CERRIX

GDPR en GRC technology

Hoe GRC-tech uw GDPR compliance kan ondersteunen

Zwolle, 25-09-2019

Wie ben ik?

- **Functie:** Manager Operations, CERRIX.
- **Verantwoordelijkheden:** Managen van CERRIX implementatietrajecten met mijn team van mensen.
- **Werkervaring:** 15 jaar ervaring met Procesmanagement, Riskmanagement, GRC-tooling, IT(audit) en een beetje GDPR.
- **Sectoren:**
  - Pensioenfondsen & Pensioenuitvoerders: PGGM, Ahold PF, ABN AMRO PF, STAP APF, AZL.
  - Verzekeraars: ASR, ZLM, ARAG, Interpolis.
  - Banken: Rabobank, NIBC, Kas Bank, CEB.
  - Onderwijs: OU, MBO-Raad, Universiteit Leiden
- **Hobby's:** BBQ, Wijn, Reizen.

Agenda

- Introductie
- Op welke gebieden van de GDPR kan GRC-tech uitkomst bieden:
  - ✓ GDPR communicatie en privacy awareness
  - ✓ Processen, asstes en data flows inzichtelijk maken
  - ✓ Privacy risico’s identificeren (DPIA) en registeren
  - ✓ Werking van beheersmaatregelen testen
  - ✓ Verbeteracties uitzetten
  - ✓ Datalekken registratie en opvolging
  - ✓ Dataregister
  - ✓ Third Party Riskmanagement
- Ronde tafel discussie

Introductie

- De GDPR heeft impact op de bedrijfsvoering van een onderneming en hoe we omgaan met persoonsgegevens.
- Impact van GDPR is vaak wijd verspreid binnen en buiten (sub-verwerkers) uw organisatie, denk aan:
  - Impact op de bedrijfscultuur (awareness van betrokkenen)
  - Impact op de wijze van uitvoeren van processen die persoonsgegevens verwerken en de beheersing van deze processen (dataminimalisatie)
  - Impact op de collectie, omgang en verstrekking van persoonsgevoelige informatie (privacy by default, rechten van betrokkenen)
  - Impact op de wijze van registreren, bewaren en beveiligen van persoonsgevoelige informatie (dataminimalisatie, bewaartermijnen, need to know, need to see, privacy by design)
  - Impact op third party management (verwerkersovereenkomsten en de monitoring van de afgesproken beheersing t.a.v. GDPR)

- De wijde verspreiding en complexiteit van de GDPR vraagt om oplossingen waarmee privacy risico's en gerelateerde beheersmaatregelen centraal gemonitord kan worden. GRC-tech kan daarbij helpen!

Introductie

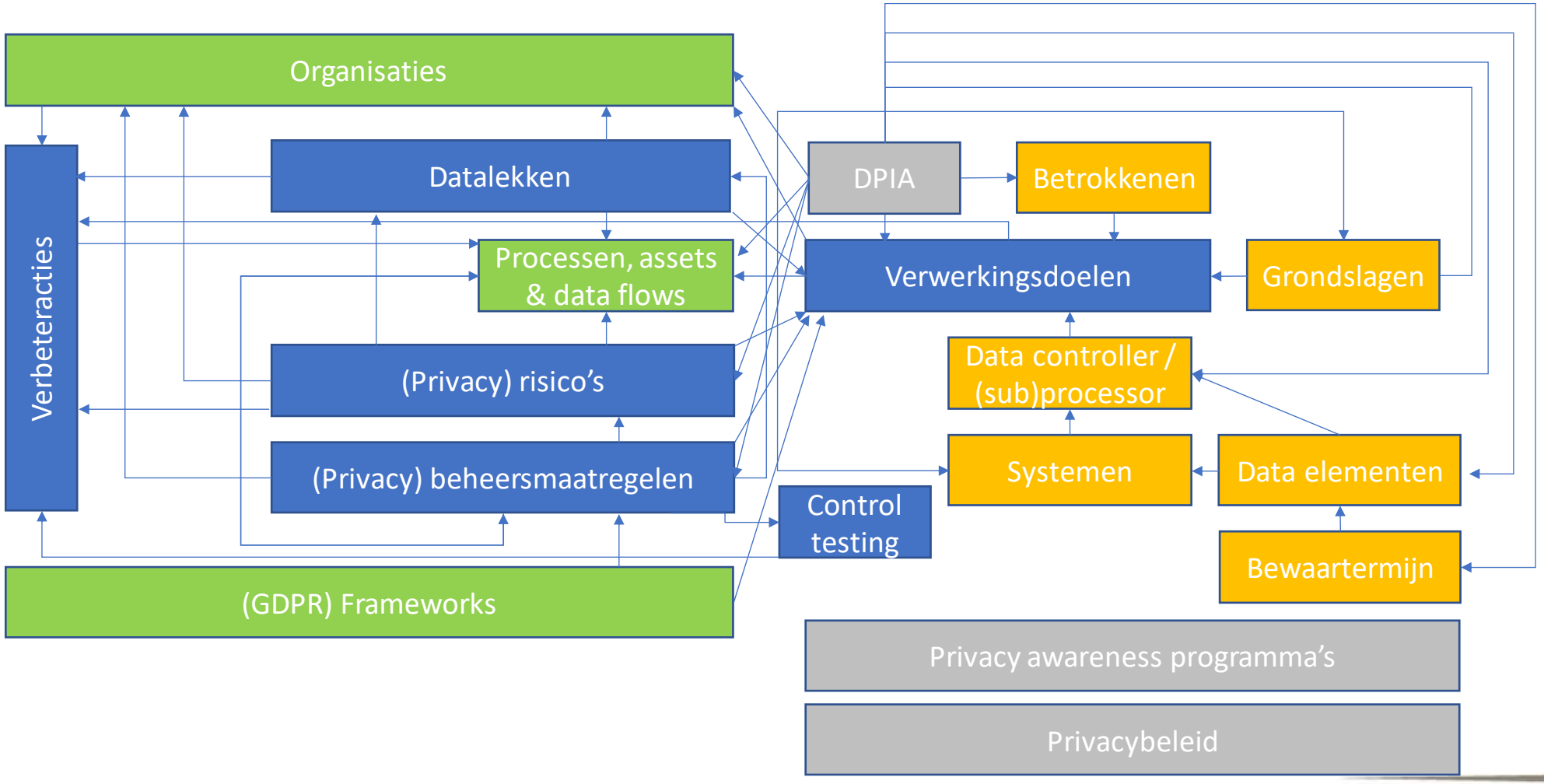
Waar zou GRC-tech kunnen helpen?

