Visma Idella B.V.

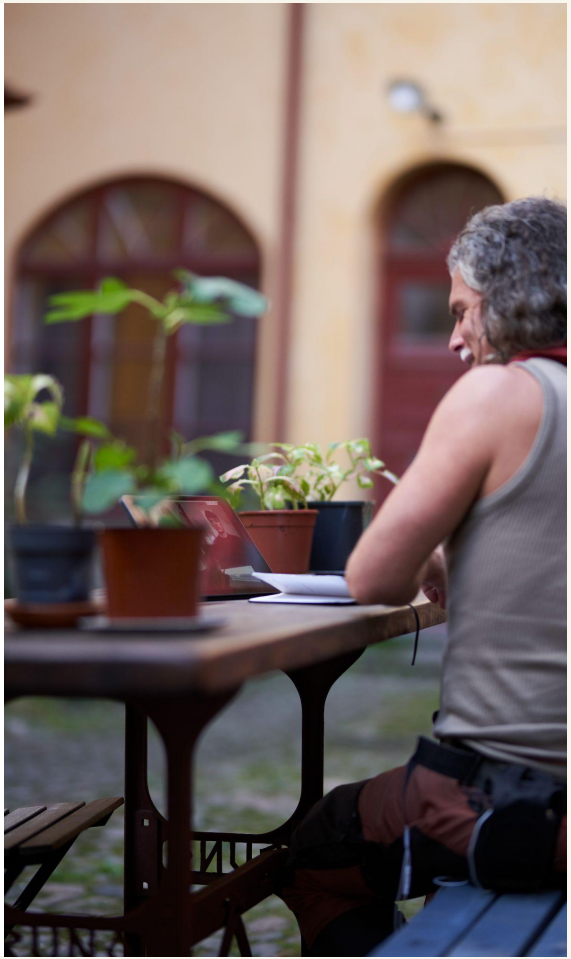
In Control met DORA

Dit webinar wordt opgenomen!

21 maart 2024

Lilian Rolefes *Risk Manager*
Corinna Angel *sr. Legal Counsel & Data Protection Manager*

VISMA | idella



Corinna ANGEL
corinna.angel@visma.com

Lilian ROLEFES
lilian.rolefes@visma.com

Introductie

Corinna Angel

- Sr. Legal Counsel
- Data Protection Manager
- Regulatory Guild
- ISB-member

Lilian Rolefes

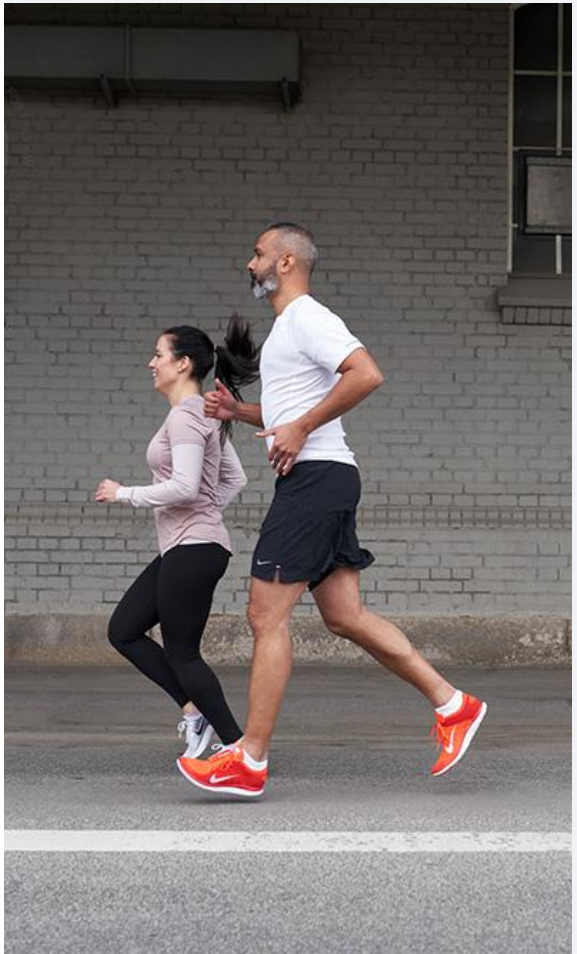
- Risk Manager
- Regulatory Guild
- ISB-member

Gerwin Dirkzwager (*afwezig*)

- Security Manager
- ISB-member

Inhoud

1. Status-update
2. Werk in uitvoering
3. Risico en rapportage
4. Volgende stap(pen)



VISMA | idella

2 maart 2024

DORA vraagt om versterking van het Digital Resilience Framework van financiële bedrijven

https://www.winmagpro.nl/dora-vraagt-om-versterking-van-het-digital-resilience-framework-van-financiele-bedrijven

25 februari 2024

Capgemini: The challenges and opportunities DORA presents

https://fintechmagazine.com/articles/capgemini-the-challenges-and-opportunities-dora-presents

