

A photograph of three young people sitting on a black metal bench outdoors. A young man with dark curly hair, wearing a grey long-sleeved shirt, is holding a smartphone and showing it to two young women. The woman next to him has long brown hair and glasses, wearing a red jacket and patterned pants. The woman on the right has long red hair and is wearing an orange jacket. They are all smiling and looking at the phone. In the background, there is a multi-story brick building with balconies and some greenery.

Integratie ISMS-KMS bij Timon

Presentatie NNK, September 2023

Presentators: Marianne Gerrits en Parastu Zahib

Voor vandaag

Een praktijkverhaal

- Relatie ISO 9001 en NEN7510
- Hoe pakten wij dit aan?
- Waar liepen we tegenaan?
- Hoe is de situatie nu?
- Discussie/vragen



Wie zijn wij

- Parastu Zahib, CISO/FG
- Marianne Gerrits, kwaliteitsadviseur, lid van de NNK
- Waar werken wij? [Timon](#). Timon bestaat 40 jaar.
- Jeugdzorg en zorg voor jongvolwassenen



Missie Timon

Gezinnen met kinderen, jongeren en jongvolwassenen helpen bij problemen met opvoeden en opgroeien op weg naar zelfstandigheid en volwassenheid.

- **Diensten:** Specialistische zorg in aanvulling op de lokale zorg en het netwerk van cliënten
- **Profiel:** Christelijke organisatie



Timon: cijfers

Helpt >4000
cliënten per jaar



992 pleegkinderen
en 1200 pleegouders



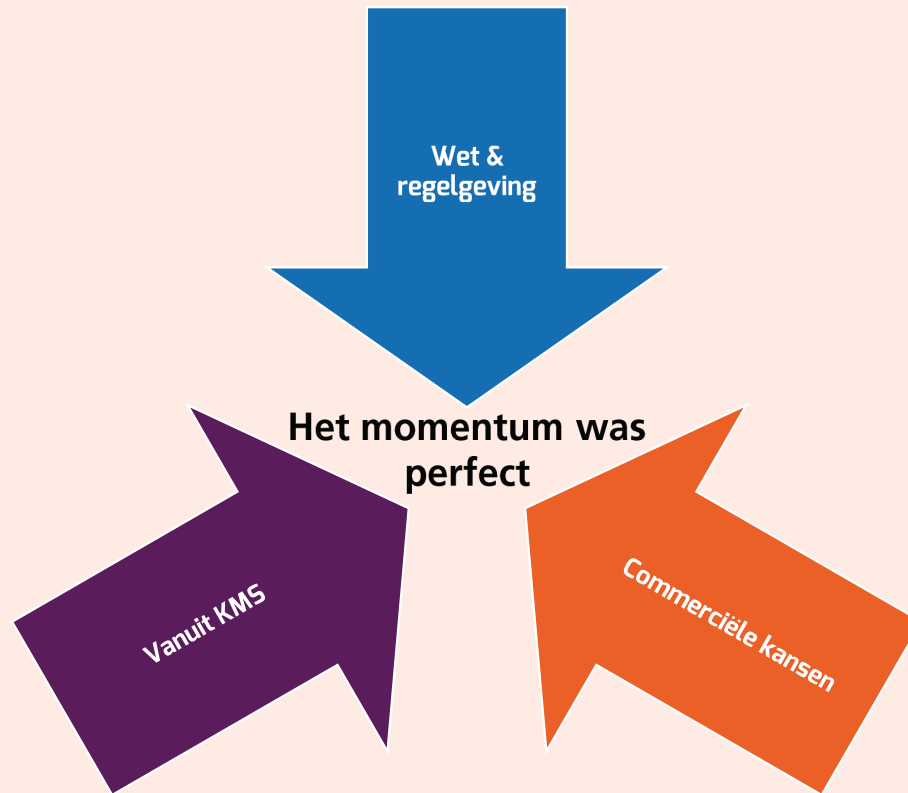
750 medewerkers



225 vrijwilligers



Waarom zijn we hieraan begonnen



Goede en veilige zorg!

