

HANDREIKING BENCHMARK IBP

<i>Datum</i>	<i>Versie</i>	<i>Auteur</i>
27 november 2024	[1.0]	Evie-Janne van Noorel

Dit document dient als stappenplan voor het invullen van je actuele volwassenheidsniveau en het instellen van je benchmarkprofiel in je TrustBound-omgeving. Het begeleid je door het gehele proces, van de voorbereiding tot het indienen van je gegevens voor zowel de informatiebeveiliging- als de privacybenchmark.

Inhoudsopgave

1	Vorbereiding	3
2	Volwassenheidsniveau aangeven	5
3	Benchmark inleveren	7
3.1	Uitwerking voor benchmark Informatiebeveiliging	8
4	Gegevens controleren en insturen	10
5	Bevestiging ontvangen	11
6	Extra ondersteuning	12
7	Bij problemen en vragen	13

Benchmark in het mbo

Benchmarken is essentieel voor MBO-instellingen om hun cyberveiligheid effectief te meten en te verbeteren. Door de huidige beveiligingsmaatregelen te vergelijken met de sectorstandaarden, krijgen scholen inzicht in hun sterke en zwakke punten. Dit stelt hen in staat om gerichte verbeteringen door te voeren en zich beter voor te bereiden op de steeds complexer wordende digitale dreigingen. Het benchmarkproces biedt een helder overzicht van de huidige staat van cyberbeveiliging en helpt bij het prioriteren van noodzakelijke acties.

Het invullen van de benchmark levert waardevolle gegevens op die niet alleen de eigen beveiliging verbeteren, maar ook de collectieve cyberveiligheid binnen het MBO versterken. Door de benchmark in te vullen, kunnen instellingen hun processen optimaliseren, risico's verminderen en bijdragen aan een veiligere leeromgeving voor alle studenten en medewerkers. De deadline voor het inleveren van de benchmark 2025 is **vrijdag 31 januari 2025**.

Met de introductie van TrustBound GRC en de externe security audits komen we gaandeweg in een situatie waarbij de benchmark geen doel op zich meer is, maar veel meer een momentopname van de actuele volwassenheid op het gebied van IB en P. De instellingen hebben het assessment al eerder ingevuld, werken het regelmatig bij en bij een toenemend aantal instellingen is het ook al gevalideerd (en bijgesteld) bij een externe security audit. Het inleveren voor benchmark is in de ideale situatie niet meer dan een export van de actuele volwassenheid IB en P.

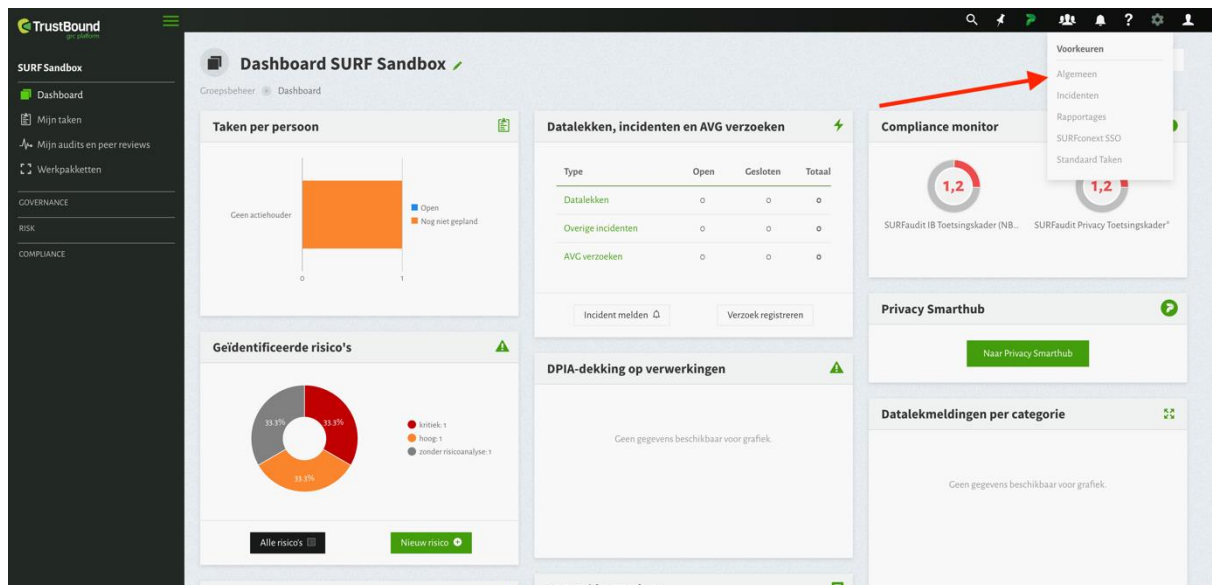
Deze handreiking is daarom opgedeeld in twee hoofdstukken:

1. Het invullen van de volwassenheidsscores voor de toetsingskaders IB en P
2. Het exporteren de volwassenheidsscores ten behoeve van de benchmark IBP

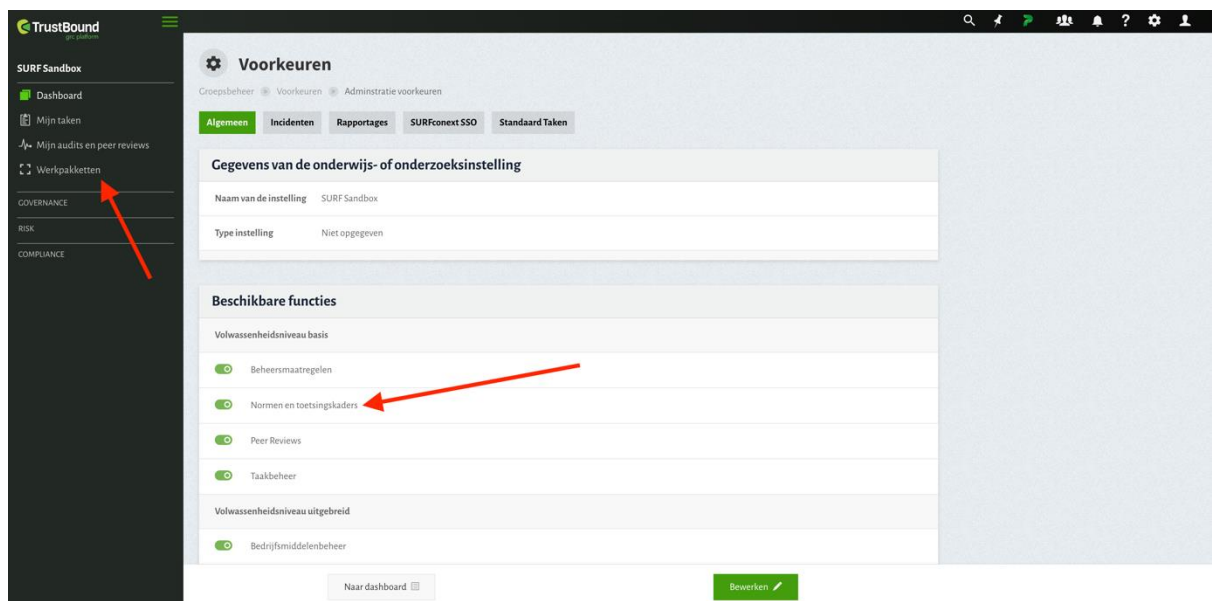
Aangezien TrustBound GRC in de meeste gevallen al volop in gebruik is voor het werken aan de volwassenheid IB en P zullen de stappen uit hoofdstuk 1 in de meeste gevallen overbodig zijn en kun je dat hoofdstuk overslaan.