7 maart 2024

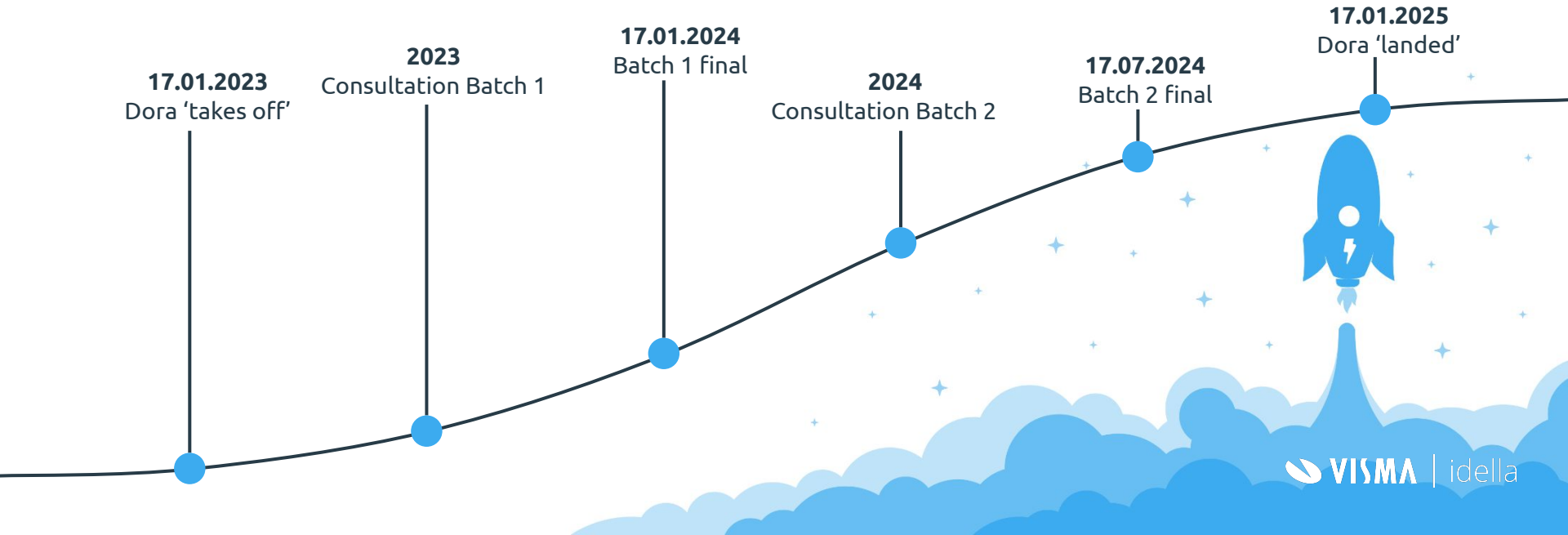
DORA-update: stel kader op voor ICT-risicobeheer

https://www.afm.nl/en/sector/actueel/2024/maart/dora-update-3

DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

VISMA | idella

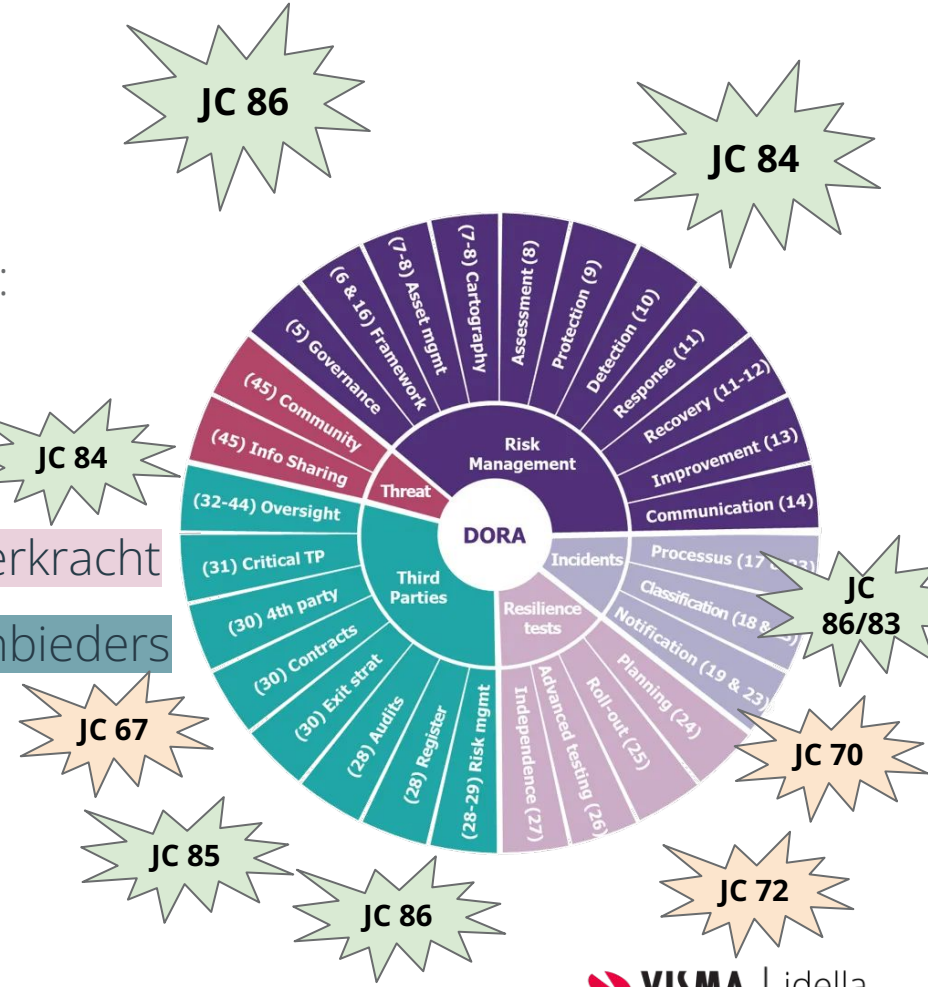
DORA: Status-update



DORA: Status-update

DORA richt zich op de volgende 5 pijlers:

