NEN – ISUNA

Making Implementation Simple and Achievable - ISO27001 Compliance

25-05-2022

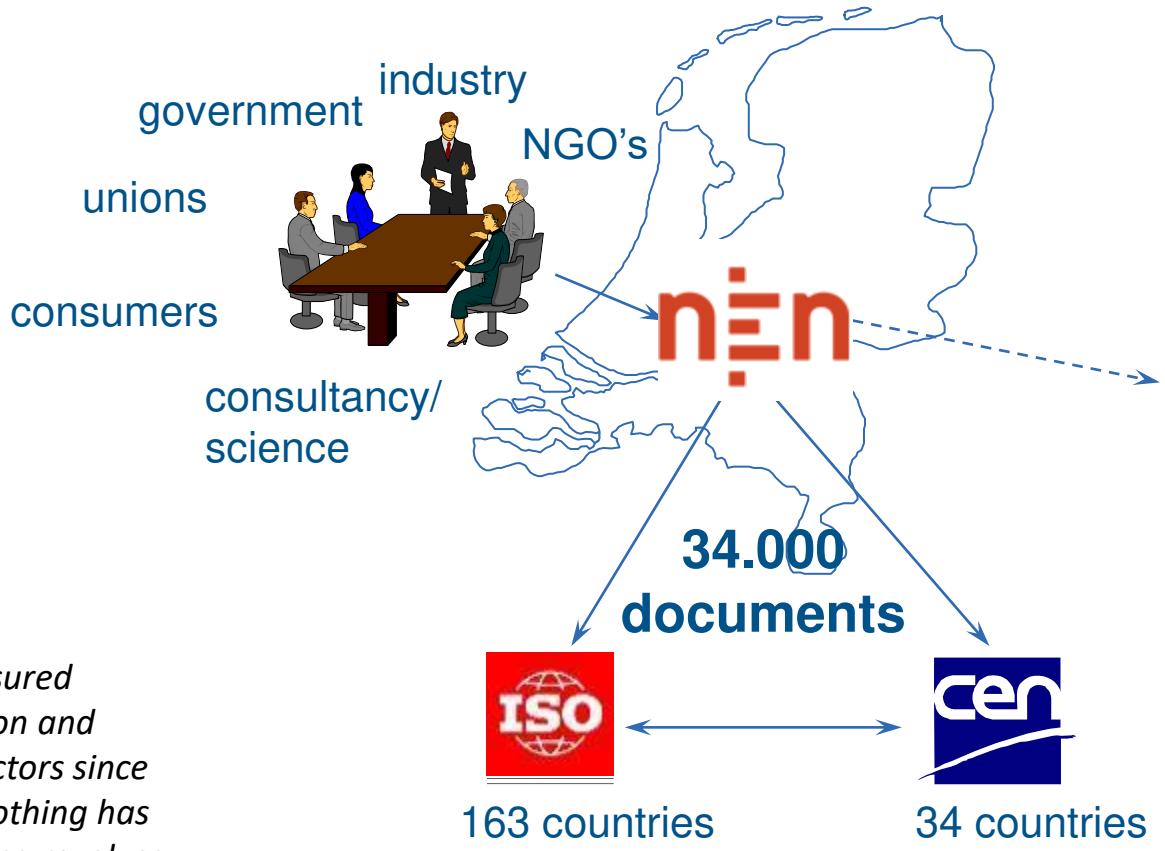
ISUNA

Standaard voor vooruitgang NEN

Programma

- Background of NEN and Isuna
- The challenges of implementing ISO27001 and the added value of the Isuna Cyber Compliance Platform
- How to further increase your trust and transparency on your digital business platforms
- Q&A

NEN, standardisation and standards



NEN

- promotes international trade, efficiency, innovation, security and sustainability.

How?

- Facilitate standardisation
- Connect networks
- publish standards/guidelines
- enable certification
- promote market adoption and implementation

NEN has ensured standardization and progress in all sectors since 1916. Basically nothing has changed, everything revolves around cooperation and joint agreements

ISUNA

nen

NEN partners and ISUNA?

