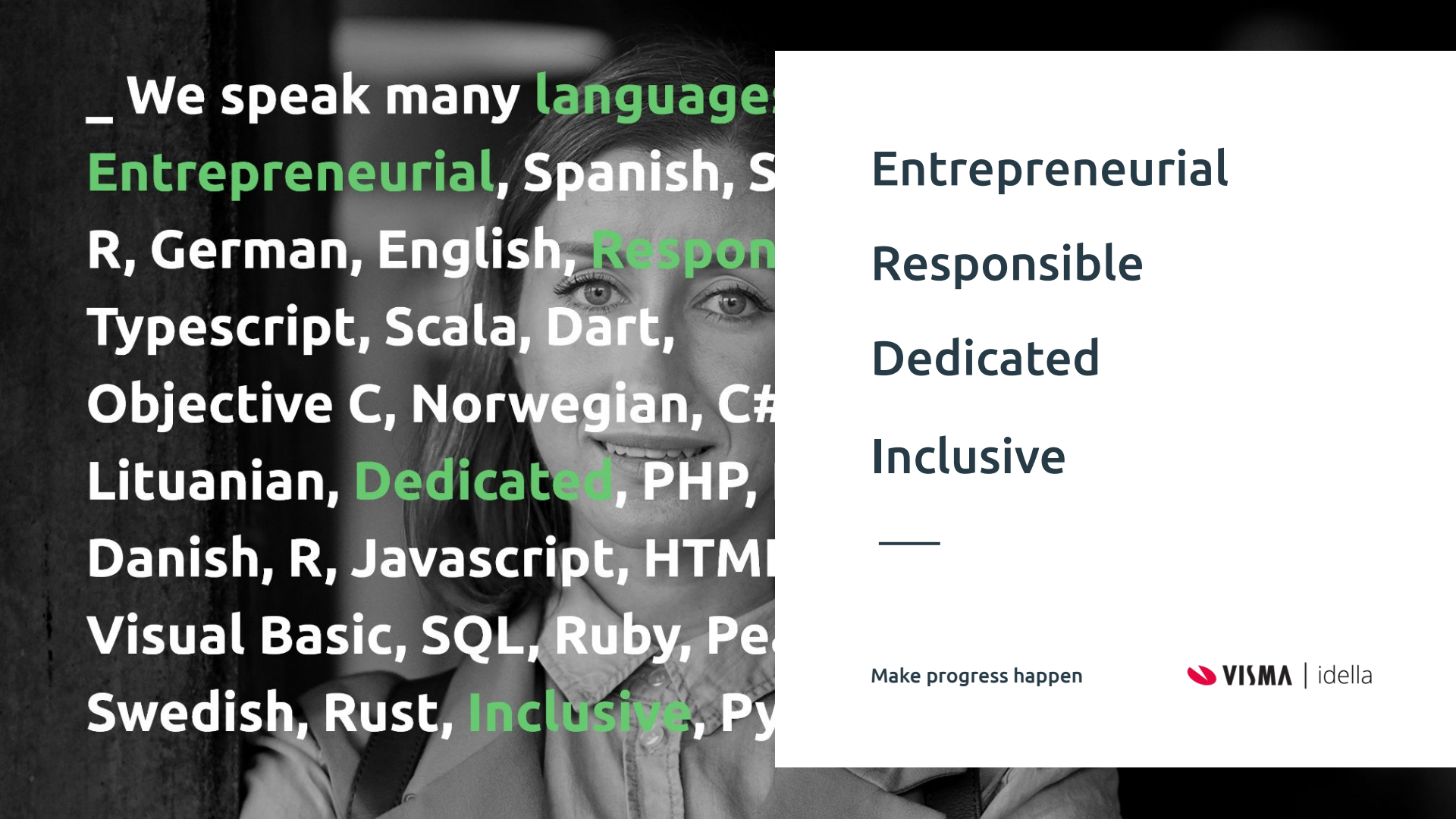
Feestelijke afronding DORA + kennissessie
- Locatie: Amersfoort
- Datum: volgt plus tijdstip

*digitaal

VISMA | idella

6. Afsluiting

VISMA | idella



Entrepreneurial

Responsible

Dedicated

Inclusive

Make progress happen

VISMA | idella