1. **ICT-risicobeheer**
2. **ICT-gerelateerde incidenten**
3. Testen van digitale operationele veerkracht
4. Beheer van ICT-risico van derde aanbieders
5. **Informatie-uitwisseling**



VISMA | idella

https://www.dora-info.eu/dora/

Visma Idella's DORA DNA-string

Analyse beleid
rule books
ESA/ DNB

Classificatie &
rapportage
incidenten

Testen
weerbaarheid

Risicobeheersing
3e partijen

Gilde wet- en
regelgeving

DORA Task
force Visma

Impact
analyse

Risk & Due
Dilligence

DORA: Status-update

- Training en kennisvergaring (eind 2023)
- Fit-gap analyse op bestaand beleid en processen (2023)
    - **8 maart 2024:** Template voor GAP analyse DORA gepubliceerd door de Pensioenfederatie
- ISO27001: opvolg audit
- DNB Self Assessment
- Eerste Batch - gefinaliseerd (januari 2024)
    - Zie o.a. RTS 86: artikelen 7-4, 7-5, 8-2-b, 13-1-m, 23-2-a, 26-4,

VISMA | idella

DORA: Status-update

Datum	Referentie	Titel
17/01/2024	JC 2023 83	Final Report on draft RTS on classification of major incidents and significant cyber threats
17/01/2024	JC 2023 84	Final report on draft RTS to specify the policy on ICT services supporting critical or important functions
17/01/2024	JC 2023 85	Final report on draft ITS on Register of Information
17/01/2024	JC 2023 86	Final report on draft RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework
30/01/2024	DORA	Register Information Templates Illustration

Bron: esma.europa.com (*laatst bezocht 04.03.2024)*

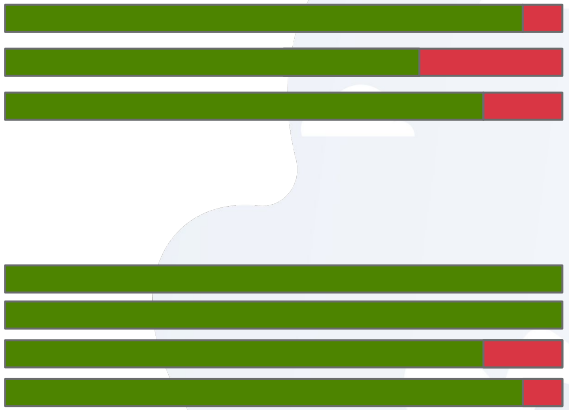
DORA: werk in uitvoering

- Beleid & processen
  - Focus-gebieden
    - Exitstrategie (art. 30.f Dora)
    - Incidentenbeleid (JC86/83/70)
    - Vendor & asset management (JC 67)

- Ketenregie
  - Initiëren gesprekken kritieke toeleveranciers
  - Tussentijdse (risk) assessment kritieke toeleveranciers
  - Tussentijdse (risk) assessment overige leveranciers
  - Risk- en DD-assessment >2025 (template)

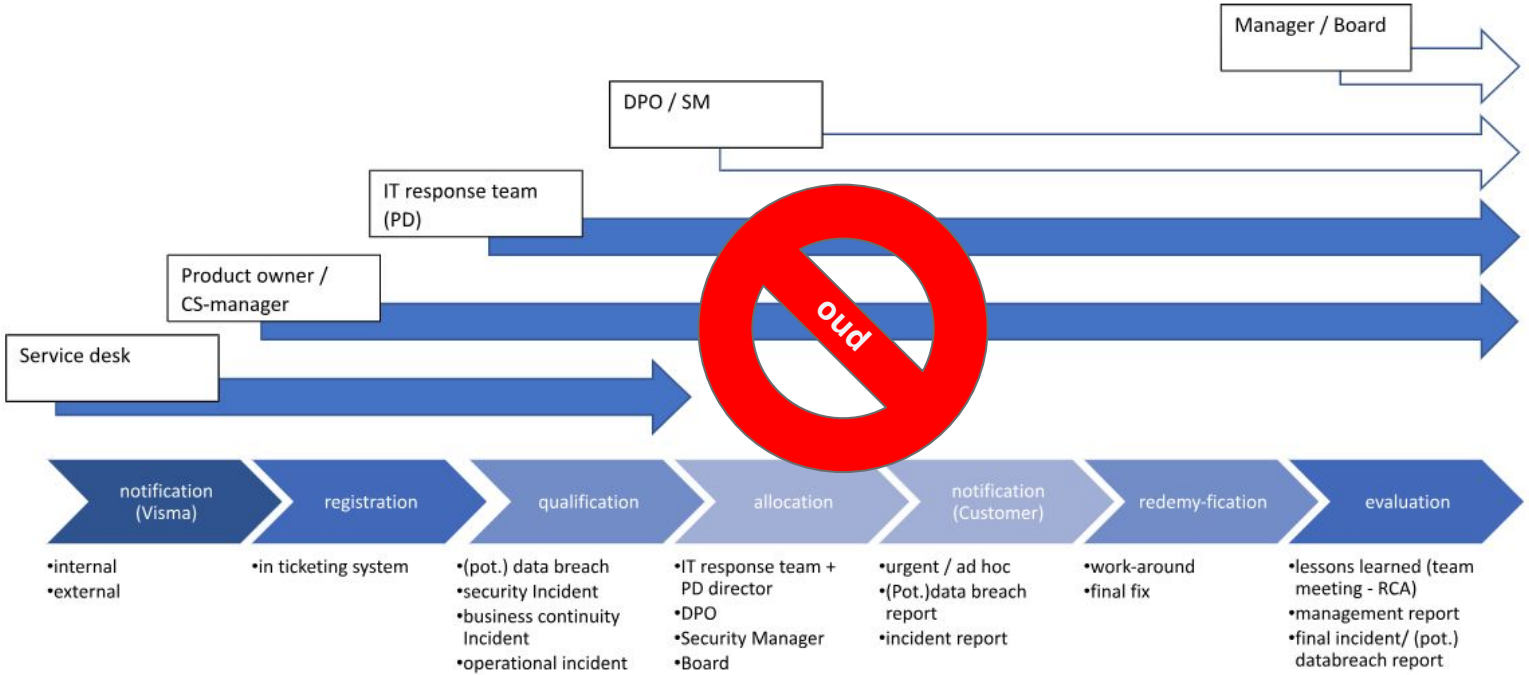
Maandelijks overleg Visma IT&C voor o.a. Azure, AWS, Google.