- NEN supports users in implementing standards
- Users have specific context in which they apply standards
- NEN can only go so far in supporting specific needs
- NEN cooperates with partners to fulfil specific needs and receive feedback

iSUNA

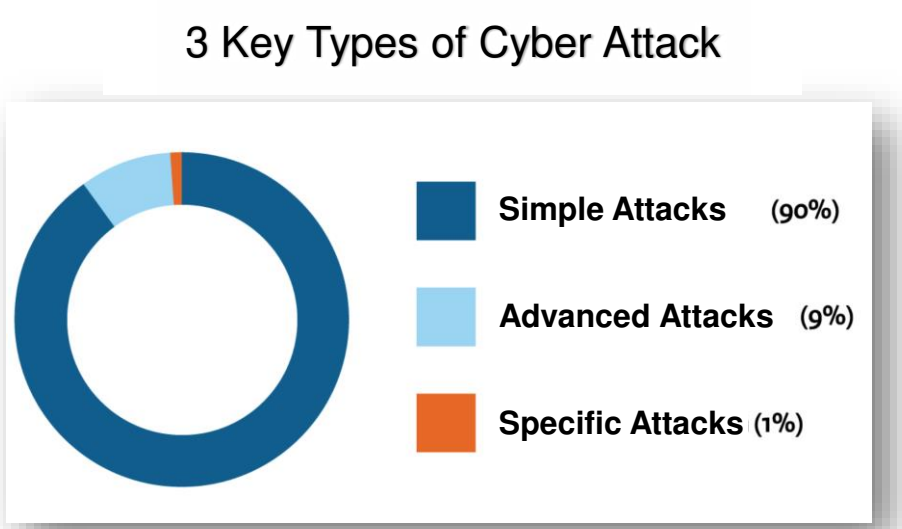
Isuna

- ISUNA delivers logical tools to users to implement standards and simplifies the process of implementation through open en easily understandable steps.

