

NEN – ISUNA

**Making Implementation Simple and
Achievable - ISO27001 Compliance**

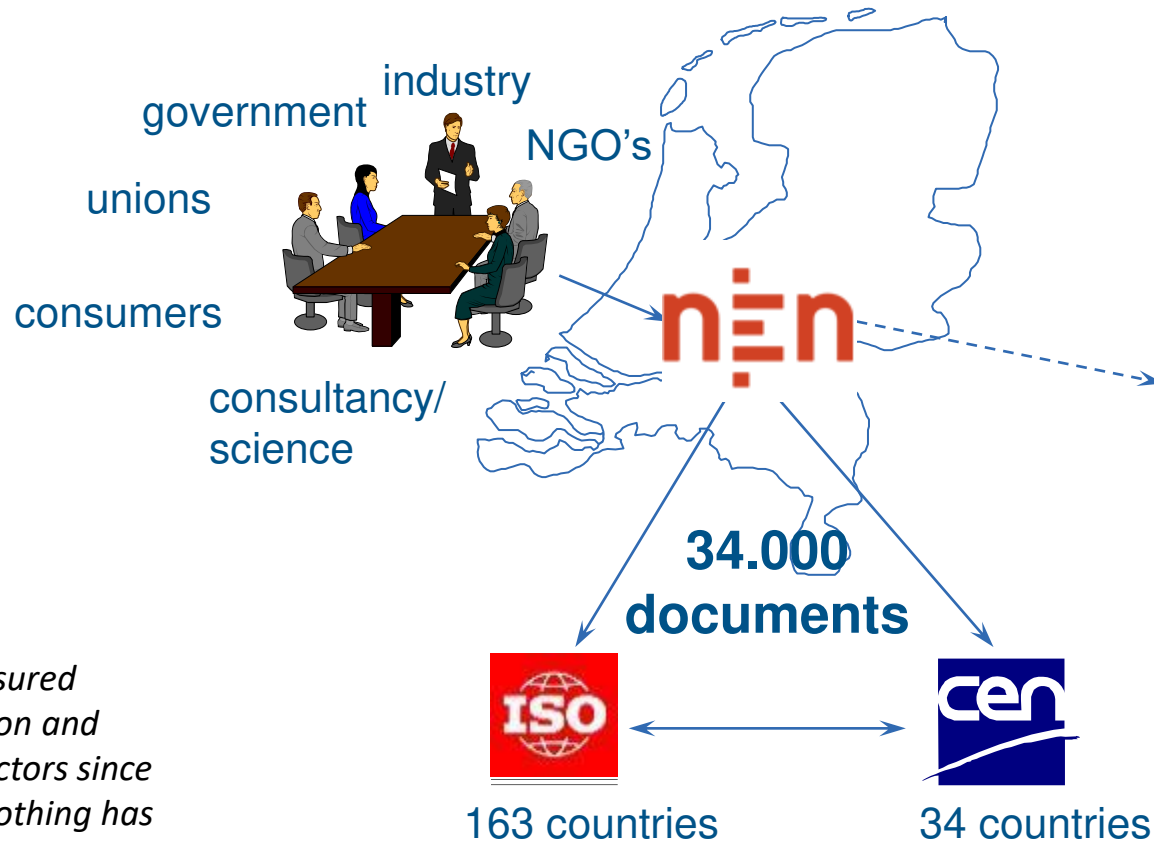
25-05-2022



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

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 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

Bekijk onze partners

Partner Isuna

Isuna biedt een platform dat implementatie van regelgeving en normen vereenvoudigt door middel van een stapsgewijs proces dat iedereen in uw bedrijf kan volgen.