Status: maart 2024



VISMA | idella

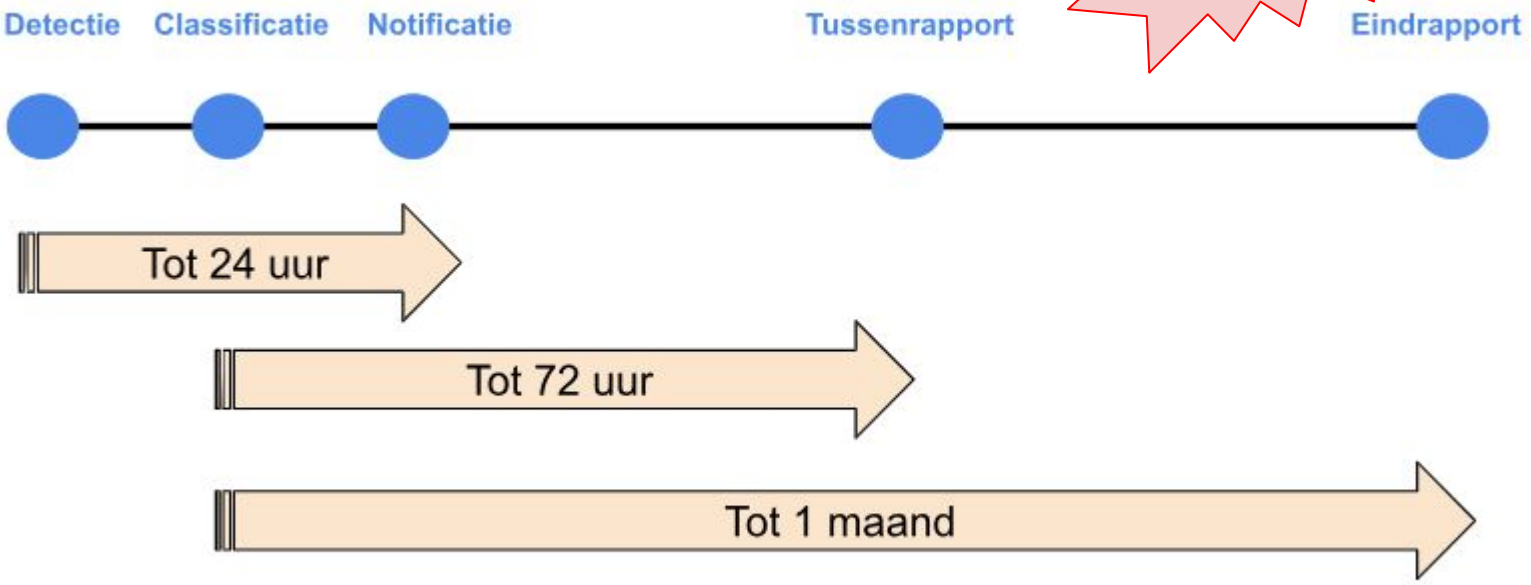
Incident(en) - algemeen -



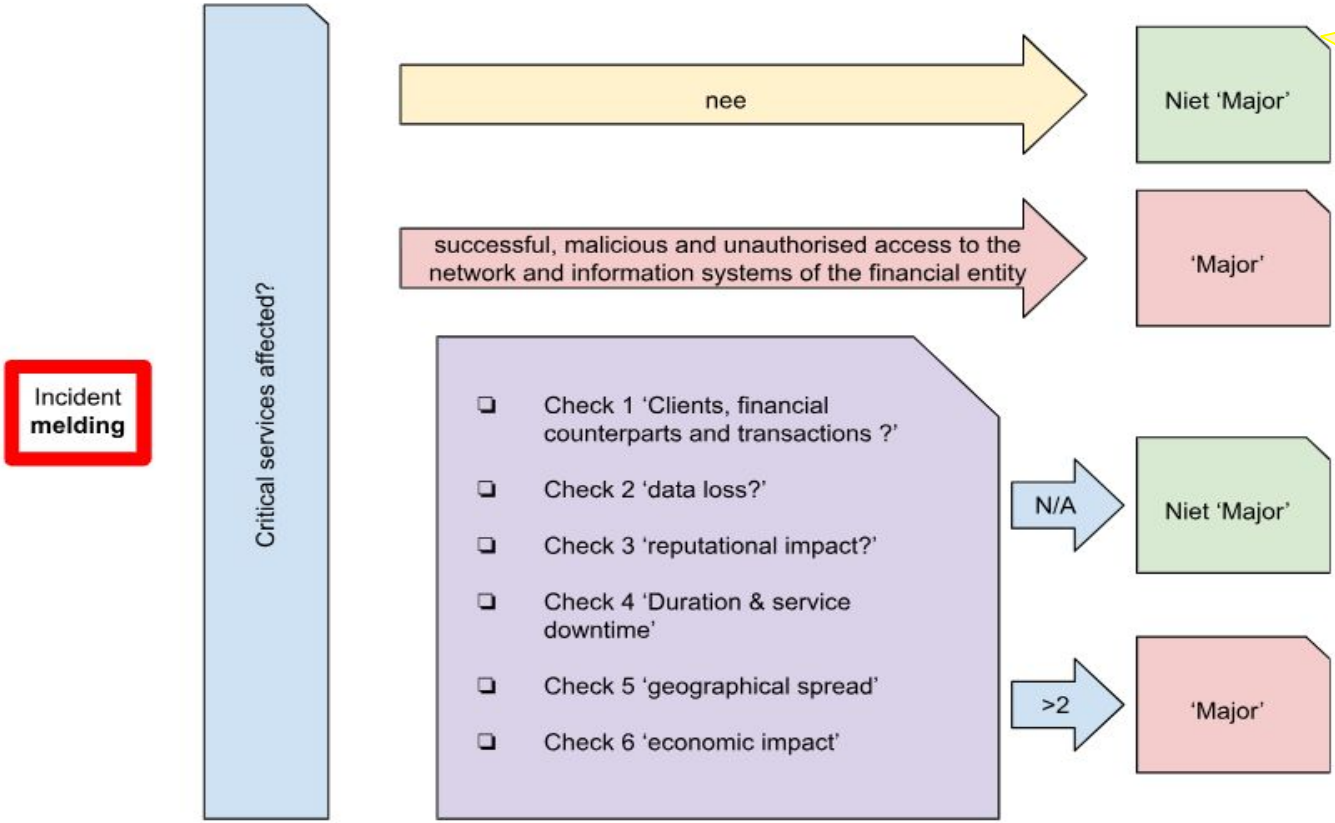
VISMA | idella

Major Incident(en)

RTS JC 70
(Draft)



Classificatie (major) incident



RTS JC 83
(figuur 1
blz.8)

VISMA | idella

Voorbeelden

Final Questions

Do you agree to and will act in full compliance with the **Visma's Code of Conduct**

- ☐ Yes
- ☐ No

Is the company currently involved in any disputes, investigations or lawsuits which might affect the deliveries to Visma?

- ☐ Yes
- ☐ No

Do (and have) you comply(ied) with applicable laws and regulations?[3]

- ☐ Yes
- ☐ No

Has the company appointed a Data Protection Responsible? Is yes provide details

- ☐ Yes
- ☐ No

