Security auditing - Now and in the future

PvIB Event

12 January 2023

EY
Building a better
working world

Agenda

1. What is (the goal of) a security audit?

   Why security auditing?

   How is security auditing performed?

   How can assurance be provided?

2. What security audit standards and frameworks are there?

   Examples of security audit frameworks and standards

   Security auditing of frameworks: what we see in practice

3. What is enough security?

   Historical perspective of car safety

   What is “normal” IT security?

4. Developments impacting security standards and audits

Peter Kornelisse

Marten de Bruin

1 What is (the goal of) a security audit?

Peter Kornelisse

Purpose | Information supporting risk management

How to (security) audit, depends on purpose

- Compliance
- Risk management
- Need for advise
- Demonstrate quality

- Organizations should determine their needs as this affects:
  - Form of the audit
  - Efficiency of the audit
  - Effectiveness of the audit

Audit modes

- Assurance mode
  - Reasonable or limited assurance
  - Mandatory in some situations
- Advisory mode
  - No assurance, mostly reporting of findings and recommendations
  - Often requested when internal expertise is insufficient or independent view is needed
- Certification mode
  - Certificate providing comfort

Assurance involves 3 parties

- Responsible party
- User of the assurance report
- Auditor

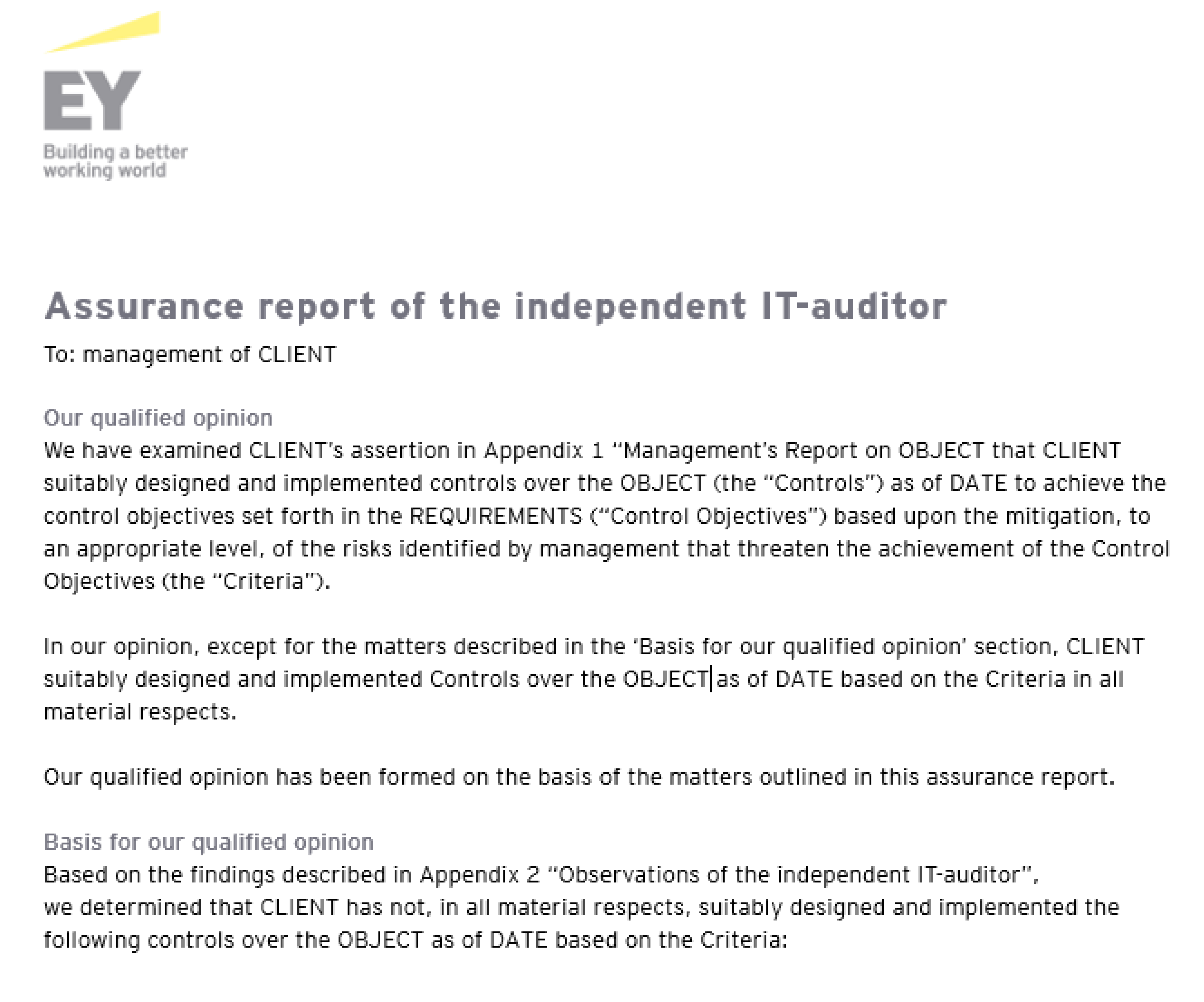
Assurance | Elements of assurance engagements