- ✓ Communiceren over privacy-beleid en privacy awareness.
- ✓ Persoonsgegevens verwerkende processen, assets en data flows identificeren (DPIA).
- ✓ Processen, assets en data flows inzichtelijk maken.
- ✓ Privacy risico's en beheersmaatregelen (m.b.v. Privacy Control Framework (NOREA) identificeren (DPIA) en registreren.
- ✓ Werking van de beheersing omtrent GDPR testen en monitoren.
- ✓ Verbeteracties uitzetten en opvolgen.
- ✓ Datalekken registratie en opvolging.
- ✓ Dataregister opzetten en onderhouden.
- ✓ Third-party risk management uitvoeren en monitoren.

Dit om uiteindelijk een overall beeld te krijgen over de status van GDPR compliance in uw organisatie.

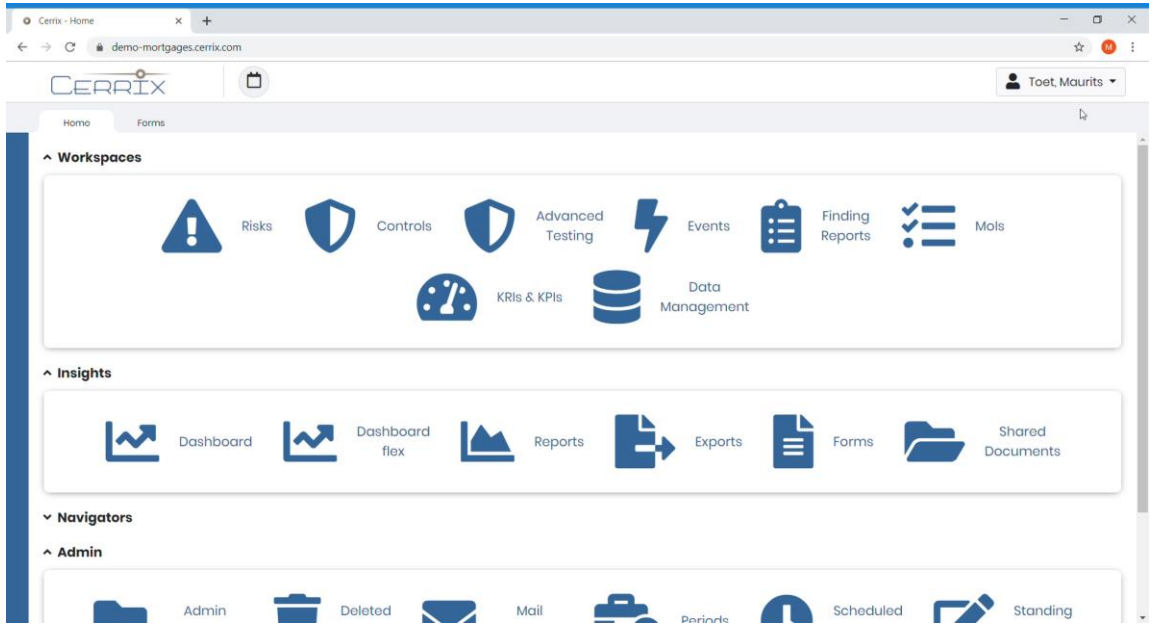
Introductie

GDPR zoals wij dat bij CERRIX zien in een relationeel model:

