Audit findings are easy to come up with, successful change from a finding is true (internal) audit value.

– Michael Piazza

auteur & consultant

Jasper Steenkamp
jasper.steenkamp@northwave.nl
06 82 991 225

Northwave

Security Officer
Business Security Consultant

Edward Ho
edward.ho@northwave.nl
06 57 840 240

Northwave

Manager Security Advisory

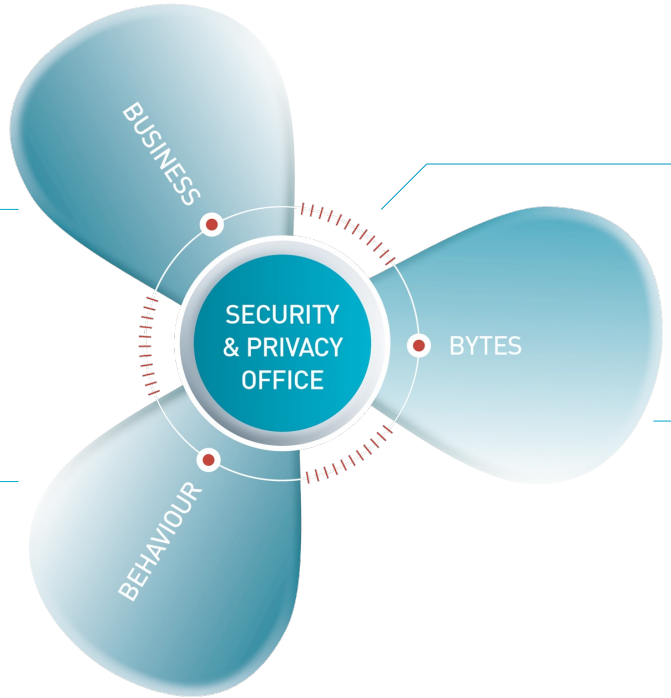
NORTHWAVE INTELLIGENT SECURITY OPERATIONS

BUSINESS
OUR PLANS, POLICIES & PROCEDURES WORK

ISO 27001, AVG Compliance
Cyber Resilience
Business Continuity
State of Security Assessment
Risk Consultancy & Audits

BEHAVIOUR
OUR PEOPLE WILL ACT 'CYBERSAFE'

Company wide ACT! Cyber Aware
Cyber Crisis Management
Security Skills Training



SECURITY & PRIVACY OFFICE
THE EFFECTIVENESS OF OUR SECURITY IS ENSURED

Security Office as a Service
Privacy Office as a Service

BYTES
OUR IT IS INTRINSICALLY SECURE

Red Team Ethical hacking
Managed Detection & Response (SOC/SIEM) Services
Cyber Threat Intelligence
CERT Forensic Investigations
Security Architecture & Design

WAAROM? *“True added value.”*

HOE? *“What you do is up to you, just do it!”*

WAT? *“All good things come in three.”*

WAT IS JULLIE ERVARING MET INTERNE AUDITS?