Does the company have a process for detecting and communicating data breaches within the organization?

Vendor risk assessment 2023/4 (oud)

Vendor vragenlijst 2023/4 (oud)

bate	: 30.01.2024
ient / Vendor	: /
	: Lilian Rolefes
Da tion Manager	: Corinna Angel
Sub	: Annual review

To ...pleted by Visma idella	
ion	: High
d by DPM	: Yes
oved by SM	: Yes
pproved by Security Board (if High)	:
Checked certificates:	ISO27001* / ISAE3000 / ISAE3402
For 2023 this is still on name Visma ITC AS. as of 2024 this will be changed to SwInt	

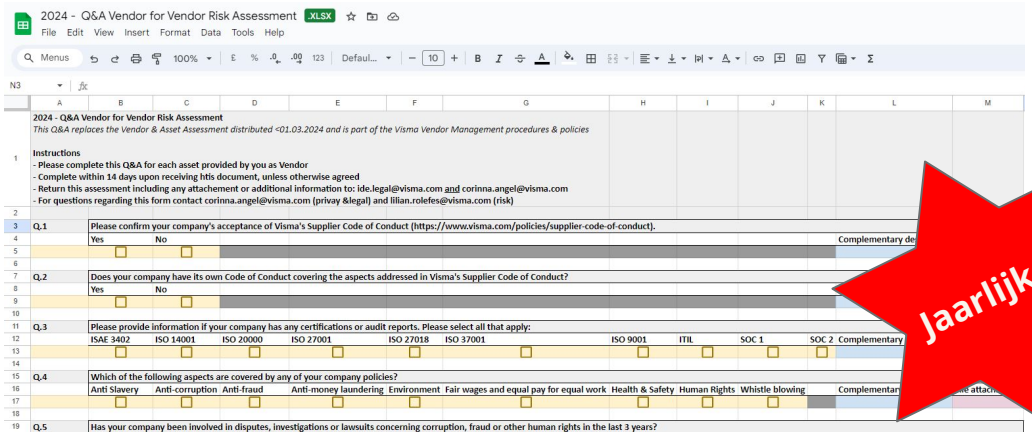
Deepdive planned to obtain more elaborate information. Contract update in order.
https://docs.google.com/document/d/1HmPCfnsWpuyZzFN4Ze0TmwI8fc59s9yqDjpDZZqX_vw/edit#heading=h.gidgxs