- Duw vanuit AVG en andere normen
- Vraag vanuit de markt
- Wil vanuit het kwaliteitsteam

"When the winds of change blow,
some people build walls, others
build windmills"

Waarom integratie?

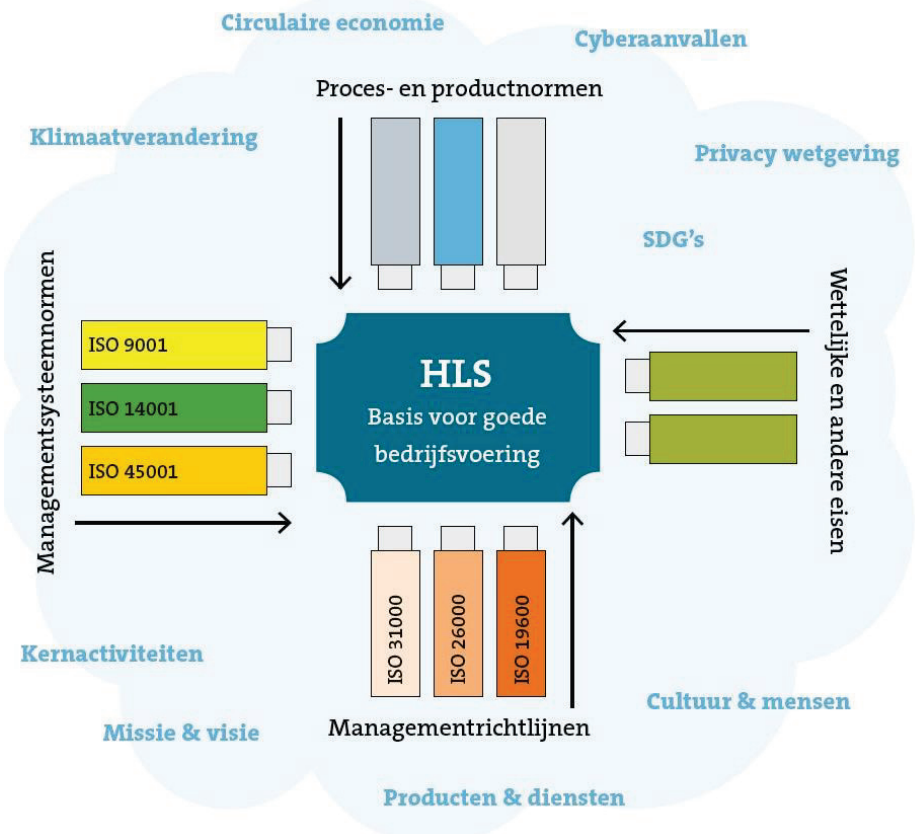
Goede *bedrijfsvoering*
continue **Verbeteren**