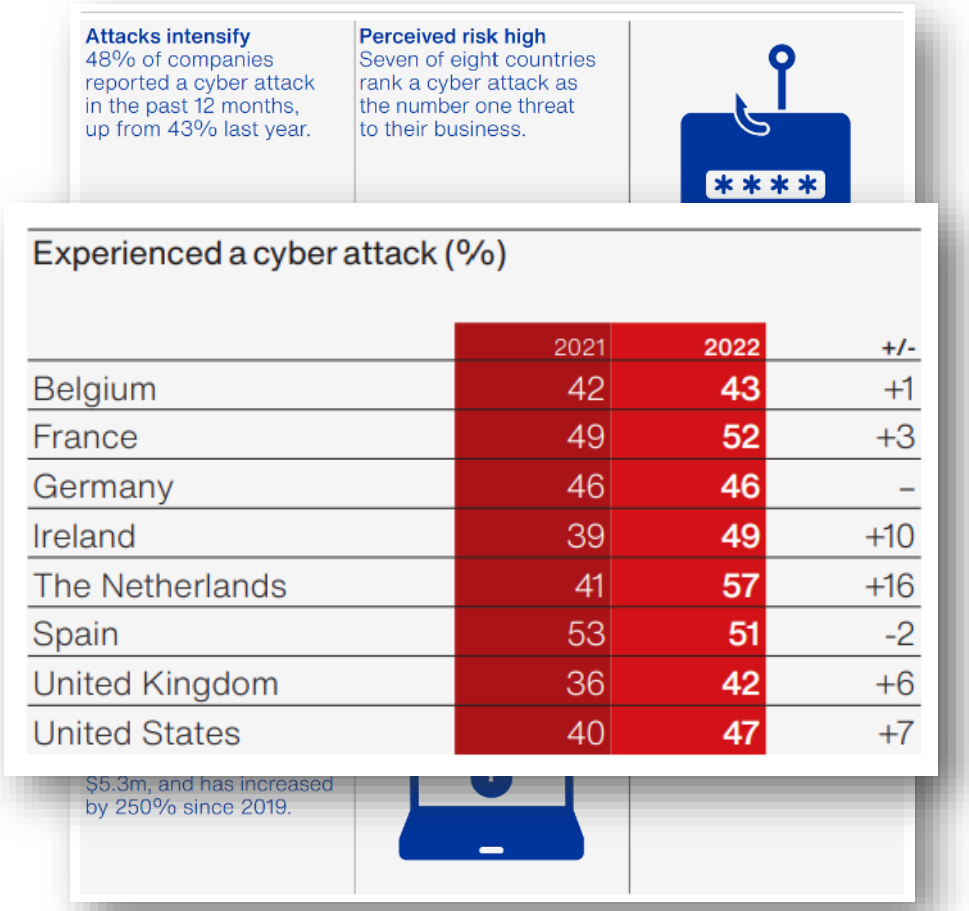
ISUNA

nen

Information Security



Source: Digital Trust Centre



Source: Hiscox Cyber Readiness Report

iSUNA

nen

Quiz Time

Problem 1

- The framework and implementation is complex
  - Technical language
  - Controls are across the guidance

Problem 2

- Many implementations take a long time
  - Tracking and checking is difficult (compliance monitoring)
  - Still using spreadsheets
  - Managing resources across departments

Problem 3

- Not possible to seek help or provide help to others
  - Increases costs and duplication of efforts
  - Do not know what works and what doesn’t
  - Who can help on a specific issue?

Live Isuna Platform Demo

- Key Spaces
  - Assessment
  - Maturity Reporting
  - Improvements
  - Help and Community Centre
  - Knowledge Centre
- User perspective;
- Implementation Focus

ISUNA

nen

Filter domeinen

Domeinen | Actueel niveau

1. Strategie en beleid
2. Operationeel
3. Personeelszaken
   - 3.1. Aanwerving 3
   - 3.2. Kwalificatie en opleiding 4
   - 3.3. On-Boarding en Exit-Boarding 2
   - 3.4. Kennis Delen 3
   - 3.5. InfoSec Opleiding 1
4. Beheer van klanten en leveranciers
5. Systeemontwikkeling
6. Gegevensbeheer
7. Configuratiebeheer
8. Identiteit & Toegangsbeheer
9. Beveiligingsmanagement
10. Technologie Beveiliging

Kwalificatie en opleiding

0 | Toepasselijk

IT-personeel dat opgeleid en gekwalificeerd is, zal het vermogen vergroten om incidenten en operaties aan te pakken, waaronder inbreuken op de beveiliging en kritieke aanvallen. Ook zal het dienstonderbrekingen beperken. Voorts zal hun voortdurende bijscholing de operationele doeltreffendheid waarborgen.

2

ISO 27001 / 7.2

ISO 27001 / A.7.2.2

Level 1

- [x] Opleiding en scholing voor IT-personeel wordt op een ad-hocbasis uitgevoerd
- [x] Er is beperkte of geen certificering van personeel

Level 2

- [x] Processen voor certificering, training en opleiding worden geïmplementeerd en geëvalueerd
- [x] Er zijn individuele persoonlijke ontwikkelingsdoelen beschikbaar voor (IT-)personeel

Level 3

- [x] Processen voor opleidings- en opleidingseisen worden geïmplementeerd en uitgevoerd
- [x] Opleiding, training en/of ervaring worden gebruikt om regelmatig te controleren of het (IT-)personeel de nodige vaardigheden heeft voor hun rollen/functies