General information/ summary

Visma IT &C BV	Visma IT&C BV

VISMA | idella

Voorbeelden


2024 - Q&A Vendor for Vendor Risk Assessment .XLSX

File Edit View Insert Format Data Tools Help

2024 - Q&A Vendor for Vendor Risk Assessment

This Q&A replaces the Vendor & Asset Assessment distributed <01.03.2024 and is part of the Visma Vendor Management procedures & policies

Instructions
- Please complete this Q&A for each asset provided by you as Vendor
- Complete within 14 days upon receiving htis document, unless otherwise agreed
- Return this assessment including any attachement or additional information to: ide.legal@visma.com and corinna.angel@visma.com
- For questions regarding this form contact corinna.angel@visma.com (privay &legal) and lilian.rolefes@visma.com (risk)

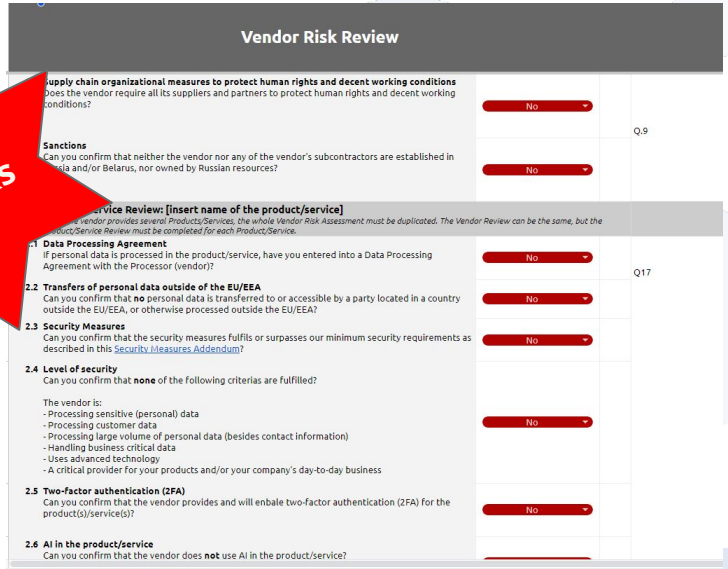
Q.1	Please confirm your company's acceptance of Visma's Supplier Code of Conduct (https://www.visma.com/policies/supplier-code-of-conduct).												
	Yes	No										Complementary de	
	☐	☐											
Q.2	Does your company have its own Code of Conduct covering the aspects addressed in Visma's Supplier Code of Conduct?												
	Yes	No											
	☐	☐											
Q.3	Please provide information if your company has any certifications or audit reports. Please select all that apply:												
	ISAE 3402	ISO 14001	ISO 20000	ISO 27001	ISO 27018	ISO 37001		ISO 9001	ITIL	SOC 1	SOC 2	Complementary	
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐		
Q.4	Which of the following aspects are covered by any of your company policies?												
	Anti Slavery	Anti-corruption	Anti-fraud	Anti-money laundering	Environment	Fair wages and equal pay for equal work		Health & Safety	Human Rights	Whistle blowing		Complementar	
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐		
Q.5	Has your company been involved in disputes, investigations or lawsuits concerning corruption, fraud or other human rights in the last 3 years?												

Vendor vragenlijst 2024/5

Jaarlijks

Vendor risk assessment 2024/5

Actie


Vendor Risk Review

Supply chain organizational measures to protect human rights and decent working conditions
Does the vendor require all its suppliers and partners to protect human rights and decent working conditions? — No

Sanctions
Can you confirm that neither the vendor nor any of the vendor's subcontractors are established in Russia and/or Belarus, nor owned by Russian resources? — No

Q.9

Service Review: [insert name of the product/service]
If the vendor provides several Products/Services, the whole Vendor Risk Assessment must be duplicated. The Vendor Review can be the same, but the Product/Service Review must be completed for each Product/Service.

2.1 Data Processing Agreement
If personal data is processed in the product/service, have you entered into a Data Processing Agreement with the Processor (vendor)? — No

Q17

2.2 Transfers of personal data outside of the EU/EEA
Can you confirm that **no** personal data is transferred to or accessible by a party located in a country outside the EU/EEA, or otherwise processed outside the EU/EEA? — No

2.3 Security Measures
Can you confirm that the security measures fulfils or surpasses our minimum security requirements as described in this Security Measures Addendum? — No

2.4 Level of security
Can you confirm that **none** of the following criterias are fulfilled?

The vendor is:
- Processing sensitive (personal) data
- Processing customer data
- Processing large volume of personal data (besides contact information)
- Handling business critical data
- Uses advanced technology
- A critical provider for your products and/or your company's day-to-day business

— No

2.5 Two-factor authentication (2FA)
Can you confirm that the vendor provides and will enbale two-factor authentication (2FA) for the product(s)/service(s)? — No

2.6 AI in the product/service
Can you confirm that the vendor does **not** use AI in the product/service?

Overview | Vendor Risk Review | Action Items


2.6 Use of AI in the product/service

If the vendor uses AI in the product/service you should:
1) Review the vendor contract in accordance with the guidelines set out in Navigating AI in Contracts.
2) Use the AI assessment to identify and mitigate any risk related to the use of AI, or use your own company specific risk assessment framework instead if that has been created for your company.