- Independent third party
- Object of investigation
- Quality elements
- Criteria
- Audit standards, i.e. NOREA-richtlijn 3000
  - A - Attest | D - Direct
- Depth of the audit
  - Design | Implementation | Operating Effectiveness
- Audience | Intended users

Assurance | Results

- **Report to intended users:**
  - Unqualified opinion
  - Qualified opinion
    - Limited
    - Negative
  - No opinion

- **Underlying file**
  - Another auditor should arrive at the same conclusion based on the audit file



EY
Building a better
working world

Assurance report of the independent IT-auditor

To: management of CLIENT

Our qualified opinion

We have examined CLIENT's assertion in Appendix 1 "Management's Report on OBJECT that CLIENT suitably designed and implemented controls over the OBJECT (the "Controls") as of DATE to achieve the control objectives set forth in the REQUIREMENTS ("Control Objectives") based upon the mitigation, to an appropriate level, of the risks identified by management that threaten the achievement of the Control Objectives (the "Criteria").

In our opinion, except for the matters described in the 'Basis for our qualified opinion' section, CLIENT suitably designed and implemented Controls over the OBJECT as of DATE based on the Criteria in all material respects.

Our qualified opinion has been formed on the basis of the matters outlined in this assurance report.

Basis for our qualified opinion

Based on the findings described in Appendix 2 "Observations of the independent IT-auditor", we determined that CLIENT has not, in all material respects, suitably designed and implemented the following controls over the OBJECT as of DATE based on the Criteria:

Independent third party | IT-auditor

- Register EDP-auditor (RE)
  - Audit and advise organizations about the management of their IT
  - Authorized to execute and sign off assurance engagements
  - Knowledgeable in the areas of
    - Information security;
    - IT control, and;
    - Business-IT alignment

- Certified Information Systems Auditor (CISA)
  - ISACA

NOREA | Nature of security objects

Nederland is een voorloper met digitalisering. Hierbij is cybersecurity van cruciaal belang, opdat digitalisering beheerst en veilig kan plaatsvinden.
Denk hierbij ook aan de toenemende ketenafhankelijkheid van organisaties en burgers, evenals het borgen van bescherming van persoonsgegevens. Goede cybersecurity is ook een enabler voor organisaties en haar producten en diensten.

De toenemende digitalisering resulteert in een toenemende gevoeligheid van organisaties voor:

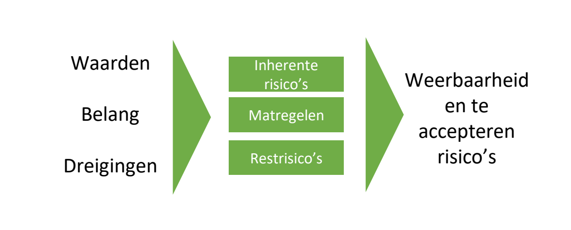
- Vertrouwelijkheid, i.e. persoonsgegevens, intellectueel eigendom;
- Continuïteit, niet alleen van administratieve processen, maar ook productieprocessen, en digitale diensten aan klanten;
- Integriteit van gegevens, zoals die van financiële rapportages.

Dit vraagt ook in toenemende mate om zekerheid over de beveiliging van digitale oplossingen. IT-auditors kunnen deze zekerheid bieden.

Van een organisatie mag worden verwacht dat zij cybersecurity heeft geregeld, op drie niveaus:

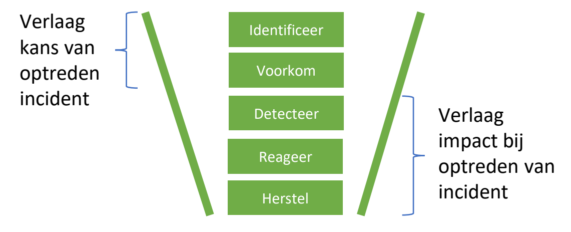
1. Risicogebaseerde keuzen voor cybersecurity door een organisatie