**Risicomanagement en kwaliteitsmanagement
zijn integraal onderdeel van de
bedrijfsvoering!**

Veranderingen in ISO-HLS

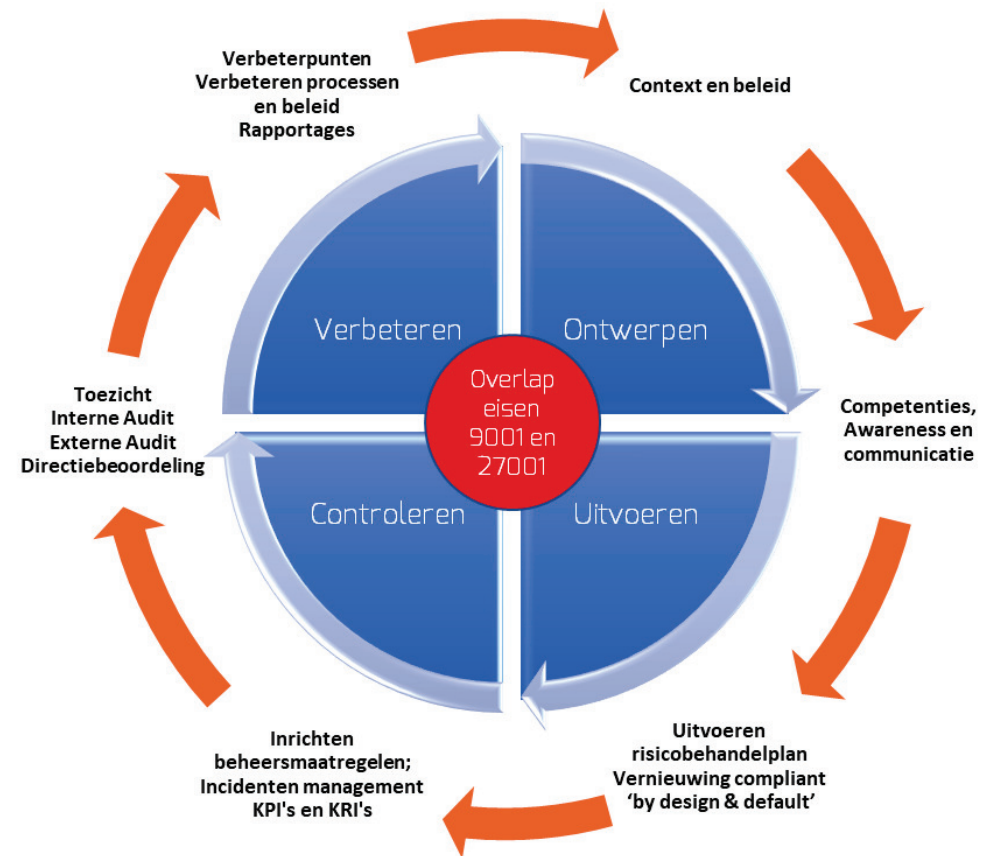
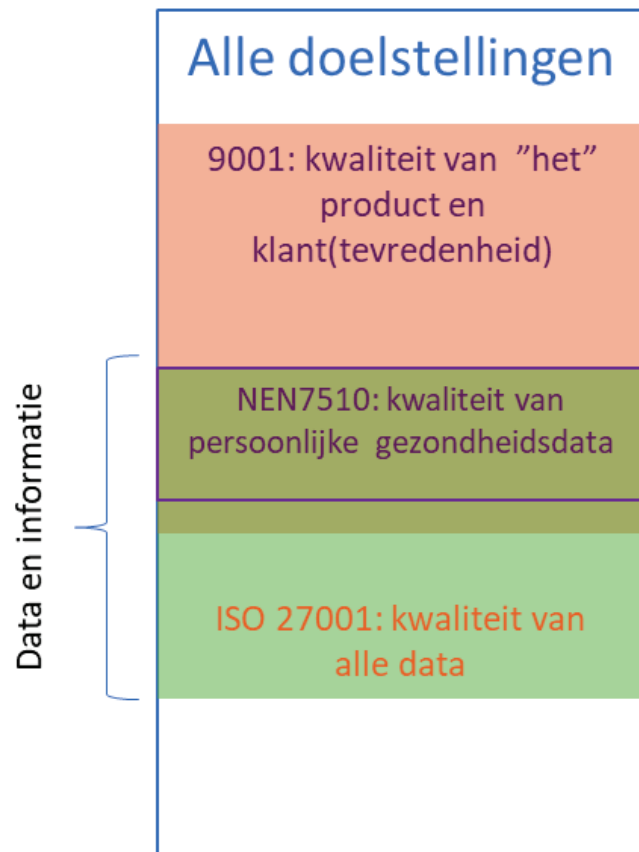
1. Scope is bedrijfsvoering
2. Focus op de effectiviteit van het systeem
3. Ketenbeheersing ipv 'Outsourcing'.
4. Verandermanagement nu in alle normen
5. Verschuiving richting continue verbetering