Navigating AI in Contracts

(Mini) AI Legal Assessment

☐

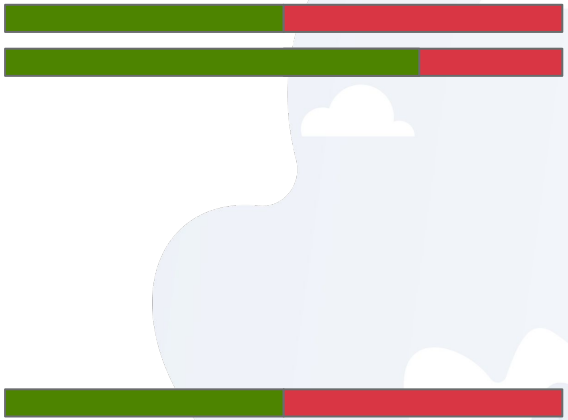
VISMA | idella

DORA: waar zijn we nu mee bezig?

- Contracten (klant)
  - Focus-gebieden
    - Bestaande klantcontracten (add.)
    - Nieuwe klantcontracten

- Contracten (leverancier)
  - Focus- gebieden
    - Audit & exitstrategie & risico

Status: maart 2024



*afhankelijkheid RTS *JS 2023 67*

VISMA | idella

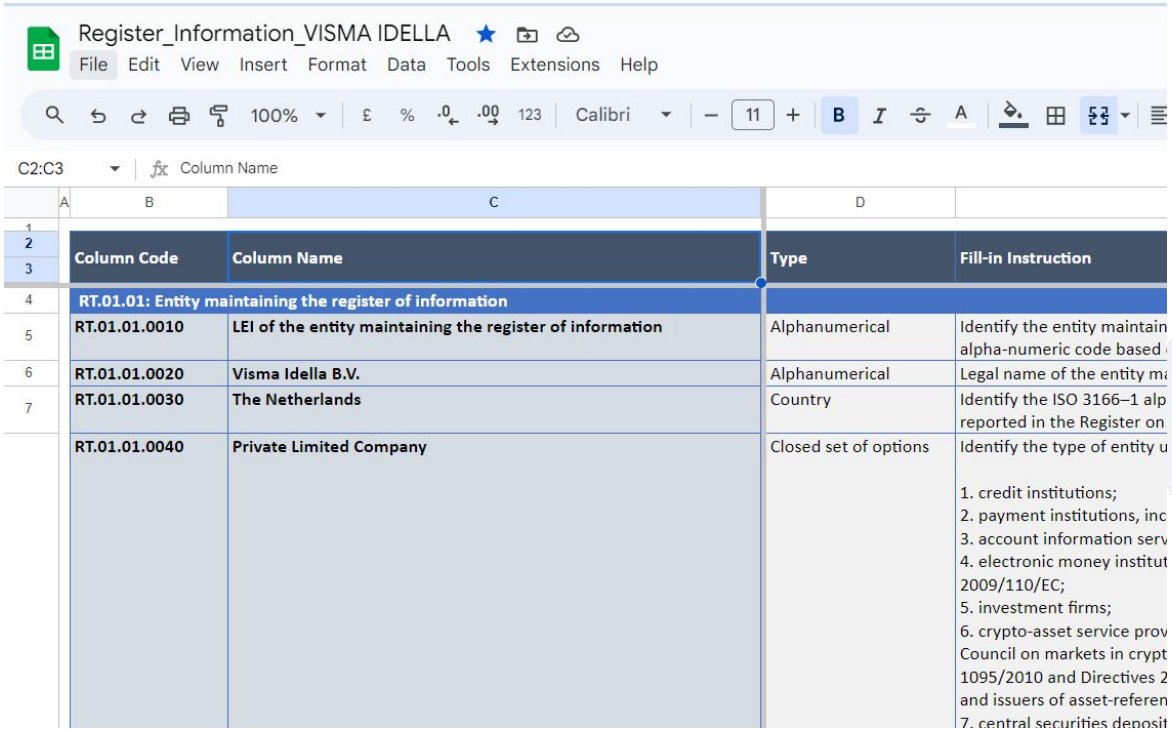
DORA: waar zijn we nu mee bezig?

DORA-clausules

Het Verbond van Verzekeraars werkt samen met Dufas en de Pensioenfederatie aan DORA-clausules, zodat contracten met leveranciers DORA-compliant kunnen worden. Deze clausules worden door een extern advocatenkantoor opgesteld en zijn naar verwachting aan het einde van het eerste kwartaal beschikbaar voor de leden van het Verbond.

Bron Verbond van Verzekeraars, 7 maart 2024

DORA: Risico en rapportage



Register_Information_VISMA IDELLA

File Edit View Insert Format Data Tools Extensions Help

C2:C3 | Column Name

Column Code	Column Name	Type	Fill-in Instruction
RT.01.01: Entity maintaining the register of information			
RT.01.01.0010	LEI of the entity maintaining the register of information	Alphanumerical	Identify the entity maintain alpha-numeric code based
RT.01.01.0020	Visma Idella B.V.	Alphanumerical	Legal name of the entity ma
RT.01.01.0030	The Netherlands	Country	Identify the ISO 3166–1 alp reported in the Register on
RT.01.01.0040	Private Limited Company	Closed set of options	Identify the type of entity u 1. credit institutions; 2. payment institutions, inc 3. account information serv 4. electronic money institut 2009/110/EC; 5. investment firms; 6. crypto-asset service prov Council on markets in crypt 1095/2010 and Directives 2 and issuers of asset-referen 7. central securities deposit

VISMA | idella

Rapportages VPaaS

VPaaS (nu)

	Per kwartaal	Per maand	Per jaar
SLA-Rapportage (Kwantitatief en kwalitatief) - Incl. incidentrapportage		X*	
ISAE 3000 Software Maintenance & maintenance VIPS			X
Privacy incident report/verslag	*Ad hoc*		
Optioneel			
DNB Security Self Assessment (Cobit 58)			X
Security- en Compliance Rapportage	X		