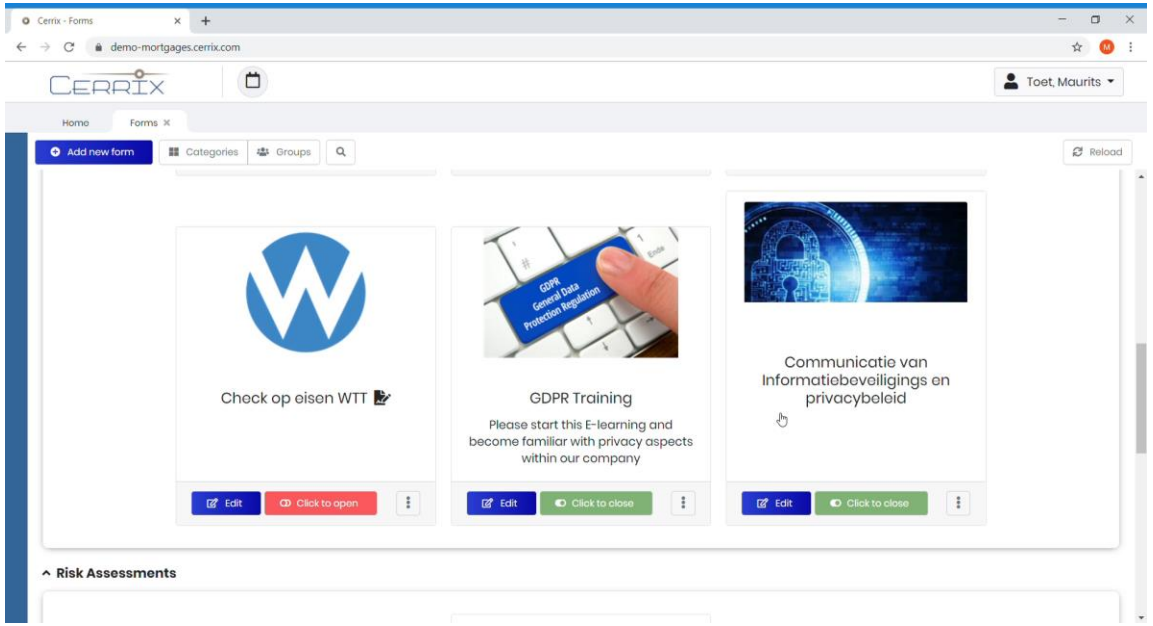


Communiceren over privacy beleid en privacy awareness

Beleid communiceren



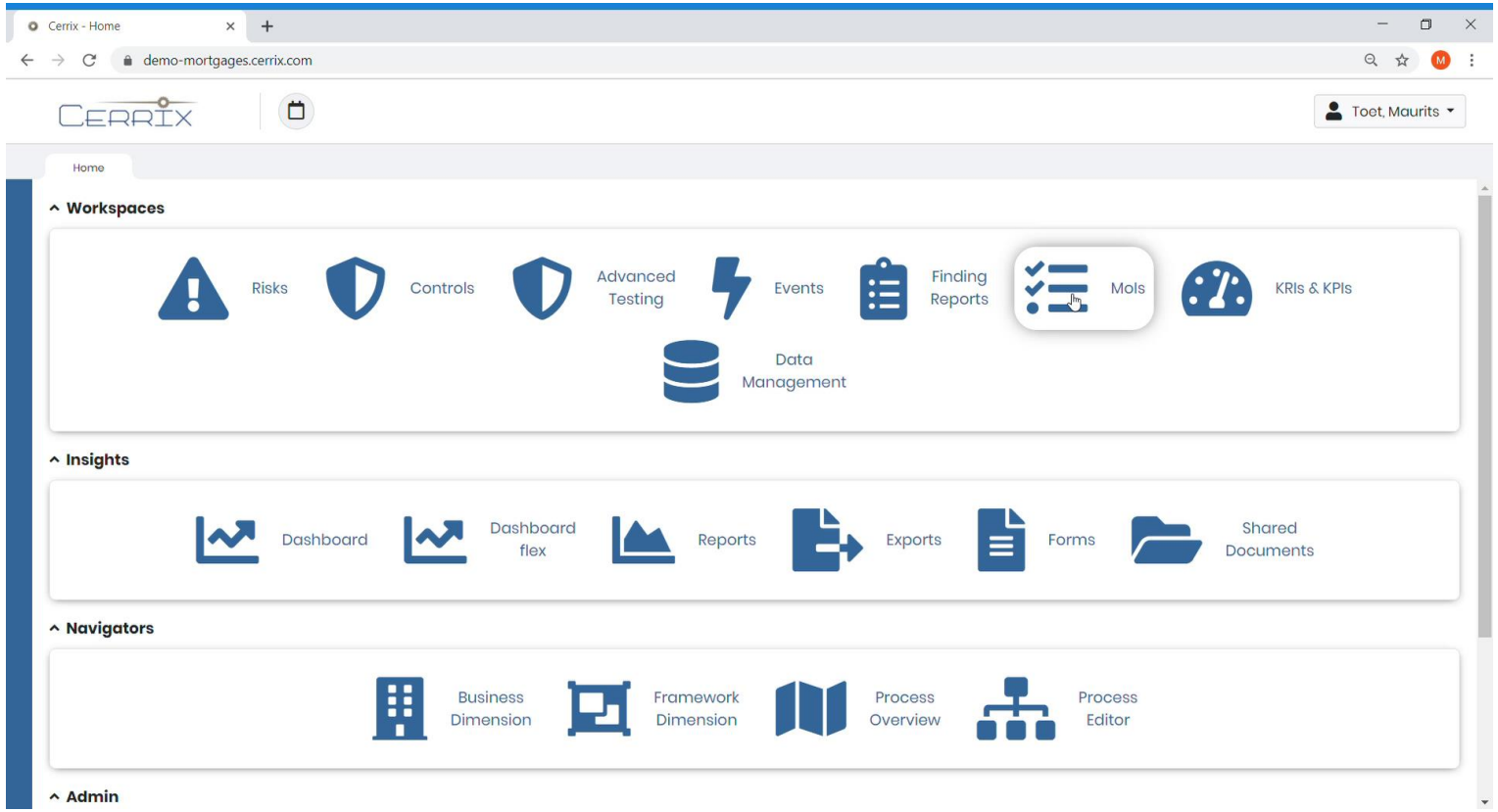
GDPR awareness training



Vraag aan de deelnemers

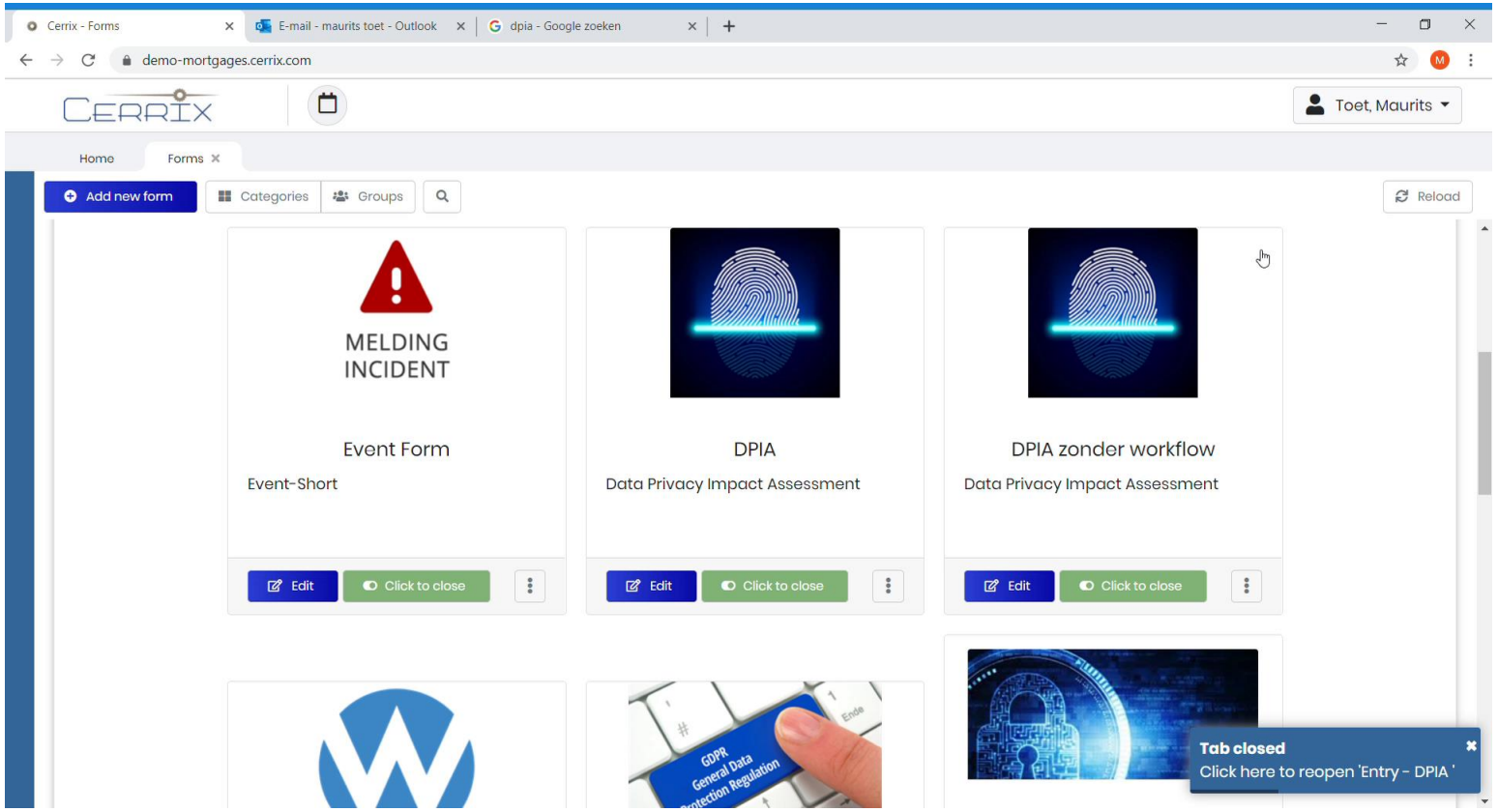
Welke toepassingen ten aanzien van communicatie over GDPR zouden nog meer relevant zijn en binnen een GRC-systeem passen?

Processen, assets en data-flows inzichtelijk maken



Vraag aan de deelnemers:
Dienen verwerkende processen, gerelateerde data flows en assets inzichtelijk te zijn alvorens tot een DPIA kan worden overgegaan?