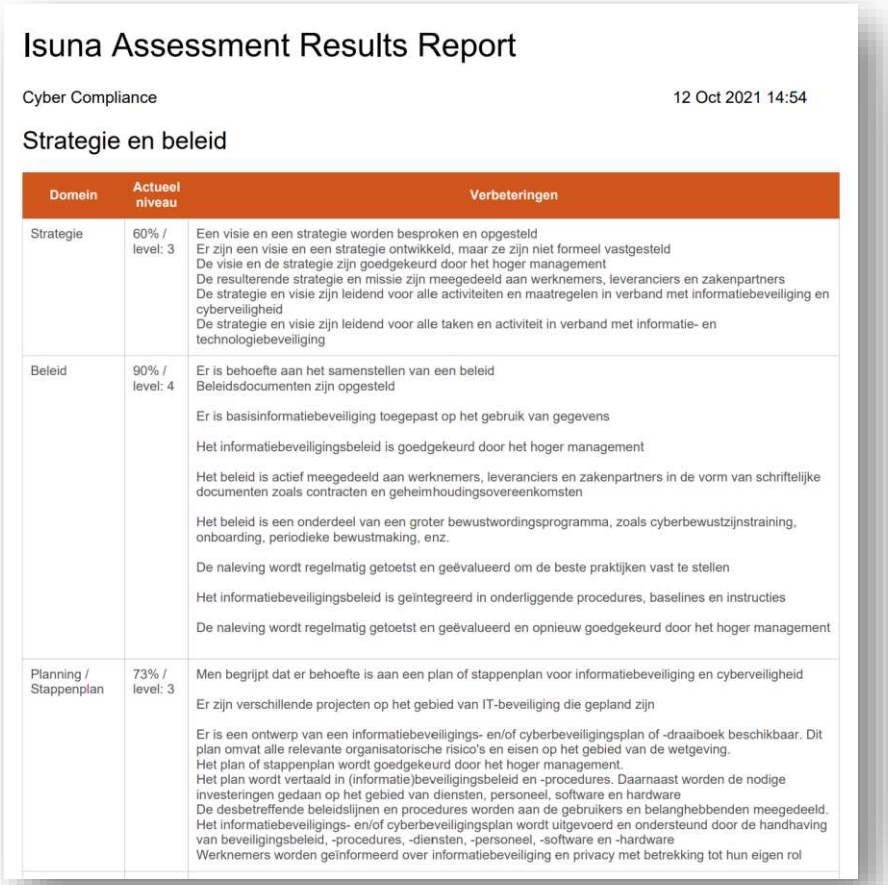
Level 4

- [x] De relevante processen worden voorgesteld aan en goedgekeurd door het (hogere) management
- [x] De vereiste kernvaardigheden (IT) zijn gedefinieerd en er worden passende kwalificatie- en certificatieprogramma's gebruikt om ervoor te zorgen dat ze behouden blijven
- [x] Er wordt toegezien op het bereiken van de persoonlijke ontwikkelingseisen of -doelstellingen

Level 5

- [ ] De uitvoering van de processen voor certificering, training en opleiding wordt jaarlijks geëvalueerd, waarbij ook het onderwijs- en trainingsmateriaal op relevantie, kwaliteit en doeltreffendheid wordt gecontroleerd