Isuna biedt een one-stop-shop-platform dat implementatie van regelgeving en normen vereenvoudigt door middel van een stapsgewijs proces dat iedereen in uw bedrijf kan volgen. Beoordeel, rapporteer en implementeer eenvoudig uw compliance en krijg een real-time

Partner ArcusIT
Wij zijn Arcus IT. Met ruim 200 ICT-experts bedienen wij vanuit onze locaties in Zwolle,

Partner Baker Tilly
Baker Tilly IT Advisory is verantwoordelijk voor IT-audit en advies. Met ons team

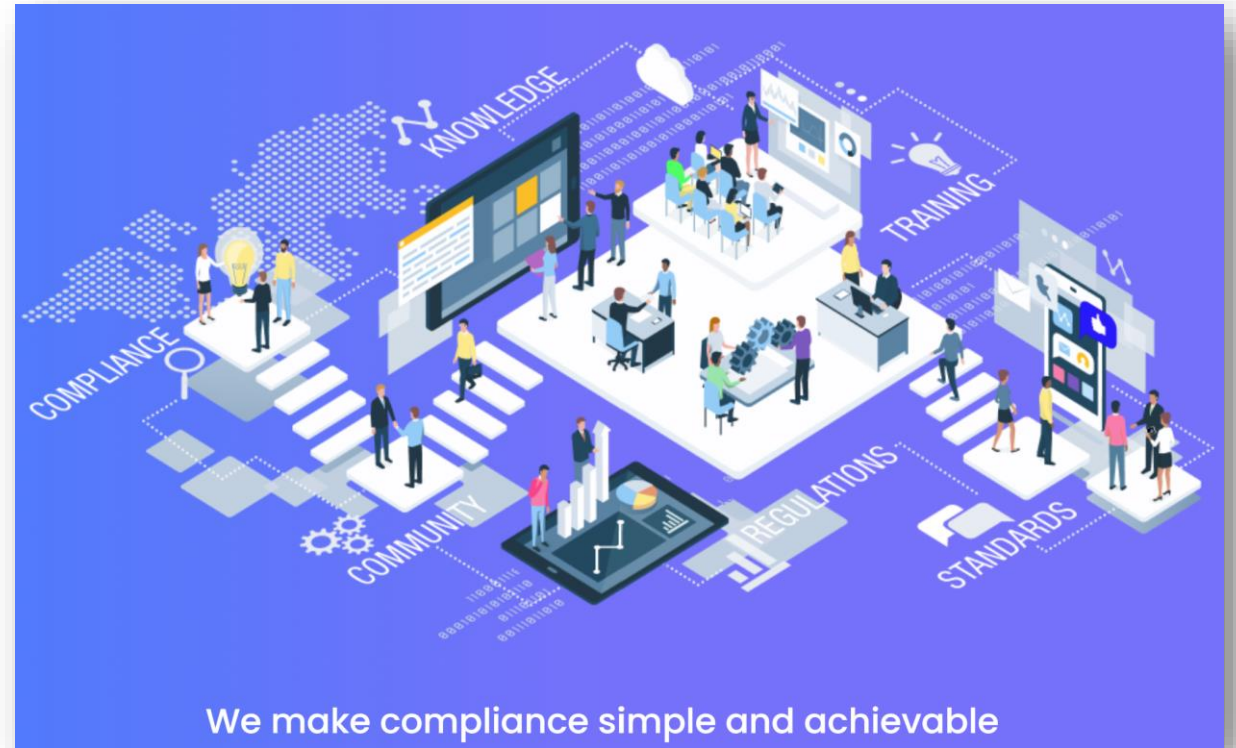
Partner Brocacef
Brocacef Supplies gespecialiseerde p

ISUNA
Naar partner website

nēn

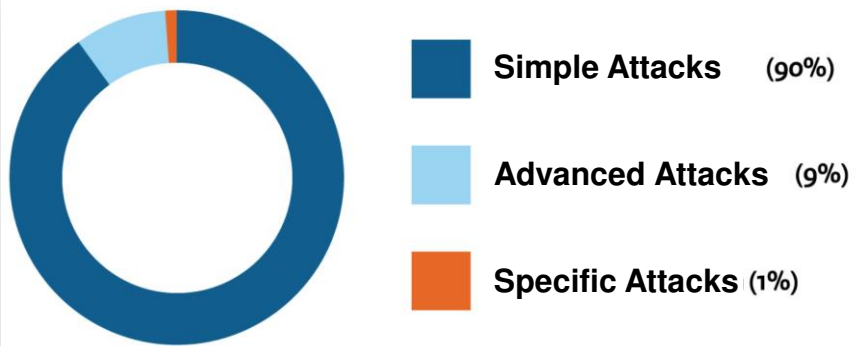
Isuna

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



Information Security

3 Key Types of Cyber Attack



Source: Digital Trust Centre

Attacks intensify
48% of companies reported a cyber attack in the past 12 months, up from 43% last year.