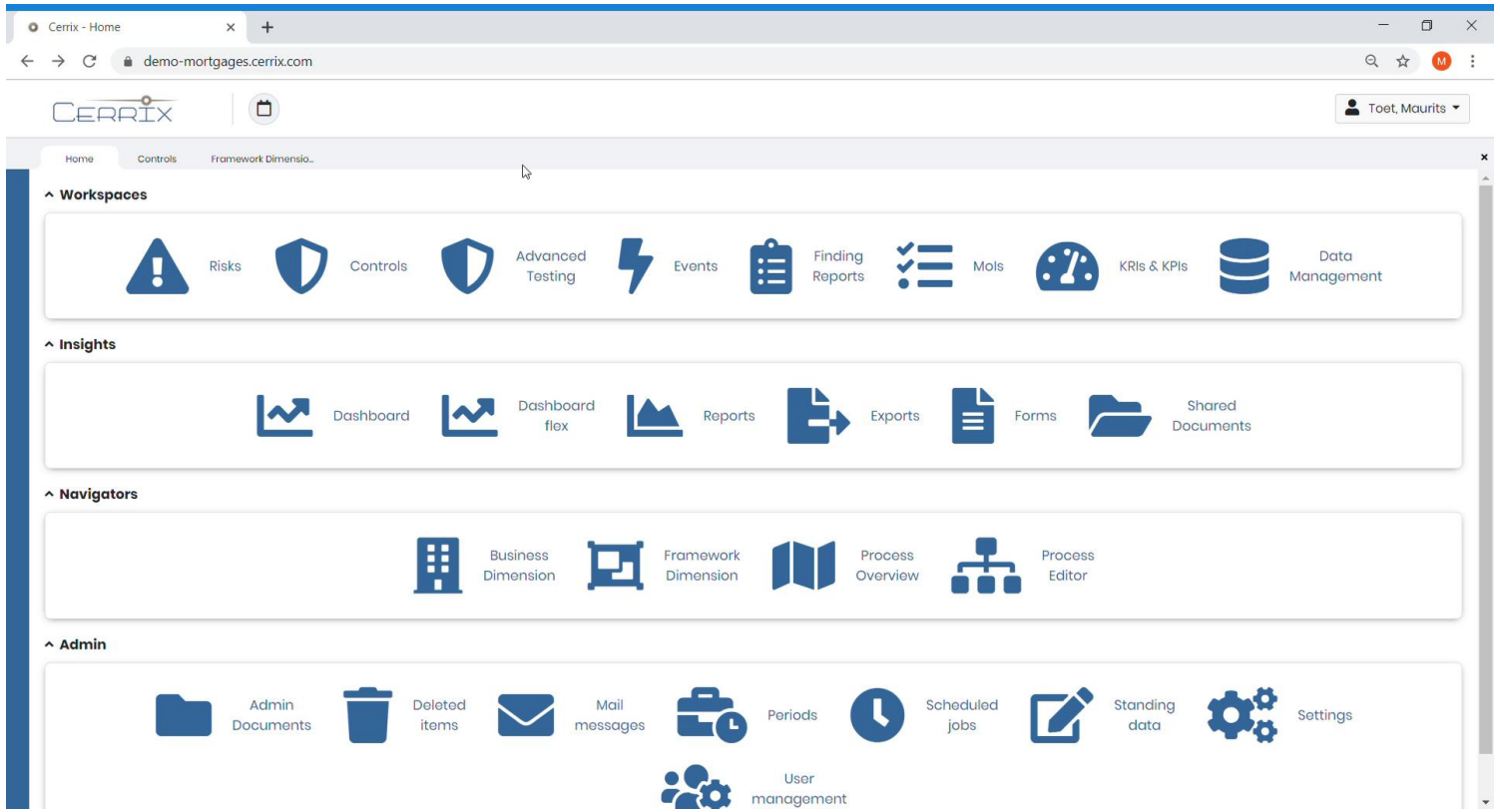
Privacy risico’s en beheersmaatregelen identificeren en registreren



Vraag aan de deelnemers

Aan welke dataelementen zouden we de DPIA willen linken in een GRC-systeem?

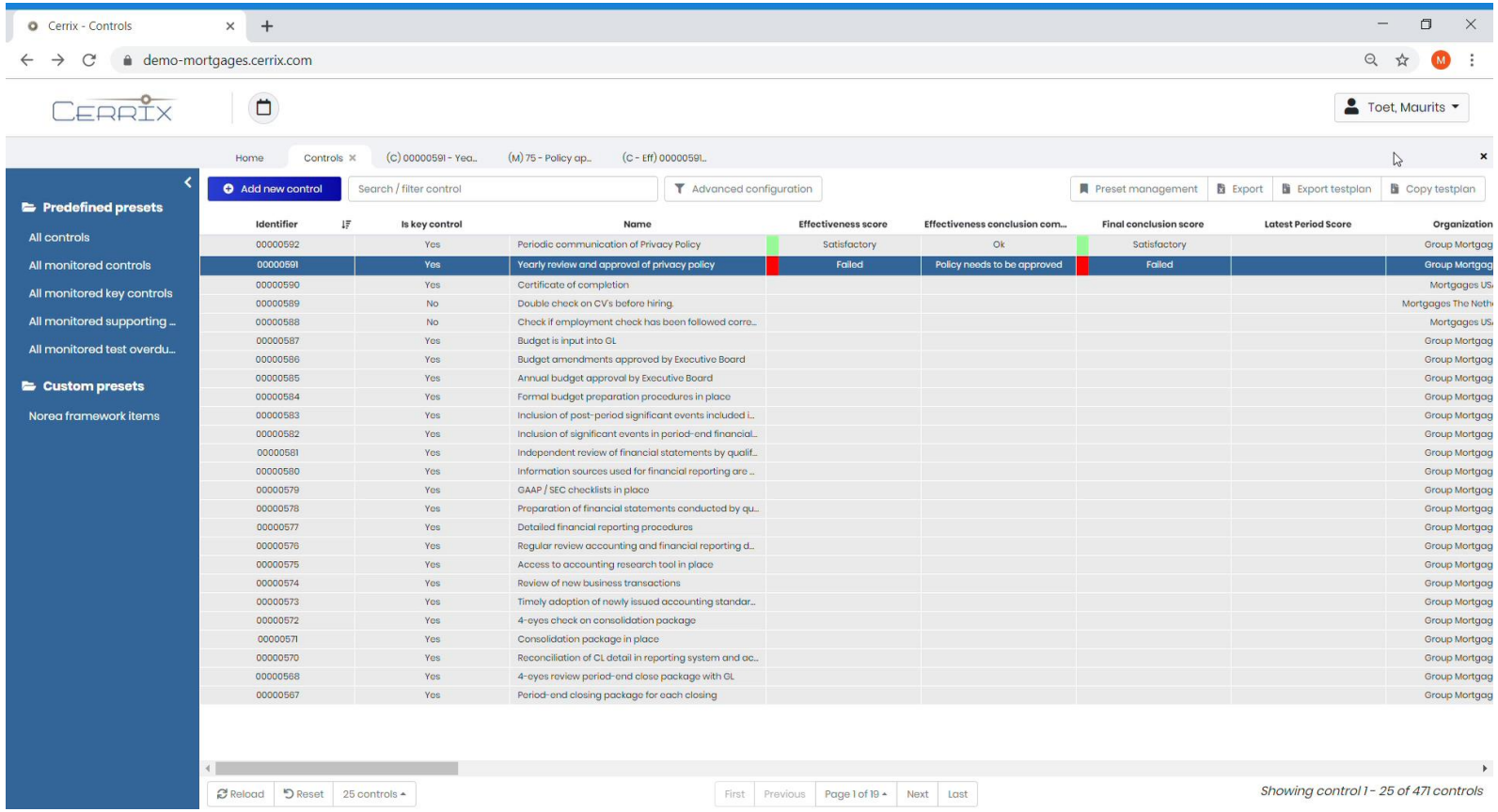
Werking van de beheersmaatregelen omtrent GDPR testen en monitoren