1 Voorbereiding

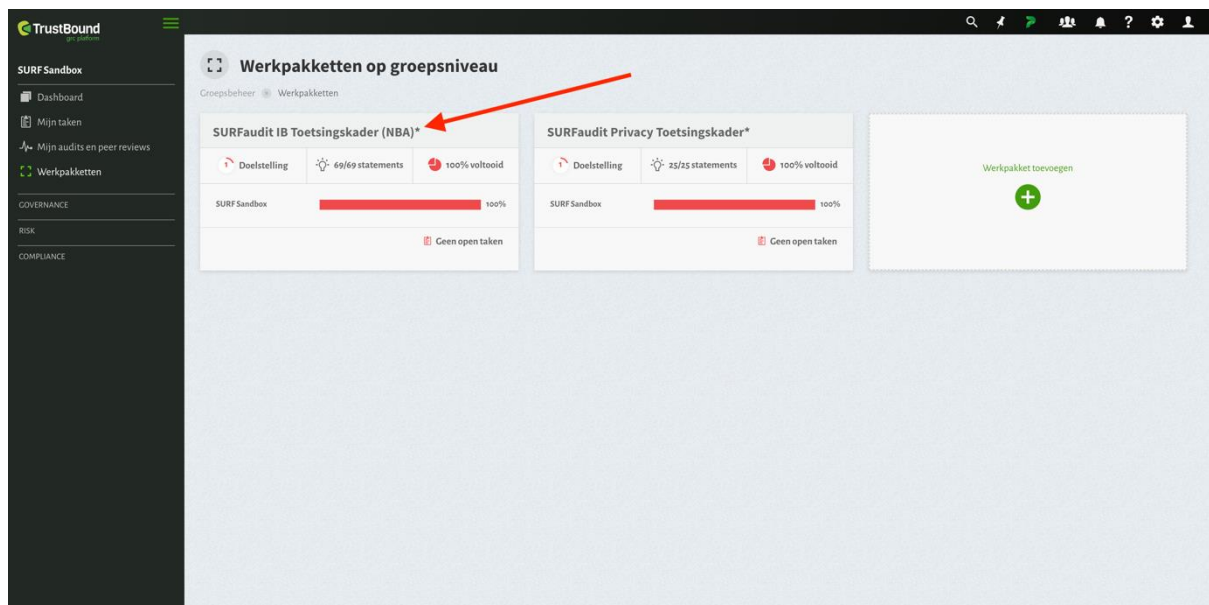
Ga eerst naar het dashboard van je live omgeving. Klik op *Algemeen* onder het wielte rechtsboven.



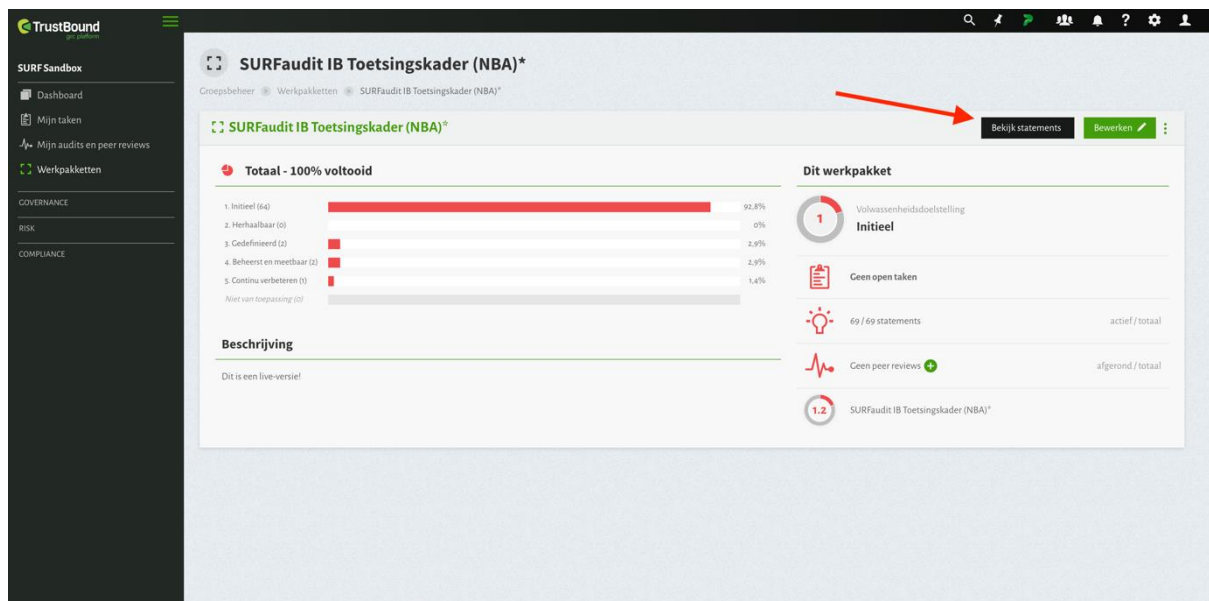
Zorg ervoor dat er een vinkje staat bij *Normen en toetsingskaders* als dat nog niet het geval is. Ga daarna naar *Werkpakketten*.



Je ziet daarna de informatiebeveiliging en privacy toetsingskaders staan.



Klik daarna op *Bekijk statements*.



2 Volwassenheidsniveau aangeven

Geef het huidige volwassenheidsniveau van je instelling aan voor elke statement/norm. Dit doe je door op het getal naast het statement te klikken, het huidige niveau aan te geven, een korte argumentatie toe te voegen met de onderbouwing van het niveau en vervolgens op toepassen te klikken. Voor statements die voor jou instelling niet van toepassing zijn, vul je *n/a* in. Doe dit voor alle statements.