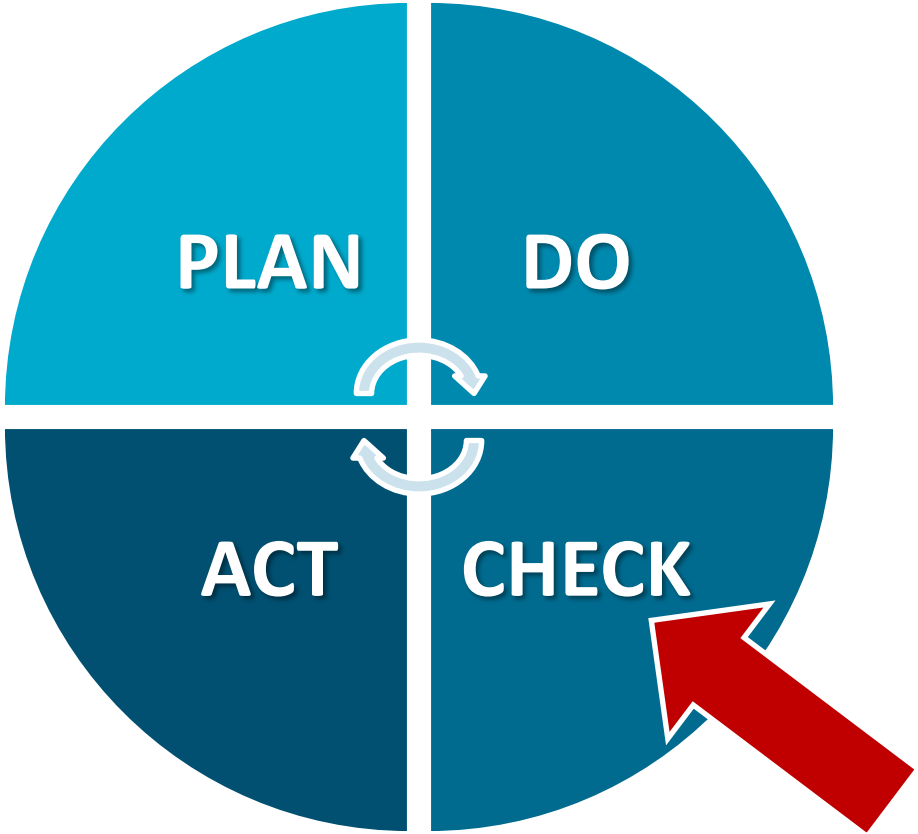
DRIE TYPEN AUDITS

Ref.	FIRST PARTY	SECOND PARTY	THIRD PARTY
Type	*Interne audit*	*Leveranciersaudit*	*Certificeringsaudit*
Doel	Vaststellen in hoeverre je als organisatie voldoet aan eigen processen en gehanteerde normenkaders.	Audit bij een (kritische) leverancier van de organisatie, om te toetsen in hoeverre deze voldoet aan jouw eisen.	Audit om te toetsen of een organisatie voldoet aan een specifieke norm met als doel het behalen van een certificaat.
Door	Door jouw eigen organisatie, of door een ingehuurde partij namens jouw organisatie.	Door jouw eigen organisatie, of door een ingehuurde partij namens jouw organisatie.	Certificerende instelling.


WAAROM?


WIE VOERT ER
INTERNE AUDITS UIT?

WAAROM?



WAAROM?

OPZET	BESTAAN	WERKING
Hoe is de opzet van mijn security management proces, plan en maatregelen?	*Kun je aantonen dat jouw opzet ook bestaat?*	*Kun je bewijzen dat het plan of maatregelen werken?*

Plan of maatregelen om risico's te beheersen.

Voorbeeld

WAAROM?

OPZET	BESTAAN	WERKING
Hoe is de opzet van mijn security management proces, plan en maatregelen?	***Kun je aantonen dat jouw opzet ook bestaat?***	***Kun je bewijzen dat het plan of maatregelen werken?***

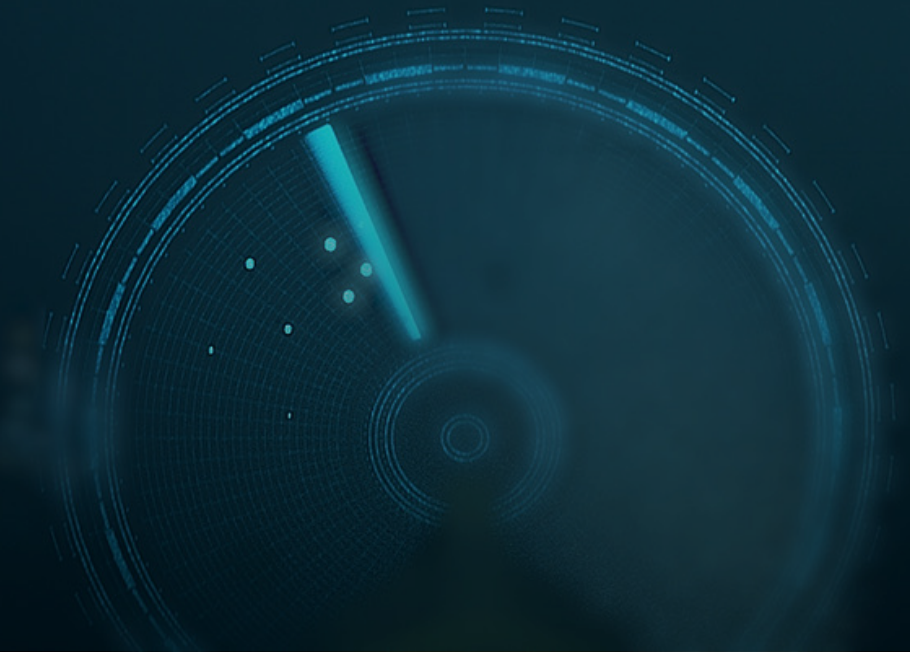
Risico: Tijdens development komen bugs in software terecht, wat kan leiden tot negatieve impact op beschikbaarheid, integriteit, vertrouwelijkheid van het eindproduct.

In je development policy staat dat usecases gereviewd en getest moeten worden, en dat bevindingen moeten worden opgevolgd, volgens een vastgesteld proces.	Kun je laten zien hoe het proces van review, testen en opvolgen gevolgd wordt tijdens development?	Op basis van een steekproef bewijzen dat de vereiste reviews, tests en opvolging zijn uitgevoerd over een langere periode.

TAKE AWAY 1 - WAAROM?

Om inzicht te krijgen in de werking en effectiviteit van jouw risicomanagement en de beheersing van jouw risico's.


HOE?



HOE ZIEN JULLIE INTERNE AUDITS ERUIT?

HOE?

Individuele interviews	Steekproeven	Observaties	Auditplan
Groepsgesprek	Technisch testen	Document reviews	Rapportage

HOE?