Vraag aan de deelnemers

1. Welke best-practices zouden jullie nog meer graag terugzien in een GRC-systeem?
2. Wordt er in jullie organisatie al actief getest op de werking van de privacy beheersmaatregelen volgens best-practices?

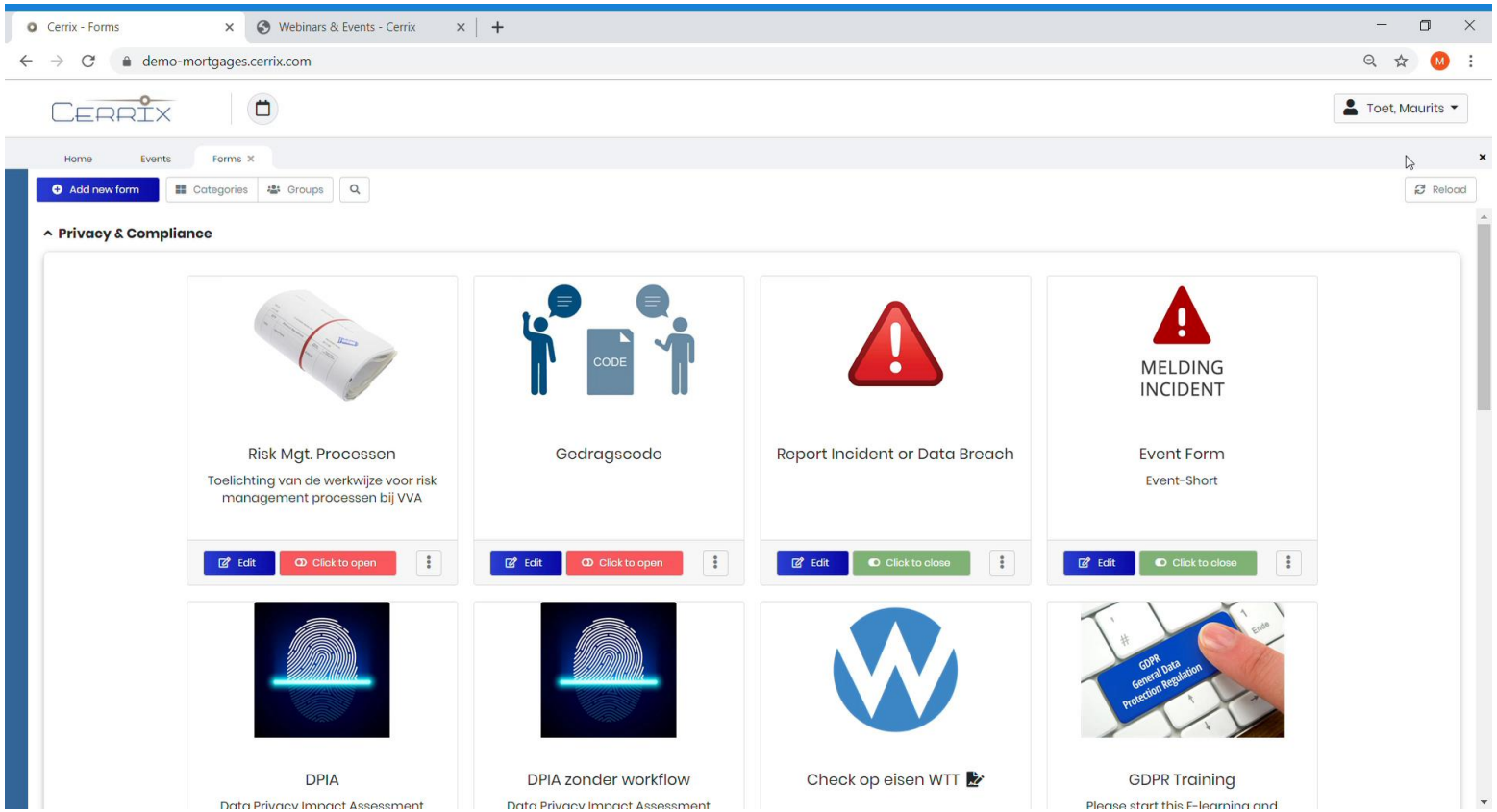
Verbeteracties uitzetten en opvolgen



Vragen aan de deelnemers

1. Wie in de zaal heeft GDPR compliance geïntegreerd als onderdeel van zijn/haar riskmanagement systeem?