Cyber Risk Management



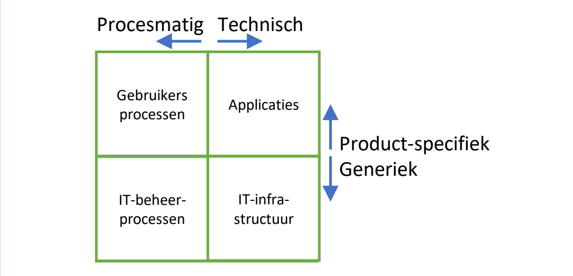
2. Cybersecurity-weerbaarheid van een organisatie

i.e. NIST Maturity level

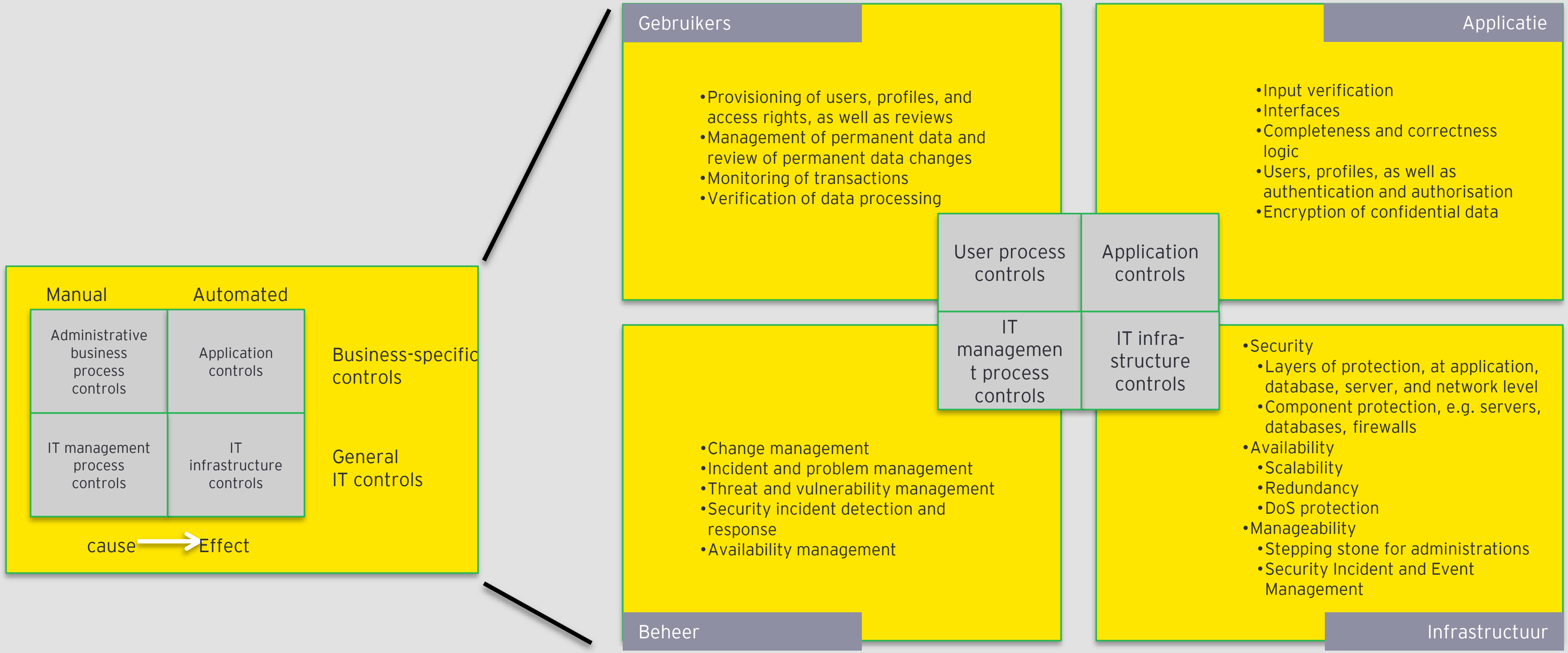

Verlaag kans van optreden incident
Identificeer
Voorkom
Detecteer
Reageer
Herstel
Verlaag impact bij optreden van incident

3. Beveiliging van producten en diensten

i.e. DigiD, SWIFT, en maatwerk



Assurance | Object of audit



Manual	Automated	
Administrative business process controls	Application controls	Business-specific controls
IT management process controls	IT infrastructure controls	General IT controls

cause → Effect

Gebruikers

- Provisioning of users, profiles, and access rights, as well as reviews
- Management of permanent data and review of permanent data changes
- Monitoring of transactions
- Verification of data processing