*** frequentie van de SLR kan per klant verschillend zijn, maar de 'standaard' mbt de nieuwe contracten is maandelijks.**

VPaaS (verwacht)

Aanvullend DORA

- **Update** incidentrapportages
- **Nieuw** Informatieregister
  - art. 28 DORA

Rapportages DPaaS

DPaaS (nu)

	Per kwartaal	Per maand	Per jaar
1e lijns Service desk (incl. klantcontactrapportage)		X	
Incidentenrapportage		X	
Privacy incident report/verslag	*Ad hoc*		
Klachtenrapportage		X	
Financiële rapportage		X	
SLA-Rapportage (Kwantitatief en kwalitatief)	X		
Niet Financiële Risico rapportage (NFR)	X		
Security- en Compliance Rapportage	X		
ISAE 3000 Software Maintenance & maintenance VIPS			X
ISAE 3402 Disbursements			X
ISAE 3402 Pensioenadministratie			X
Optioneel			
DNB Security Self Assessement			X

DPaaS (verwacht)

Aanvullend DORA

- **Update** NFR
- **Update** incidentrapportages
- **Nieuw** informatieregister
  - art. 28 DORA

VISMA | idella

DORA: Volgende stappen

Datum	Referentie	Titel
17/07/2024	**JC 2023 67**	**Consultation Paper on draft RTS subcontracting**
17/07/2024	JC 2023 68	Consultation Paper on draft GL on costs and losses
17/07/2024	JC 2023 69	Consultation Paper on draft RTS on oversight harmonisation
17/07/2024	**JC 2023 70**	**Consultation Paper on draft RTS and ITS on major incident reporting under DORA**
17/07/2024	JC 2023 71	Consultation Paper on draft Guidelines on oversight cooperation
17/07/2024	**JC 2023 72**	**Consultation Paper on draft RTS on TLPT**
17/07/2024	DORA CP	DORA public consultation on the second batch of policy products - overview document

Bron: esma.europa.com (*laatst bezocht 04.03.2024*)

DORA: Volgende stappen

Planning (onder voorbehoud)

Voorjaar:
- Kennissessie 2 (mei/juni*)
- Mapping DNB GP Informatiebeveiliging ‘23
- DNB Security Self Assessment
- ISO27001 (re-audit)

Zomer:
- Kennissessie 3 (augustus/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)

*digitaal

Najaar:
- Kennissessie 4 (oktober/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)

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

Afsluiting

VISMA | idella

Entrepreneurial

Responsible

Dedicated

Inclusive

Make progress happen

VISMA | idella

Vragen van klanten

Hoe borgt VISMA Idella dat haar onderaannemers ook voldoen aan de te stellen eisen?

Welke Assurance rapportages gaan wij krijgen specifiek voor DORA?

Hoe gaan jullie je klanten meenemen in jullie vorderingen qua implementatie van de DORA wetgeving?

Gaat Visma Idella kosten doorbelasten en zo ja op welke wijze?

DORA - waar staan we nu?

Artikel 30 DORA

- *Testen*: art. 24 lid 1 DORA
  - MAVA/Pentesten (VASP)
- *Incidenten*: artt. 17, 18, 19, 30(2)(I), 11(2), 12(7)
  - Update Richtlijn Meldplicht datalekken

JC 2023 83
Classificatie van ‘major incidents’ & significante ‘cyber threat’

JC 2023 83

Scope: **artikel 18 DORA**
- Classificatie art. 18 lid 1
  - hoeveelheid en relevantie, duur, spreiding, dataverlies, kriticiteit, economische impact;

Rapportage*termijnen* + inhoud voor grote incidenten
⇒ artikel 20a van DORA (2e Batch)

Proces voor melden van grote incidenten
⇒ artikel 19 van DORA.

Sidenote:
- Operationele incidenten vallen ook onder de reikwijdte van ICT-gerelateerde incidenten.
- Artikelen 18 en 19 van DORA hebben ook betrekking op de rapportage van operationele of veiligheidsbetalingsgerelateerde incidenten.

- Incident classificatieproces
  - Aanwezig.
  - Update gepland voor eind Q2, ‘24
- ICT-related incident management *proces* voor detectie, beheer en melden van ICT-gerelateerde incidenten
  - Aanwezig.
  - Eerste update gepland voor eind Q2, ‘24
  - Tweede update gepland voor eind Q4, ‘24

Contract:

-

Major incident reporting (juli ‘24, JC 2027 70)

JC 2023 84
ICT services die kritieke of belangrijke functies ondersteunen

JC 2023 84

Scope: **artikel 28 DORA**

- Strategie omtrent ICT-derdenrisico incl. beleid inzake het gebruik van ICT-diensten ter ondersteuning van kritieke of belangrijke functies geleverd door externe ICT-dienstverleners.

- Strategie ICT derde-risico
  - Aanwezig.
  - Update gepland voor eind Q2, ‘24
- Beleid gebruik ICT diensten
  - Aanwezig.
  - Eerste update gepland voor eind Q2, ‘24

ISO27001

JC 2023 85
ICT Informatieregister

JC 2023 85

Scope: **artikel 28 DORA**

-

JC 2023 86
ICT risicomanagement raamwerk

JC 2023 86

Scope: **artikel 15 en 16 DORA**

-

Rapportages

- Rapportage (mapping)
  - DPaaS
  - VPaaS