2. Welke actiesoorten zouden in het kader van GDPR in een GRC-systeem handig zijn?

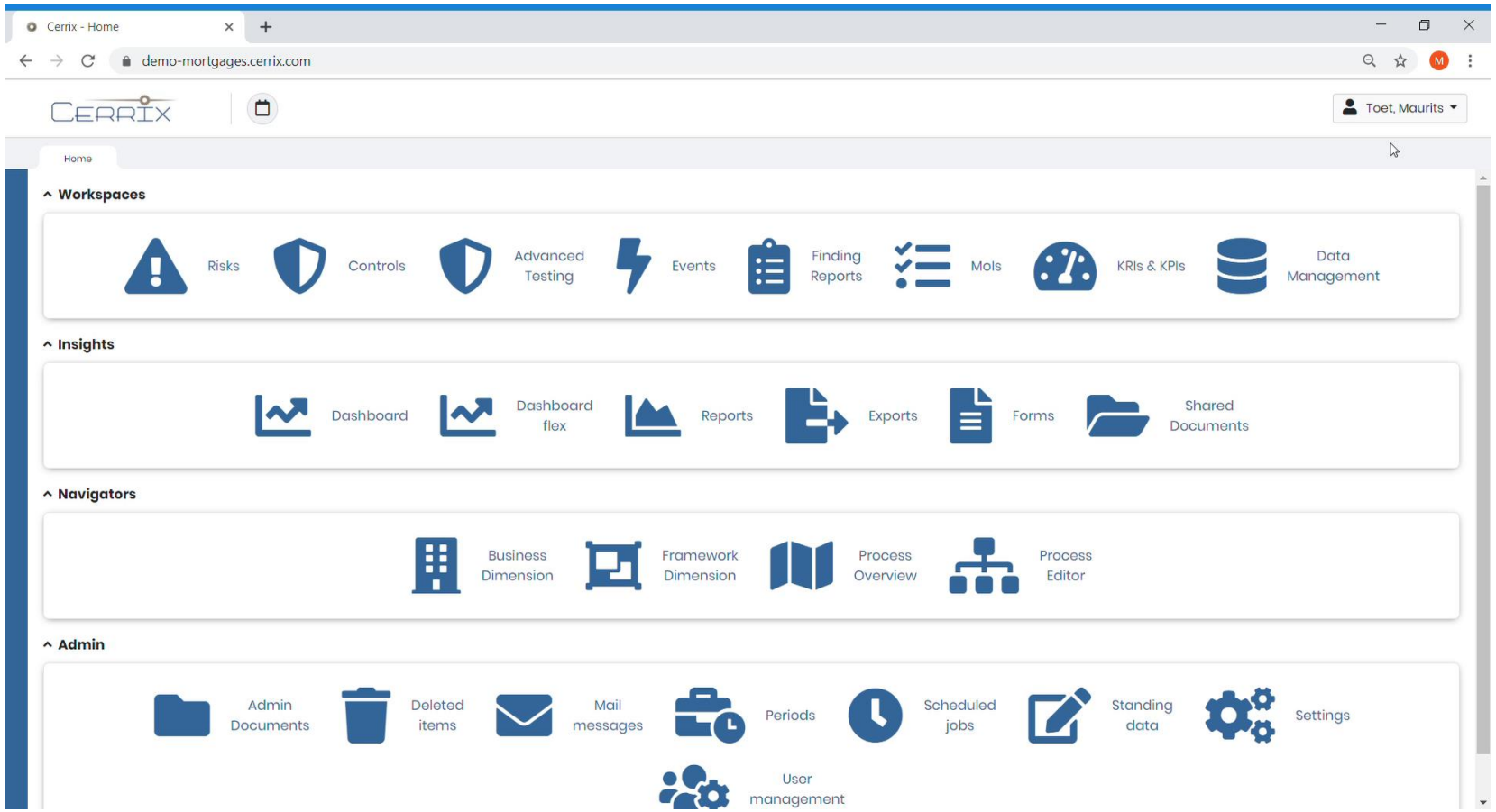
Datalekken registratie en opvolging.



Vragen aan de deelnemers

1. Moet het melden en opvolgen van incidenten/datalekken onderdeel uitmaken van een GRC-systeem?
2. In hoeverre worden datalekken meegenomen in jullie reguliere risicomanagement / auditproces?