Applicatie

- Input verification
- Interfaces
- Completeness and correctness logic
- Users, profiles, as well as authentication and authorisation
- Encryption of confidential data

User process controls	Application controls
IT management process controls	IT infra-structure controls

Beheer

- Change management
- Incident and problem management
- Threat and vulnerability management
- Security incident detection and response
- Availability management

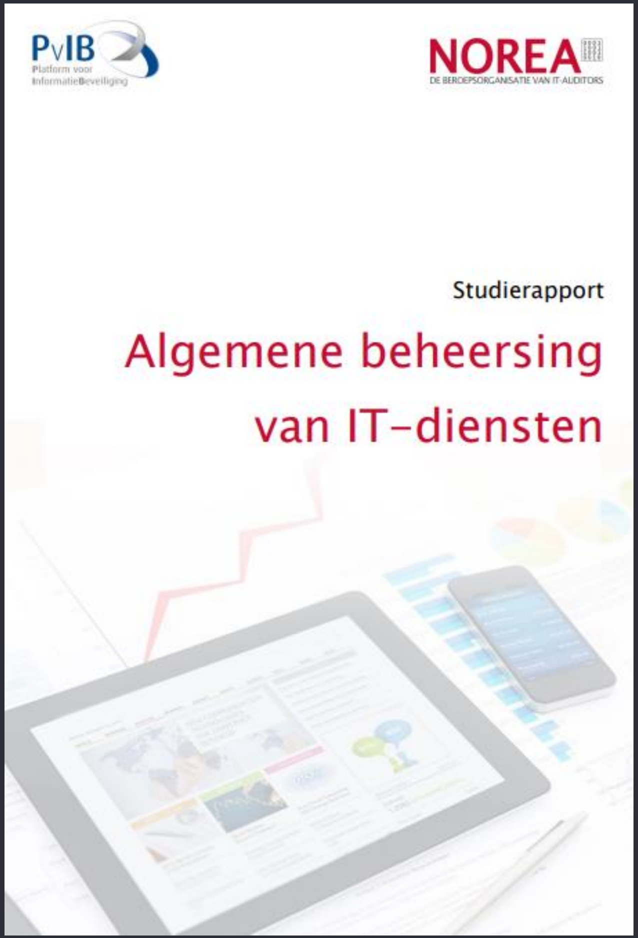
Infrastructuur

- Security
  - Layers of protection, at application, database, server, and network level
  - Component protection, e.g. servers, databases, firewalls
- Availability
  - Scalability
  - Redundancy
  - DoS protection
- Manageability
  - Stepping stone for administrations
  - Security Incident and Event Management

Assurance | Topics

- SNBB – “Standaard Normen voor Beheer en Beveiliging”

IT components (configuration)	IT architecture (coherence)
Identification Authentication Authorization Logging Signaling Via processes - Baselines - Patching - Vulnerabilities management	Zoning Redundancy Identification Authentication Authorization Logging Signaling



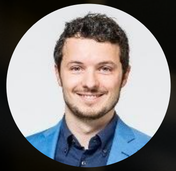
PvIB
Platform voor InformatieBeveiliging

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Studierapport

Algemene beheersing van IT-diensten

2 What security audit standards and frameworks are there?



Marten de Bruin

Examples of security audit frameworks and standards

Baseline Info.bev. Overheid (BIO)

ISO27001 (Security)
NEN7510

ISO27701 (Privacy)

Privacy Framework and WPG (NOREA)

Sector-specific (e.g. TISAX)

SNBB (NOREA)

DigiD

ISA/IEC 62443 (OT)

Webtrust for CA (Public keys)

SWIFT

NIST Cyber Security Framework

NIST 800 series standards

Horizontaal Toezicht

SURF

SOC2 (AICPA) – Focused on service organizations

SOC for Cyber (AICPA) – Cyber Risk Management

PCI DSS (Payment industry)