Lees het volledige artikel in: [Harmonized approach to MSS_QWSUMMER2021.pdf \(nen.nl\)](#)

Relaties tussen normen en systemen

Overlap ISO 9001, ISO27001 en NEN7510



Hoe doen wij
het bij Timon

**The combination
of hard work
and smart work
is efficient work.**

Robert Half

Timon

KMS en ISMS integratie bij Timon

Prioriteit	Must have			Context analyse Analyse Kritische Processen Interne Audit Directiebeoordeling 
	Should have	Externe Audit IB en AVG Incidenten Toezicht Compliant by design & default	Middelen, ondersteuning Beleidsontwikkeling Verbetermatrix (PDCA) Rollen en verantwoordelijkheden	Kwartaal Rapportages
	Nice to have	Behandelplan Doelstellingen Implementatie beleid	Awareness	
		Niet	Gedeeltelijk	Volledig

Mate van integratie

Aanpak: Reis van Timon

Start KMS

- HKZ met 4 schema's
- 2018 ISO 9001

2019 Start ISMS

- 2019 projectplan IB
- 2020: 0 meting door extern auditor
- 2021: Projectleider NEN aangesteld
- Risico inventarisatie ingezet
- Start ISMS Interne audits en week van de privacy

2021 NEN7510 certificering

- 2021: de echte externe audit
- 2022: Inrichting Forum IB

2022: Vervolg Integratie

- Gezamenlijke Interne audits
- 2023: Forum IB nieuwe stijl
- Directiebeoordeling
- Jaarplan IB

**We zitten allemaal
in hetzelfde schuitje,
alleen de een roeit
en de ander vist.**

OM
MENSEN

3
Voorbeelden

Cyclus

- 2x per jaar
- Dekking kritische processen 1x3 jaar

Team

- KMS
- Medewerkers Timon
- CISO team

Opzet

- Peer review
- 2x jaar training
- 4 thema's per jaar, inclusief
- IB en AVG

Voorbeeld 1: Interne Audits

1. Incidenten:

Vanuit de incidentenrapportages lijkt het er op dat de meldingsbereidheid verschilt per regio/team. Doel is om beter zicht te krijgen op de bekendheid met het proces, doet iedereen wat hij moet doen, hoe geef je opvolging aan een incident en wat leer je ervan in het team. Dit thema is belangrijk bij Jeugdzorg Nederland (dialogoog over geweld) en AVG en Informatiebeveiliging.

2. Toegang tot dossiers

Toegang tot dossiers is een belangrijk thema voor een adequate dienstverlening en in het kader van de informatiebeveiliging. Het is mogelijk dat medewerkers "de rode knop" gebruiken om een dossier in te zien. Je kunt dan een dossier openen waar je binnen je autorisatie geen toegang tot hebt. Hier moet wel een gegronde reden voor zijn (denk bijv. aan de Bereikbaarheidsdienst).

Voorbeeld 2: Awareness Week

Volgende week is het weer zover: de Security Awareness Week met het thema 'En zo doen we het!'.

PROGRAMMA

MAANDAG

- KICK-OFF
- WIST JE DAT?
- EN ZO DOEN WE HET!
- DIEV TRAINING

DINSDAG

- WIST JE DAT?
- EN ZO DOEN WE HET!
- TEST
- FILMPJE

WOENSDAG

- WIST JE DAT?
- EN ZO DOEN WE HET!
- QUIZ EN TEST
- FILMPJES

DONDERDAG

- EINDQUIZ
- FAQ
- QUIZ EN TEST
- FILMPJES

VRIJDAG

- DE GROTE EINDQUIZ

SECURITY AWARENESS WEEK 2023

HET PROGRAMMA

MAANDAG Datalekken

- Kick off
- Privacy Quiz

DINSDAG Wachtwoorden

- Wist je dat?
- Check je wachtwoord

WOENSDAG Social engineering

- Privacy app
- Filmpjes

DONDERDAG Phishing

- Eindquiz
- FAQ
- Check veilige linkjes

VRIJDAG Afsluiting

- Evaluatie
- Eindquiz

IEDERE DAG

- Filmpjes
- Kruiswoordpuzzels

Voorbeeld 3: Jaarplan IB on a page

Het informatiebeveiligingsplan is een hulpmiddel bij het bereiken van de IB-doelstellingen en beheersen van de risico's.