The screenshot shows the TrustBound SURFaudit IB Toetsingskader (NBA)* interface. The left sidebar contains navigation options like 'Dashboard', 'Mijn taken', 'Mijn audits en peer reviews', 'Werkpakketten', 'GOVERNANCE', 'RISK', and 'COMPLIANCE'. The main area displays a list of statements with a maturity level indicator (a circle with numbers 1-5) and a 'Toepassen' button. Red arrows and numbers 1, 2, and 3 highlight the steps: 1. Click on the maturity level indicator, 2. Select the desired maturity level, and 3. Click the 'Toepassen' button.



Wees je ervan bewust dat het invullen van de volwassenheid op statementniveau voldoende is voor het invullen van de benchmark, maar niet voor de [security audit](#). Voor de security audit is het noodzakelijk om ook bewijsmateriaal toe te voegen, zoals documenten, rapportages en andere ondersteunende informatie. Dit vereist extra tijd en zorgvuldigheid, dus begin ruim van tevoren met het verzamelen en aanleveren van de benodigde gegevens. Door vroeg te starten, voorkom je vertragingen en zorg je ervoor dat het proces soepel verloopt.

Voor de audit is het ook belangrijk de door jou behaalde score te onderbouwen door het schrijven van een korte argumentatie op statement niveau, zoals hierboven beschreven. Ons advies is om ook al de onderliggende beheersmaatregelen te openen, te activeren en daar een toelichting op de beheersmaatregel te schrijven. Dus bijvoorbeeld niveau 2 openen en toelichten waarom je vindt dat je dat niveau hebt gehaald. Daar kun je ook bewijsmateriaal toevoegen!

Soms heb je ook delen van een volgend volwassenheidsniveau al ingericht, bijvoorbeeld niveau 3. Open dan ook die beheersmaatregel, activeer deze en beschrijf wat je al op

niveau 3 uitvoert. Waarschijnlijk doe je nog niet alles van dit niveau, maar daar zou je vervolgens taken op kunnen definiëren en toevoegen. Op die wijze gaat TrustBound voor je werken als GRC systeem, waarbij je in controle komt wat te doen voor een bepaald volwassenheidsniveau.

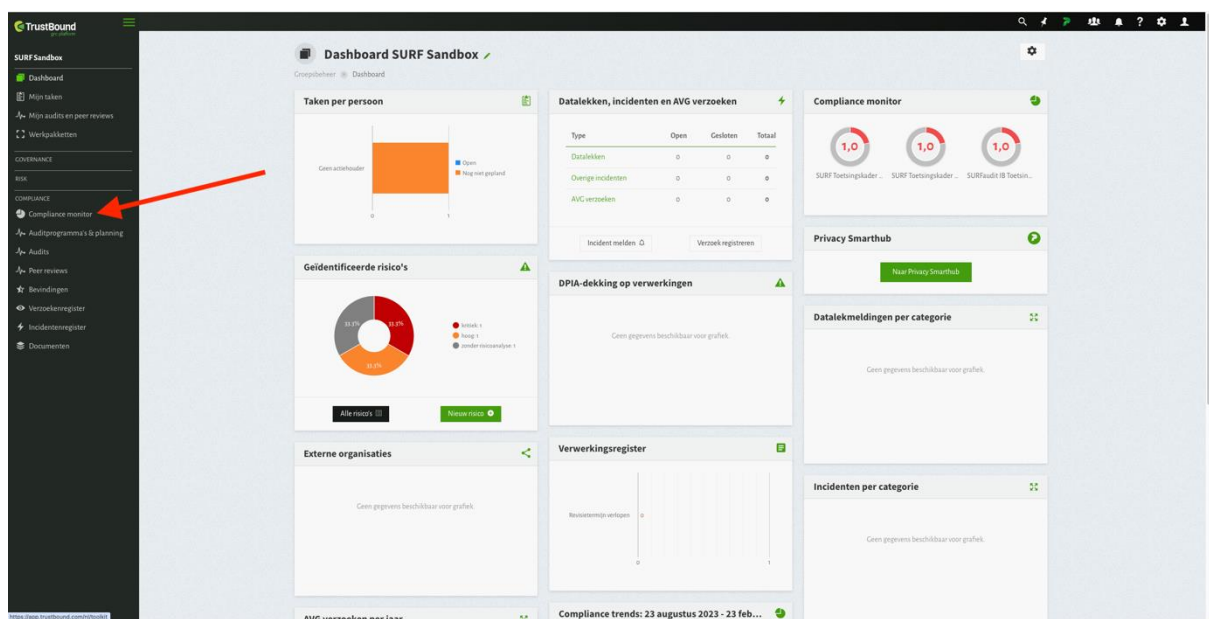
Voor meer informatie, toelichting op de inhoud van de statements, andere tips en tricks, raadpleeg [de handreiking over de security audits](#).