NIST Ransomware Risk Management

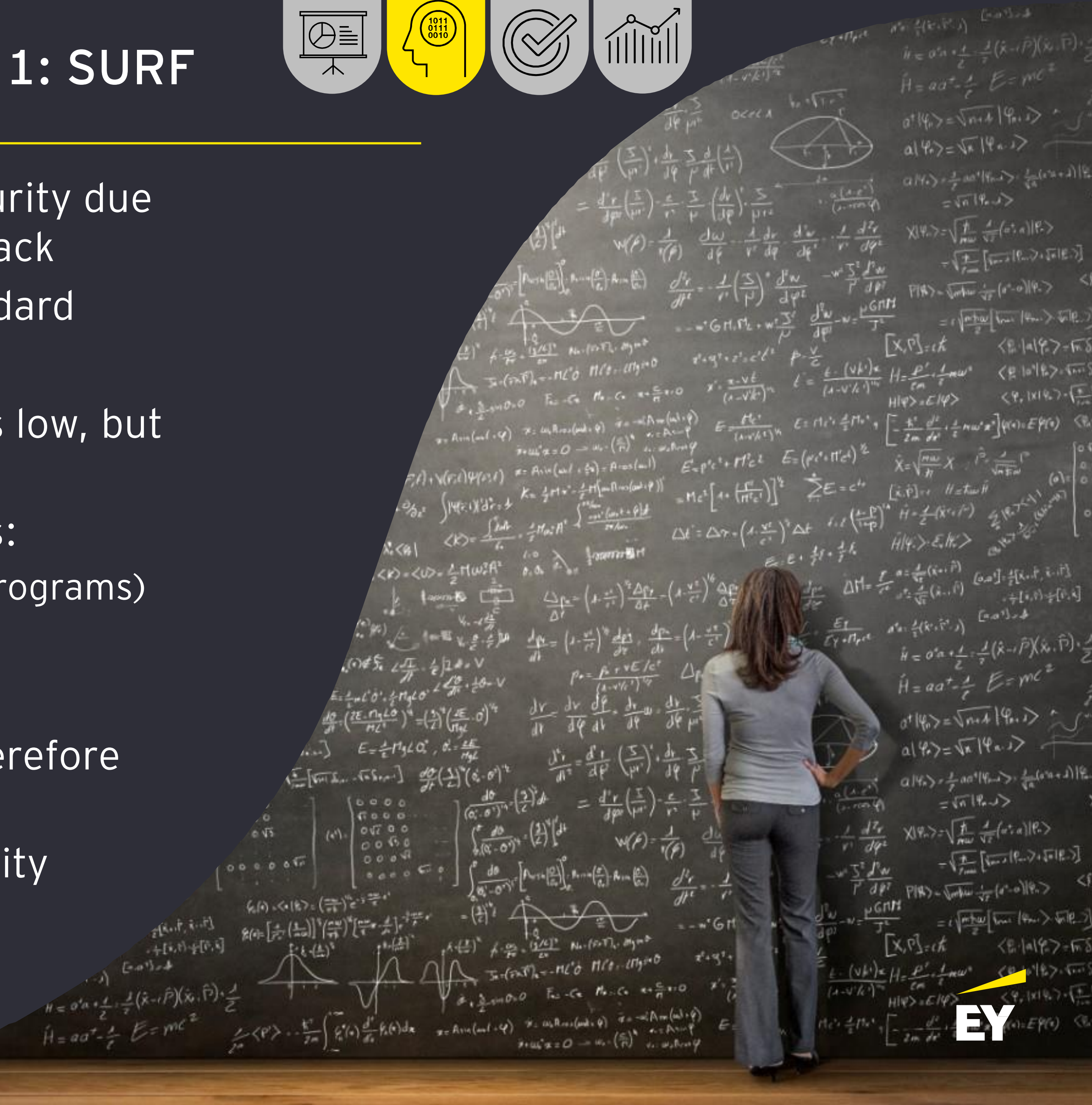
NIS Directive (vital infrastructure)

What we see in practice. Example 1: SURF

- Increased attention to information security due to Maastricht University ransomware hack
- SURF framework as a sector-wide standard

- Overall information security maturity is low, but the goal is to reach level 3 out of 5
- Many improvements over the last years:
  - University-specific (e.g. improvement programs)
  - Sector-wide (e.g. SURF SOC)

- Lack of mature (IT) audit functions, therefore many external audit support
- Sector has a hard time attracting security (audit) personnel



What we see in practice. Example 2: BIO

- BIO standard supersedes the BIR
- Mandatory for various governmental institutions
- Implementation is lagging behind due to:
  - Lack of priority and accountability
  - Lack of expertise
  - BIO is a generic standard that requires local translation and implementation
- Implementation can be considered a one time effort, but maintenance is a continuing effort that requires solid information security governance

What we see in practice. Example 3: SWIFT

- SWIFT is an international banking platform to which many banks and other large organizations are connected
- SWIFT standards applicable to users and suppliers of the SWIFT infrastructure:
  - Customer Security Controls Framework (CSCF)
  - Cyber Security Service Provider program (CSSP)

- Assessment / audit increasingly mandatory (from self-assessment to independent audit)

- Level of compliance is usually high due to criticality of the SWIFT service
- No sanctions for non-compliance yet, but could be in the future