We werken met 1 Plan, waarbij wordt gewerkt met een geïntegreerde benadering. De BAU activiteiten, toezicht en monitoring komen bij elkaar.

Top risico's <ul style="list-style-type: none"> • Logische toegangsbeveiliging • Leveranciersmanagement • Training en Bewustzijn 		Kritische processen <ul style="list-style-type: none"> • Leveranciersmanagement • Werving & Selectie • Instroom 	
Doelstellingen: <ul style="list-style-type: none"> • Adequate overgang naar de nieuwe organisatie • Aantoonbaar in control voor IB en AVG • Verlengen van NEN7510 certificaat • Verhogen van volwassenheid AVG processen. 		KPI's: <ul style="list-style-type: none"> • Stoplicht rapportage ingevuld voor minimaal 2 onderdelen. • Min 1 controle activiteit op top 3 kritische processen • IB-Beleid aangepast en geïmplementeerd. • Min 2 Training en/of Awareness activiteiten 	
Type werkzaamheden	Zelfevaluatie (1ste lijn) <ul style="list-style-type: none"> • Horizontaal (thematisch) • Verticaal (per regio/ onderdeel) 	CISO en FG (2de lijn) <ul style="list-style-type: none"> • Verbeterpunten • Eigen onderwerpen • Leveranciersmanagement • Bewustzijn 	Audit (3de lijn) <ul style="list-style-type: none"> • Interne Audit 2x per jaar • Externe Audit ISO9001 • Externe Audit NEN7510 • FG thema's
	Jaarplan 2023	<ul style="list-style-type: none"> • Directiebeoordeling • TIM CV • Logische toegang in-dooruitstroom • Leveranciersbeoordelingen 	<ul style="list-style-type: none"> • Noodknop procedure • Dataopslag buiten Care4 (NEN7510) • Aanpassing beleid en organisatie TTB • Risico assessment AFAS • Awareness week 2x • Herijken DPIA proces • Herijken Leveranciersmanagement

ONDERWIJS
MAAK JE
SAMEN



KWALITEIT
EN VERBETERING
VRAAGT OM EEN CULTUUR
VAN ONVERBIDDELIJKE
REFLECTIE.



Vrij naar:
The Toyota Way, Liker, 2003

Illustrated with love at [inkcreativity.com](#)



Wat ging goed?

Wat ging goed

- Bestuurssecretaris overkoepelend
- Integratie vanaf begin als gedachtegoed
- Interne audits gecombineerd
- Verbetermatrix

Wat ging niet goed

- Afhankelijkheid van de externe kennis en capaciteit
- Onduidelijkheid rond rol proceseigenaar en kwaliteit.
- Processen zoals directiebeoordeling en leveranciersmanagement te tijdrovend en inefficiënt

Wat heeft het ons opgeleverd?

- 2 certificaten aan de muur: ISO 900:2015 en NEN7510
- Medewerkers zijn zich, naast het kwaliteitsdenken, nu ook meer bewust wat informatiebeveiliging inhoudt
- Betere vindbaarheid en zichtbaarheid
- Minder belastend voor de organisatie
- Efficiency en capaciteitsbesparing binnen kwaliteit (KMS en CISO)
- Betere continuïteit binnen team

We zijn er nog niet

- Borging interne capaciteit en kennis
- Geïntegreerde Externe Audits
- Sommige processen efficiënter en geïntegreerd opzetten
- Awareness en betrokkenheid Directie en Senior management