Het is in uitzonderlijke situaties mogelijk om statements Niet Van Toepassing te verklaren (Not Applicable in TrustBound). Let op dat je goed beargumenteert waarom je vindt dat een statement niet van toepassing is. Hoewel dit voor de benchmark niet nodig is, zal de auditor straks wel degelijk doorvragen over statements die je niet van toepassing hebt verklaard. Bijvoorbeeld de statements SD.01 en SD.02 over systeemontwikkeling; veel instellingen zetten deze statements op niet van toepassing. Maar we merken dat de auditor bijvoorbeeld vragen stelt over zelf ontwikkelde scripts of managementrapportages in PowerBI en deze activiteiten soms beschouwd als systeemontwikkeling. Wees dus terughoudend en kritisch bij het niet van toepassing verklaren van statements.

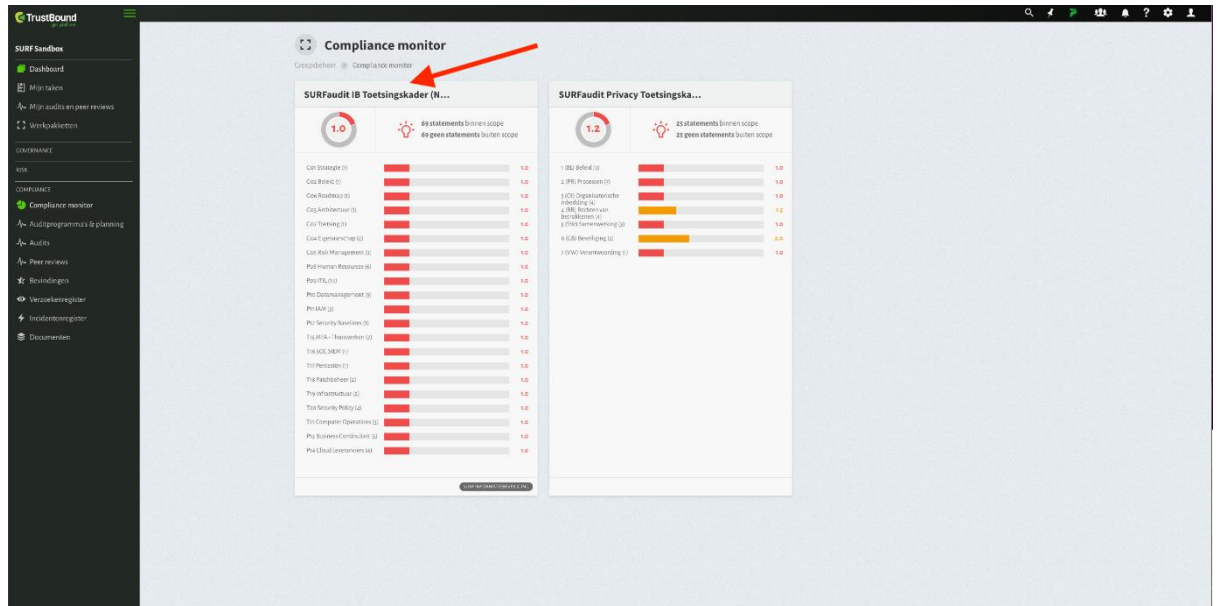
3 Benchmark inleveren

Nadat je alle statements hebt voorzien van een volwassenheidsniveau, klik op *Compliance monitor* in het dashboard.