3 What is enough security?

Peter Kornelisse

Normal car safety | Seat belts

First applied by Saab in 1958

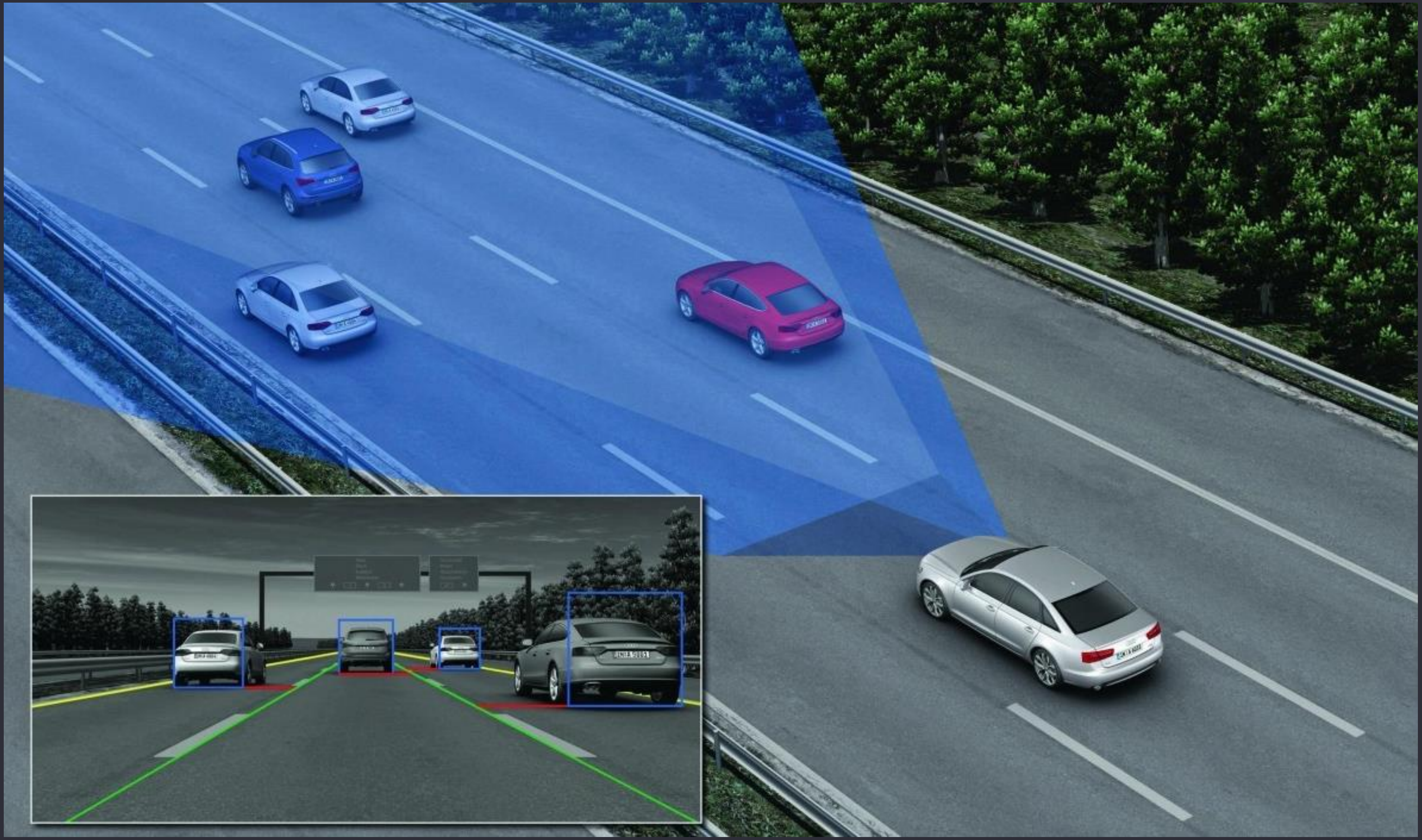
From 1 January 1971 onwards, seat belts are mandatory for driver and seats next to driver connecting to a car door

Normal car safety | Airbags

During the 80s and 90s, airbags became the ‘Normal’