Perceived risk high
Seven of eight countries rank a cyber attack as the number one threat to their business.



Experienced a cyber attack (%)

	2021	2022	+/-
Belgium	42	43	+1
France	49	52	+3
Germany	46	46	-
Ireland	39	49	+10
The Netherlands	41	57	+16
Spain	53	51	-2
United Kingdom	36	42	+6
United States	40	47	+7

\$5.3m, and has increased by 250% since 2019.



Source: Hiscox Cyber Readiness Report

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



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
- 11. Werken op afstand en sociale media

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.

Level 1

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

Level 2

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

Level 3

- ✓ Processen voor opleidings- en opleidingseisen worden geïmplementeerd en uitgevoerd
- ✓ 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

- ✓ De relevante processen worden voorgesteld aan en goedgekeurd door het (hogere) management
- ✓ De vereiste kernvaardigheden (IT) zijn gedefinieerd en er worden passende kwalificatie- en certificatieprogramma's gebruikt om ervoor te zorgen dat ze behouden blijven
- ✓ 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

ISO 27001 / 7.2



ISO 27001 / A.7.2.2



2

📖

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

Filter domeinen

1. Strategy and Policy

2. Operational

3. Human Resources

4. Client and Supplier Management

5. System Development

6. Data Management

7. Configuration Management

8. Identity & Access Management

9. Security Management

10. Technology Security

DOMEINEN

1. Strategy and Policy

▼ 1.1. Strategy

Action	Risk	Planning
Business operations have been defined with regard to the strategy and vision for security	<div>Waarschijnlijkheid Medium</div> <div>Impact High</div> <div>Financiële waarde 25000</div>	<div>Ammi Virk 2021/01/18 - 2021/01/22</div>
The strategy is enforced and checked on a regular basis	<div>Waarschijnlijkheid High</div> <div>Impact High</div> <div>Financiële waarde 50000</div>	<div>Vadim Lazuko 2021/02/02 - 2021/02/18</div>

Community and Knowledge Centre

Top discussions



How often does a company need to be recertified?

Once your organization is ISO certified the certification is valid for three years and you will be audited elements of the standard.



What if my company does not meet every section of the standard?

There is a chance that not every section of the standard applies to your organization. For example, if you list that section as an exclusion and provide a justification by explaining why it does not apply to your organization.



Does my company need a quality manual?

The most recent version of the standard does not require your company to have a quality manual.



What is a continual improvement

A continual improvement is an improvement of any kind to a business process. Some examples of this could be gaining experience, developing work instructions, or hiring a consultant to facilitate ISO implementation.



What documentation do you need for ISO certification?

It is imperative that your documentation is in good order. Documents must be controlled and easily accessible. International Standard:...

Last users



Saskia Green
CPRM



Vadim Pink
Isuna

Knowledge Center

Filter

Cyber

Organizational policies

System and software policies

Incident management policies

Intelligence

Standards

Info / guides

User	Date	Title	Approved
Ammi Virk @ Isuna	2020-10-09 15:30:53	Isuna CyberThreat Assessment September2020	<div>yes</div> <div></div>
Ammi Virk @ Isuna	2020-10-11 15:30:53	Phishing attacks dealing suspicious emails infographic	<div>yes</div> <div></div>
Ammi Virk @ Isuna	2020-10-13 14:30:53	Recovering hacked online accounts infographic	<div>yes</div> <div></div>
Ammi Virk @ Isuna	2020-10-13 08:30:53	Protecting devices from viruses malware infographic	<div>yes</div> <div></div>

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