Maturity Reporting and Improvements

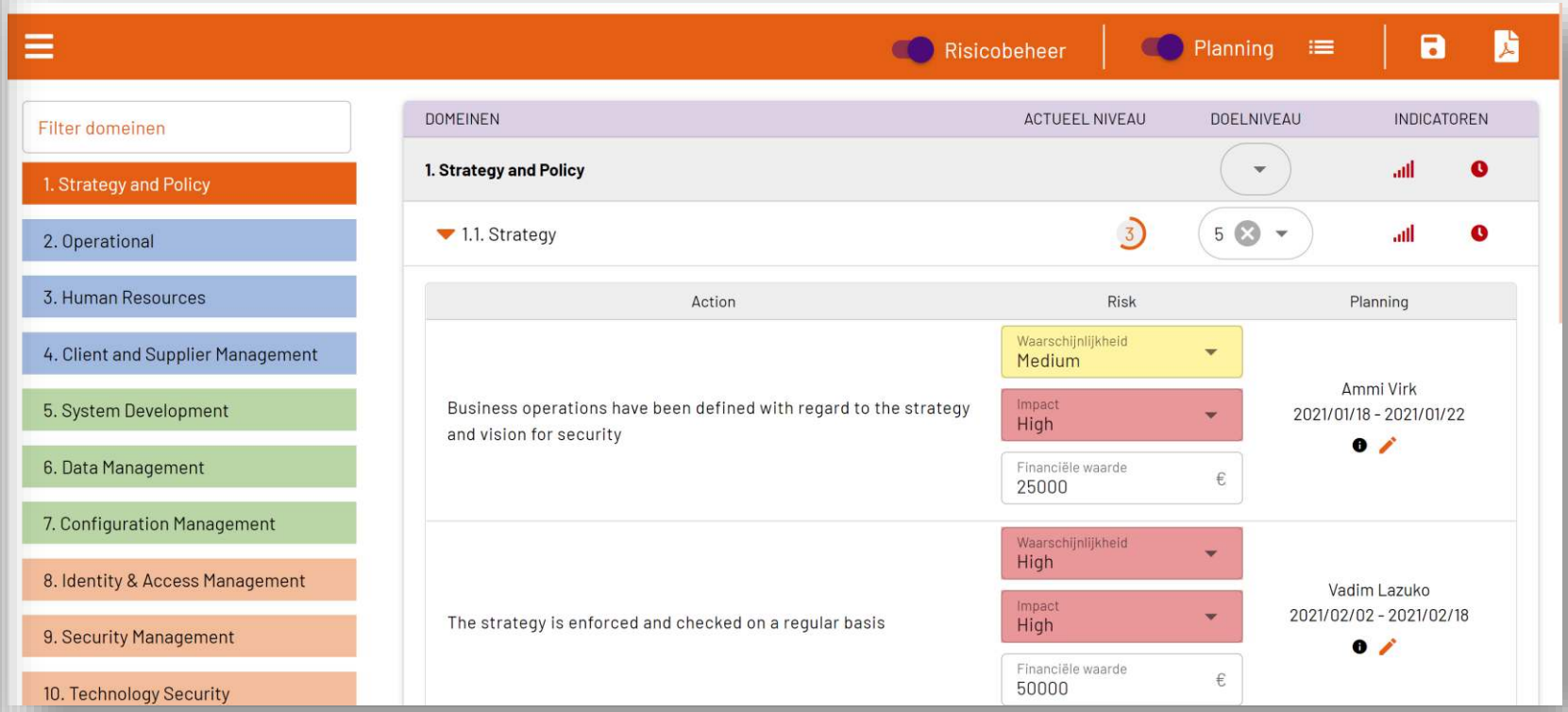


Isuna Assessment Results Report

Cyber Compliance 12 Oct 2021 14:54

Strategie en beleid

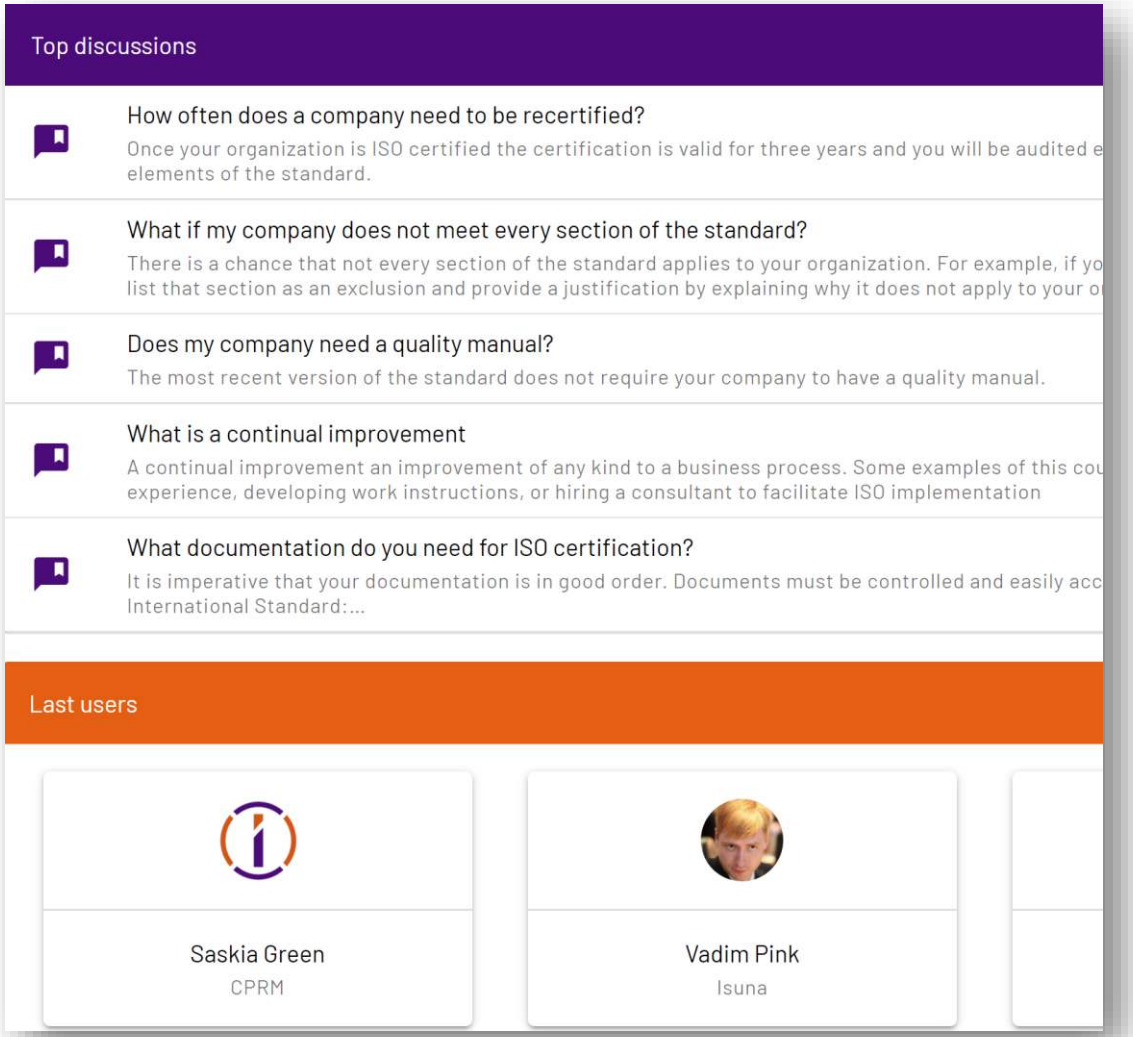
Domein	Actueel niveau	Verbeteringen
Strategie	60% / level: 3	Een visie en een strategie worden besproken en opgesteld Er zijn een visie en een strategie ontwikkeld, maar ze zijn niet formeel vastgesteld De visie en de strategie zijn goedgekeurd door het hoger management De resulterende strategie en missie zijn meegedeeld aan werknemers, leveranciers en zakenpartners De strategie en visie zijn leidend voor alle activiteiten en maatregelen in verband met informatiebeveiliging en cyberveiligheid De strategie en visie zijn leidend voor alle taken en activiteit in verband met informatie- en technologiebeveiliging
Beleid	90% / level: 4	Er is behoefte aan het samenstellen van een beleid Beleidsdocumenten zijn opgesteld Er is basisinformatiebeveiliging toegepast op het gebruik van gegevens Het informatiebeveiligingsbeleid is goedgekeurd door het hoger management Het beleid is actief meegedeeld aan werknemers, leveranciers en zakenpartners in de vorm van schriftelijke documenten zoals contracten en geheimhoudingsovereenkomsten Het beleid is een onderdeel van een groter bewustwordingsprogramma, zoals cyberbewustzijnstraining, onboarding, periodieke