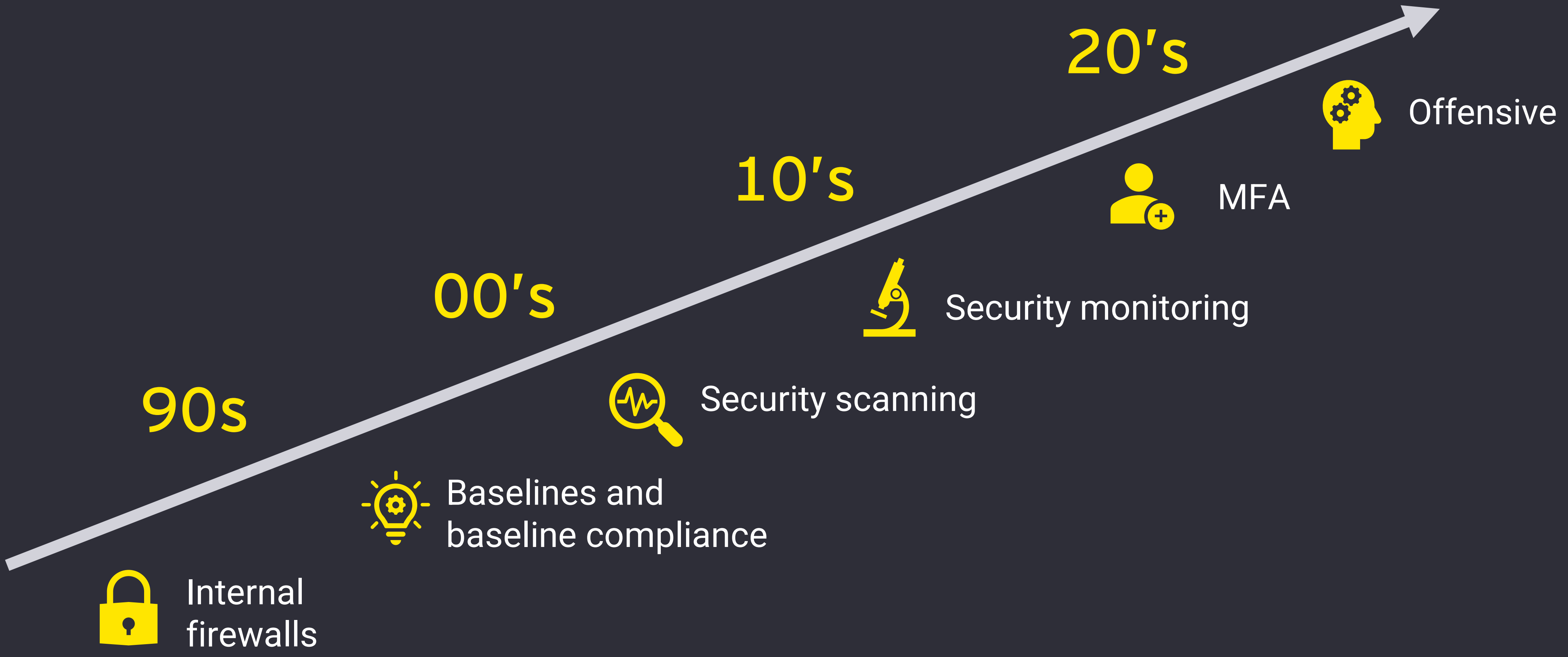
Note that airbags are not legally required !

Normal car safety | Adaptive cruise control



First adaptive cruise control in 1992, becoming ‘normal’ in the 20s

Normal IT Security



90s

Internal firewalls

00's

Baselines and baseline compliance

Security scanning

10's

Security monitoring

MFA

20's

Offensive

Security in historical perspective

'80	'90	'00	'10	'20
Point solutions	**Code of Practice for Information Security**	**Secure IT services**	**Cyber Defense framework**	**Adaptive Security**
Security is add-on	BS7799 -> ISO27001	Security by design	Cyber resilience	Focus on IT-enabled activities and risks Learn and improve

4 Developments impacting security standards and audits

Marten de Bruin

Developments that may impact security audits (1/2)

- **New and revised laws and regulations.** For example:

NIS2 Directive (replacing the NIS Directive)	- Critical infrastructure
RCE (Resilience Critical Entities)	- Critical infrastructure
Cyber Resilience Act (CRA)	- Products with a digital component
Digital Operations and Resilience Act (DORA)	- Digital Finance
AI Act	- Safety framework' around AI risk

- Security standards increasingly used as starting point for information security / mandatory (e.g. NIS1 implementation)