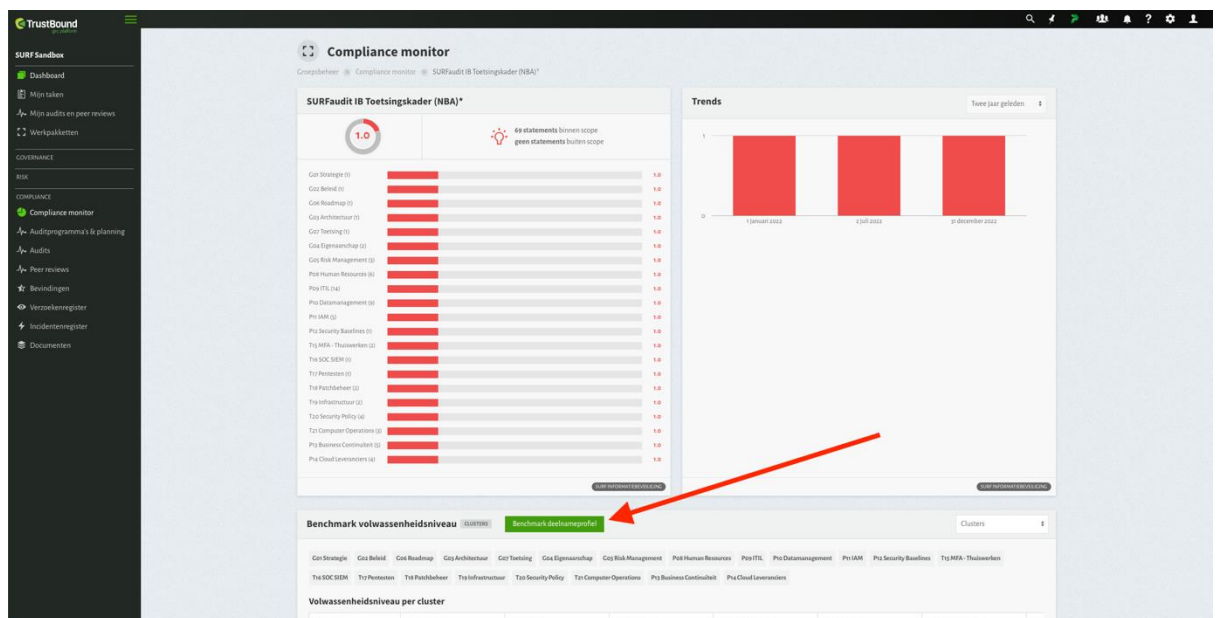


3.1 Uitwerking voor benchmark Informatiebeveiliging

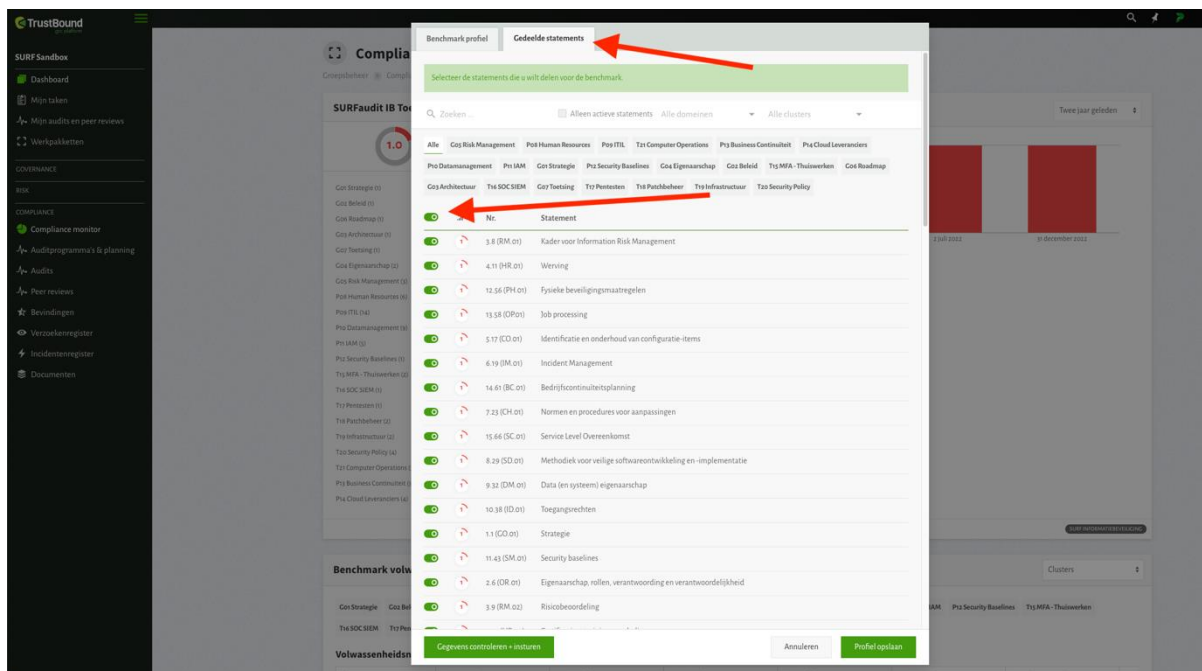
Klik op het toetsingskader voor informatiebeveiliging.