Individuele interviews	Steekproeven	Observaties	Auditplan
Groepsgesprek	Technisch testen	Document reviews	Rapportage

Voorbeeld

AUDIT PLANNING

Dag 1	Dag 2*	Dag 3*	Dag 4*	Dag 5/6*
Voorbereiding en planning	Audit: ISMS	Audit: Annex A (1)	Audit: Annex A (2)	Documentatie review + rapportage

* Benodigde tijd is afhankelijk van de scope en grootte van de organisatie

TAKE AWAY 2 - HOE?

Een effectieve audit start bij een goede planning en afstemming.

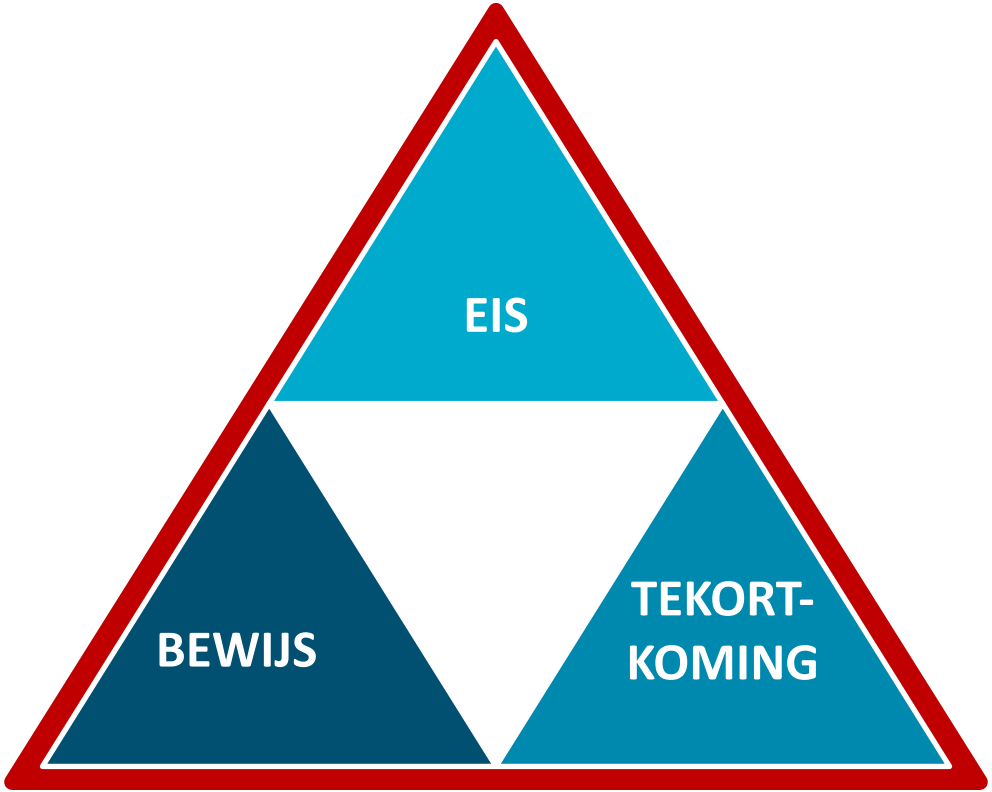

WAT?

WAT AUDITEN JULLIE?

a) SECURITY MANAGEMENTPROCES
b) SECURITY GOVERNANCE
c) ANNEX A – MAATREGELEN
d) RISICOBEHEERSING

WAT?

WAT?



Voorbeeld

WAT

EIS	BEWIJS	TEKORTKOMING
Risico: Tijdens development komen bugs in software terecht, wat kan leiden tot negatieve impact op beschikbaarheid, integriteit, vertrouwelijkheid van het eindproduct.		
In je development policy staat dat elke usecase gereviewd, getest en bevindingen moeten worden opgevolgd, volgens een vastgesteld proces.	Kun je laten zien hoe het proces van review, testen en opvolgen gevolgd wordt tijdens development?	Op basis van een steekproef bewijzen dat de vereiste reviews, tests en opvolging zijn uitgevoerd over een langere periode.
Er wordt aangegeven dat development gedaan wordt op basis van *Development policy_v1.3.pdf*	Uit de steekproef blijkt dat maar een klein deel van de ontwikkelde code is gereviewd en getest, uit de periode dat het beleid van toepassing was.	Uit de steekproef van zes usecases blijkt dat de development policy in vier gevallen niet is nageleefd, zoals is voorgeschreven in de development policy.

TAKE AWAY 3 - WAT?

DUIDELIJK VERWOORDE BEVINDINGEN ZIJN EEN WAARDEVOLLE KANS VOOR JOUW ORGANISATIE OM TE VERBETEREN.

RECAP

WAAROM? *“True added value.”*

HOE? *“What you do is up to you, just do it!”*

WAT? *“All good things come in three.”*

RECAP

WAAROM?
Om inzicht te krijgen in de werking en effectiviteit van jouw risicomanagement en de beheersing van jouw risico's.

HOE?
Een effectieve audit start bij een goede planning en afstemming.

WAT?
Duidelijk verwoorde bevindingen zijn een waardevolle kans voor jouw organisatie om te verbeteren.

WAT GA JIJ VANAF MORGEN (ANDERS) DOEN?


A safe digital journey