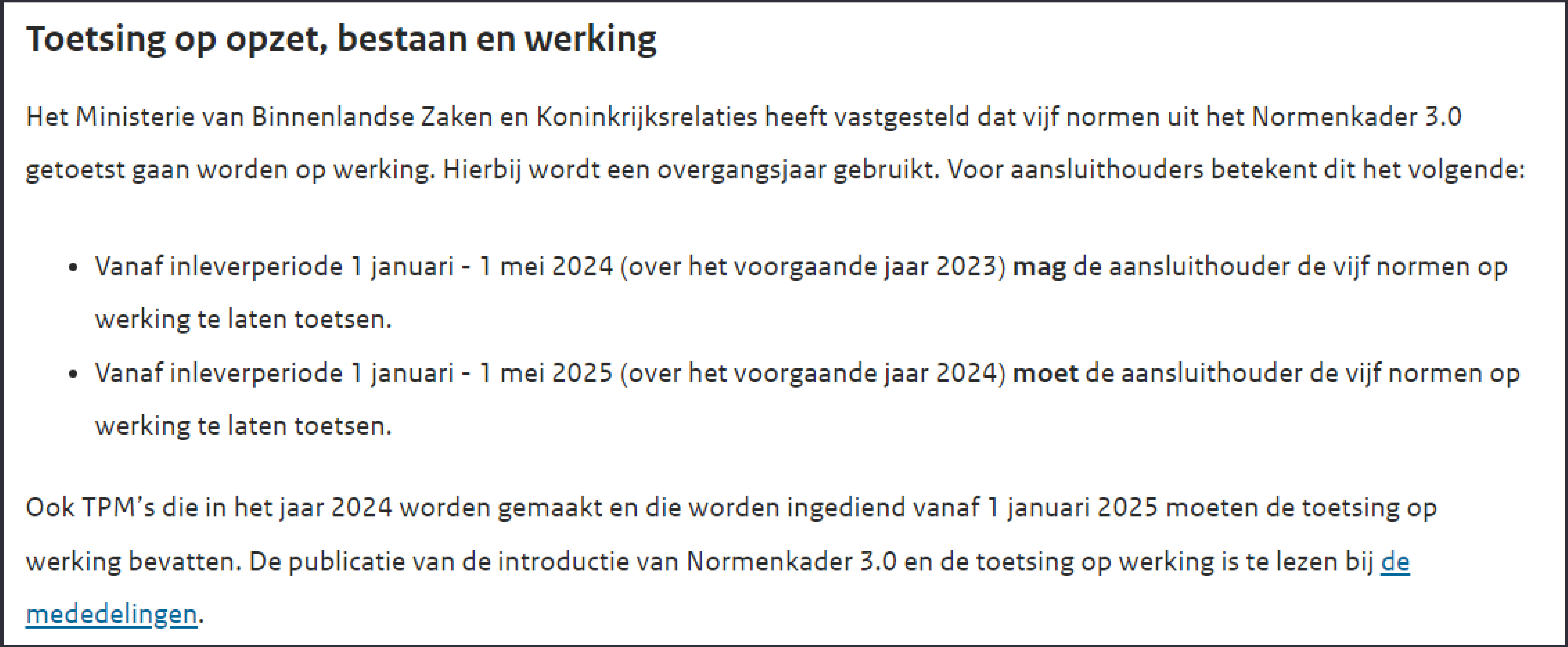
- Increased security awareness (e.g. due to increase in high profile incidents)

- Increased use of third party cloud / IT services (e.g. SaaS), but also security services (e.g. SOC as a Service). Users required to manage their vendors leading to increasing assurance needs

Developments that may impact security audits (2/2)

- **Security auditing increasingly required** due to:
  - Laws and regulations
  - Expectations from stakeholders:
    - Clients (e.g. users of IT services)
    - Banks (security part of financial statements or separate IT audit statement)
    - Society (e.g. civilians expecting proper security)
- Examples are increasing requirements SWIFT and DigiD (operating effectiveness)
- Challenges in the labour market, especially in security functions
  - Need for security professionals is expected to further increase
  - Shortage of security professionals likely to be higher
  - Some sectors (education, healthcare) have a hard time attracting information security staff
  - Increasing demand for external security auditors

Example from practice: DigiD requirements are increasing



Toetsing op opzet, bestaan en werking

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft vastgesteld dat vijf normen uit het Normenkader 3.0 getoetst gaan worden op werking. Hierbij wordt een overgangsjaar gebruikt. Voor aansluithouders betekent dit het volgende:

- Vanaf inleverperiode 1 januari - 1 mei 2024 (over het voorgaande jaar 2023) **mag** de aansluithouder de vijf normen op werking te laten toetsen.
- Vanaf inleverperiode 1 januari - 1 mei 2025 (over het voorgaande jaar 2024) **moet** de aansluithouder de vijf normen op werking te laten toetsen.

Ook TPM's die in het jaar 2024 worden gemaakt en die worden ingediend vanaf 1 januari 2025 moeten de toetsing op werking bevatten. De publicatie van de introductie van Normenkader 3.0 en de toetsing op werking is te lezen bij de mededelingen.

5 Questions?