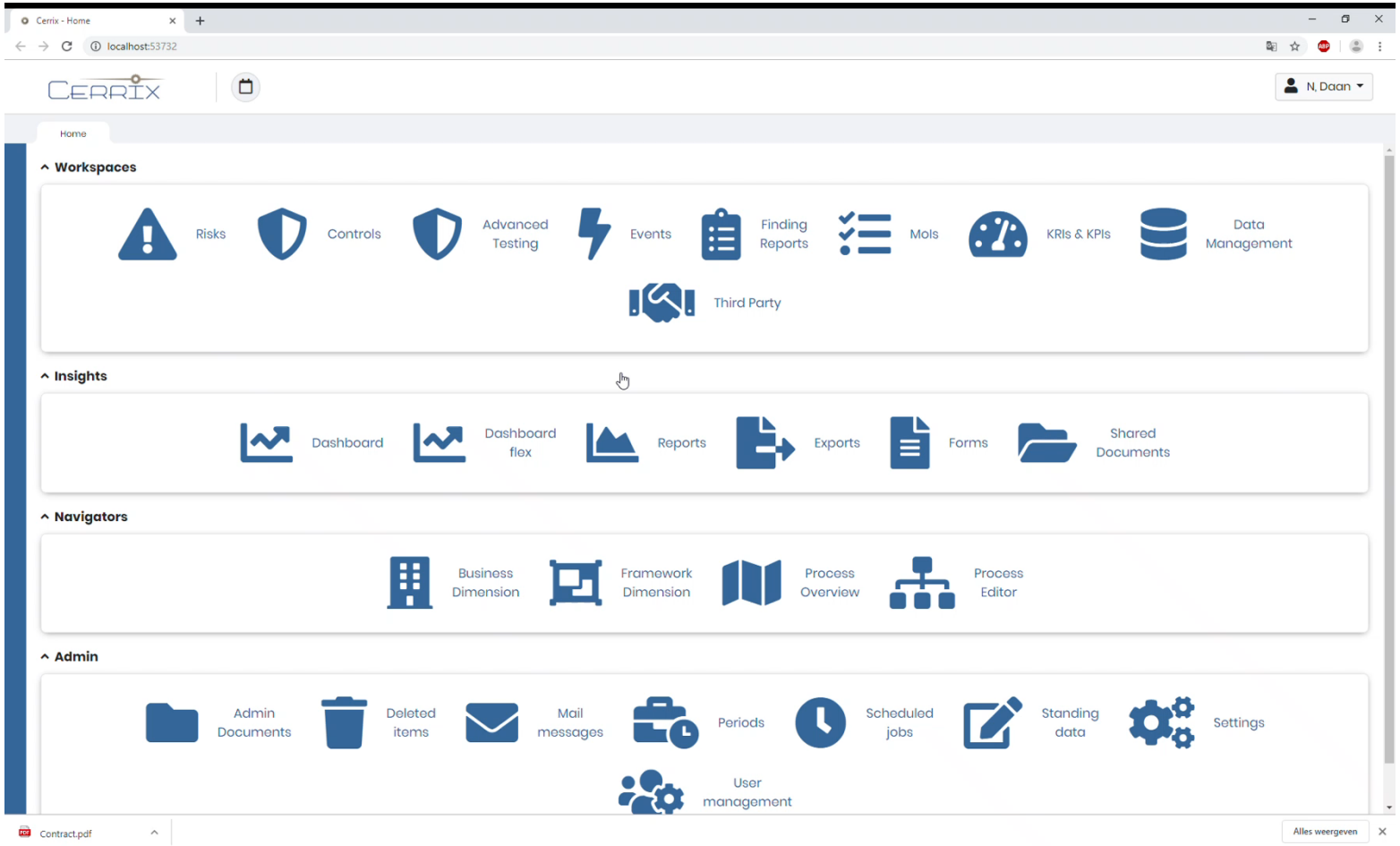
Dataregister opzetten en onderhouden



Vraag aan de deelnemers

1. Zou een GRC-systeem ook de geautomatiseerde periodieke update van het dataregister moeten faciliteren of dient dit in het werkproces geborgd te worden?

Third Party Riskmanagement



Vraag aan de deelnemers

1. Wat zijn jullie ervaringen met Third Party Riskmanagement en GRC systemen?

Ontwikkelingen op de GRC-tech horizon

- Centralisering van Risk, Compliance & Audit werkprocessen in 1 tool.
- Third-Party riskmanagement wordt steeds belangrijker en vraagt om specifieke monitoring opties.
- API’s tussen GRC-systeem en bronsystemen van de klant.
- Integratie van ketens met als doel continuous assurance.

Ronde tafel discussie

Stelling 1:

“GRC-tech kan veel ondersteuning bieden bij GDPR-compliance maar is nog niet voldoende doorontwikkeld.”

Ronde tafel discussie

Stelling 2:

“De mogelijkheden van GRC-tech in relatie tot GDPR worden op dit moment niet (voldoende) benut door het bedrijfsleven.”

Ronde tafel discussie

Stelling 3:

“Er is bij FG’ers en/of Data Privacy Officers te weinig kennis van de mogelijkheden van GRC-tech.”

Uitnodiging

Graag nodigen wij u uit voor het CERRIX event op donderdag 17 oktober 2019 in Hotel Restaurant Karel V te Utrecht.

Het thema is:
“Business in Control, hoe verbinden we alle betrokkenen?”

Inschrijven kan op www.CERRIX.com

Vragen?

Voor meer informatie:

Maurits.Toet@cerrix.com
06-55781325