bewustmaking, enz. De naleving wordt regelmatig getoetst en geëvalueerd om de beste praktijken vast te stellen Het informatiebeveiligingsbeleid is geïntegreerd in onderliggende procedures, baselines en instructies De naleving wordt regelmatig getoetst en geëvalueerd en opnieuw goedgekeurd door het hoger management
Planning / Stappenplan	73% / level: 3	Men begrijpt dat er behoefte is aan een plan of stappenplan voor informatiebeveiliging en cyberveiligheid Er zijn verschillende projecten op het gebied van IT-beveiliging die gepland zijn Er is een ontwerp van een informatiebeveiligings- en/of cyberbeveiligingsplan of -draaiboek beschikbaar. Dit plan omvat alle relevante organisatorische risico's en eisen op het gebied van de wetgeving. Het plan of stappenplan wordt goedgekeurd door het hoger management. Het plan wordt vertaald in (informatie)beveiligingsbeleid en -procedures. Daarnaast worden de nodige investeringen gedaan op het gebied van diensten, personeel, software en hardware De desbetreffende beleidslijnen en procedures worden aan de gebruikers en belanghebbenden meegedeeld. Het informatiebeveiligings- en/of cyberbeveiligingsplan wordt uitgevoerd en ondersteund door de handhaving van beveiligingsbeleid, -procedures, -diensten, -personeel, -software en -hardware Werknemers worden geïnformeerd over informatiebeveiliging en privacy met betrekking tot hun eigen rol