Klik op *Benchmark deelnameprofiel*

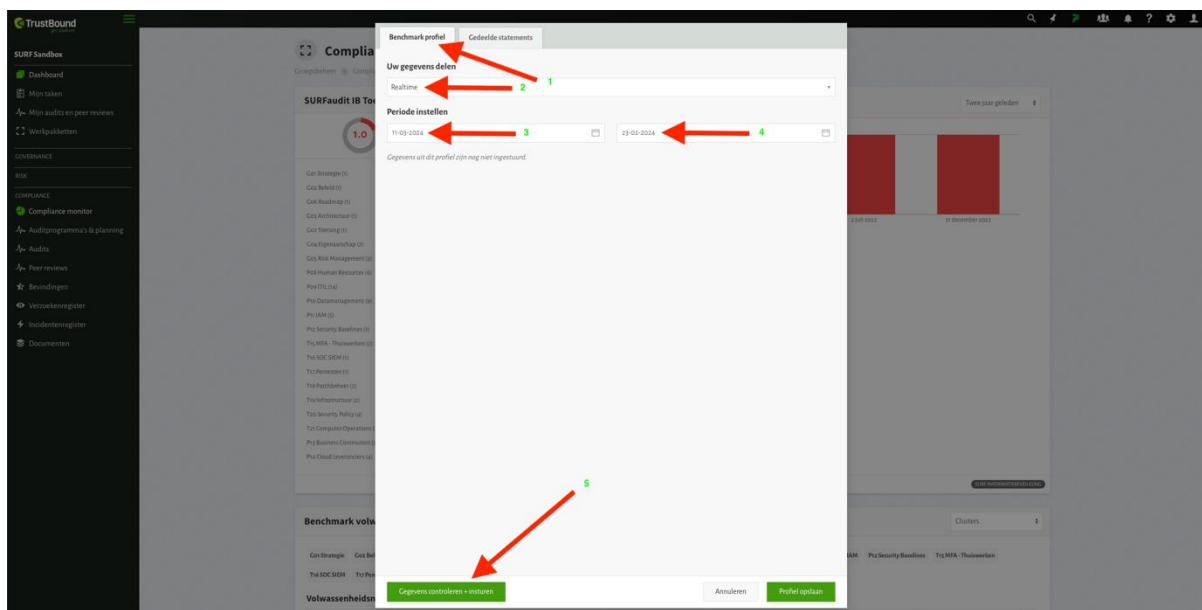


Ga naar *Gedeelde statements* en klik twee keer op het schuifje om alle statements te selecteren.



Klik weer terug op Benchmark profiel en stel het als volgt in:

- Uw gegevens delen:
 - Realtime**
- Periode instellen:
 - Wij willen jullie vragen om de gegevens beschikbaar te stellen tot **15 februari 2025**. Dit maakt het voor SURF mogelijk om tot 15 februari 2025 de cijfers voor de benchmark op te halen en het biedt uitwijkmogelijkheden voor het geval er iets misgaat.



4 Gegevens controleren en insturen

Klik op *Gegevens controleren + insturen*. Controleer je scores. Als deze correct zijn, klik op *Akkoord + verzenden*.

The screenshot shows the TrustBound interface with a modal window titled 'Benchmarke gegevens versturen naar koepel | 69 items'. The modal contains a table of benchmark items with columns 'No.' and 'Statement'. A red arrow points to the 'Akkoord + verzenden' button at the bottom right of the modal.

No.	Statement
3.8 (RM.01)	Kader voor Information Risk Management
4.11 (IR.01)	Werving
12.58 (PH.01)	Fysieke beveiligingsmaatregelen
13.58 (CPR.01)	Job processing
5.17 (CD.01)	Identificatie en onderhoud van configuratie-items
6.19 (IM.01)	Incident Management
14.61 (BC.01)	Bedrijfscontinuïteitsplanning
7.23 (CH.01)	Normen en procedures voor aanpassingen
15.66 (SC.01)	Service Level Overeenkomst
8.29 (SD.01)	Methodiek voor veilige softwareontwikkeling en -implementatie
9.32 (DM.01)	Data (en systemen) eigendom
10.38 (ID.01)	Toegangrechten
1.1 (CO.01)	Strategie
11.43 (DM.01)	Security baselines
2.4 (DR.01)	Eigendom, rollen, verantwoording en verantwoordelijkheid
3.9 (RM.02)	Risicobeoordeling
4.12 (IR.02)	Certificering, training en scholing
12.57 (PH.02)	Beheer van fysieke toegangrechten
13.59 (CPR.02)	Procedures voor back-up en herstel
5.18 (CD.02)	Configuratiegegevens en baseline
6.20 (IM.02)	Incident escalatie

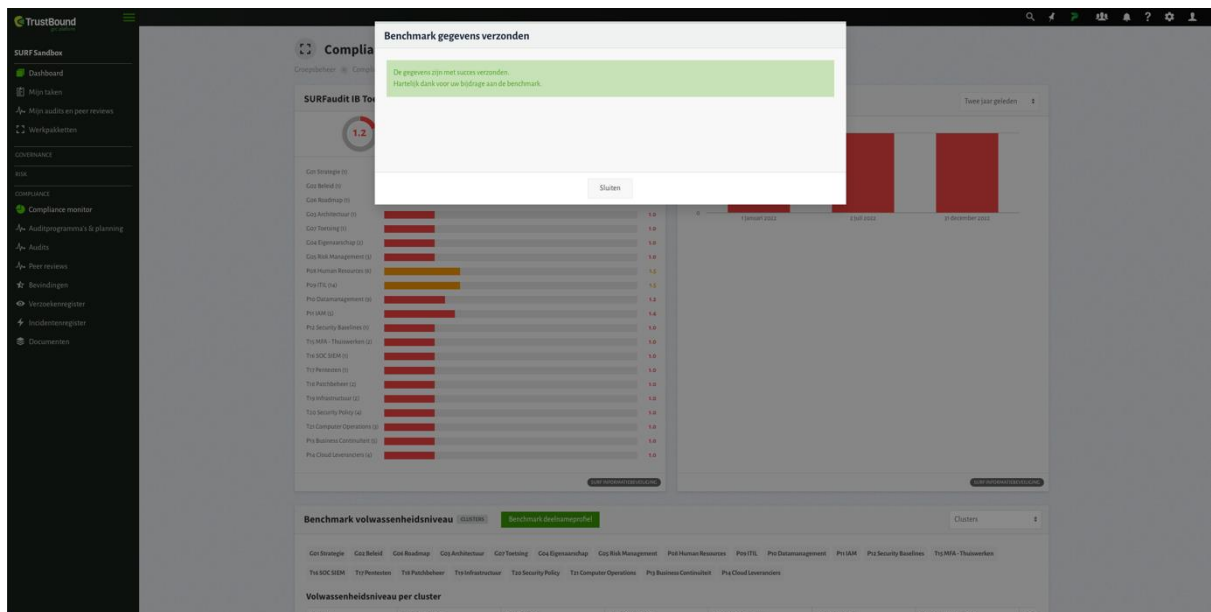
Buttons: Annuleren, Akkoord + verzenden

5 Bevestiging ontvangen



Op dit moment zijn wij met TrustBound in gesprek om in het inleverproces te verbeteren, zoals het ontvangen van een bevestiging als de scores ingeleverd zijn en het verkrijgen van een overzicht van de ingediende scores. Vanwege doorontwikkelingen in TrustBound kan het daardoor zijn dat onderstaande afbeeldingen kunnen afwijken.

Als het proces succesvol is voltooid, krijg je een bevestiging te zien.



Herhaal deze stappen ook voor de benchmark privacy om ervoor te zorgen dat beide benchmarks correct zijn ingesteld.

6 Extra ondersteuning

Voor eventuele vragen of onduidelijkheden over de benchmark, organiseren we twee online bijeenkomsten. Deze vinden plaats op [donderdag 9 januari 2025 van 16.00 – 17.00 uur](#) en op [dinsdag 14 januari 2025 van 16.00 – 17.00 uur](#). TrustBound zal ook aansluiten om eventuele vragen over de GRC-tool te kunnen beantwoorden. We moedigen je aan deel te nemen aan deze sessies als je extra hulp nodig hebt.

7 Bij problemen en vragen

Heb je na het lezen van deze handleiding nog vragen of ondervind je problemen met het indienen van je benchmarkgegevens? Aarzel dan niet om een e-mail te sturen naar ibp@mbodigitaal.nl.



MBO Digitaal is een platform van MBO Raad voor samenwerking aan digitalisering in het mbo. MBO Digitaal werkt samen met alle mbo-instellingen en heeft sterke banden met MBO Voorzieningen, Kennisnet en Surf.

MBO Digitaal
Houttuinlaan 6
3447 GM Woerden

Telefoon +31 (0) 348 – 75 35 00
Email info@mbodigitaal.nl
Website mbodigitaal.nl