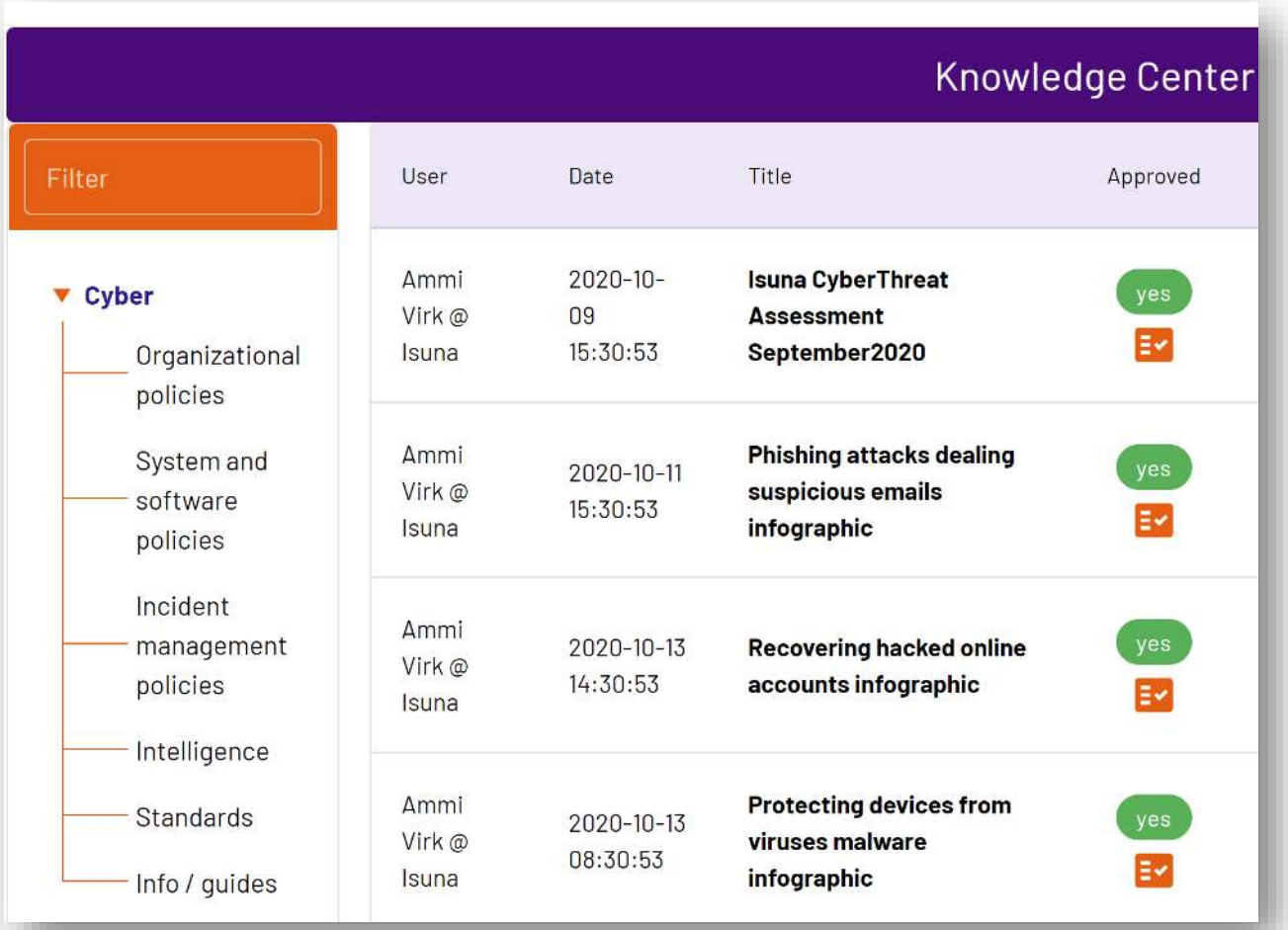


ISUNA

nen

Community and Knowledge Centre





Summary

- Background of NEN and about Isuna
- The challenges of implementing ISO27001 and the added value of the Isuna Cyber Compliance Platform
- How to further increase your trust and transparency on your digital business platforms

For more information:

www.nen.nl/isuna

www.isuna,.net

info@isuna.net