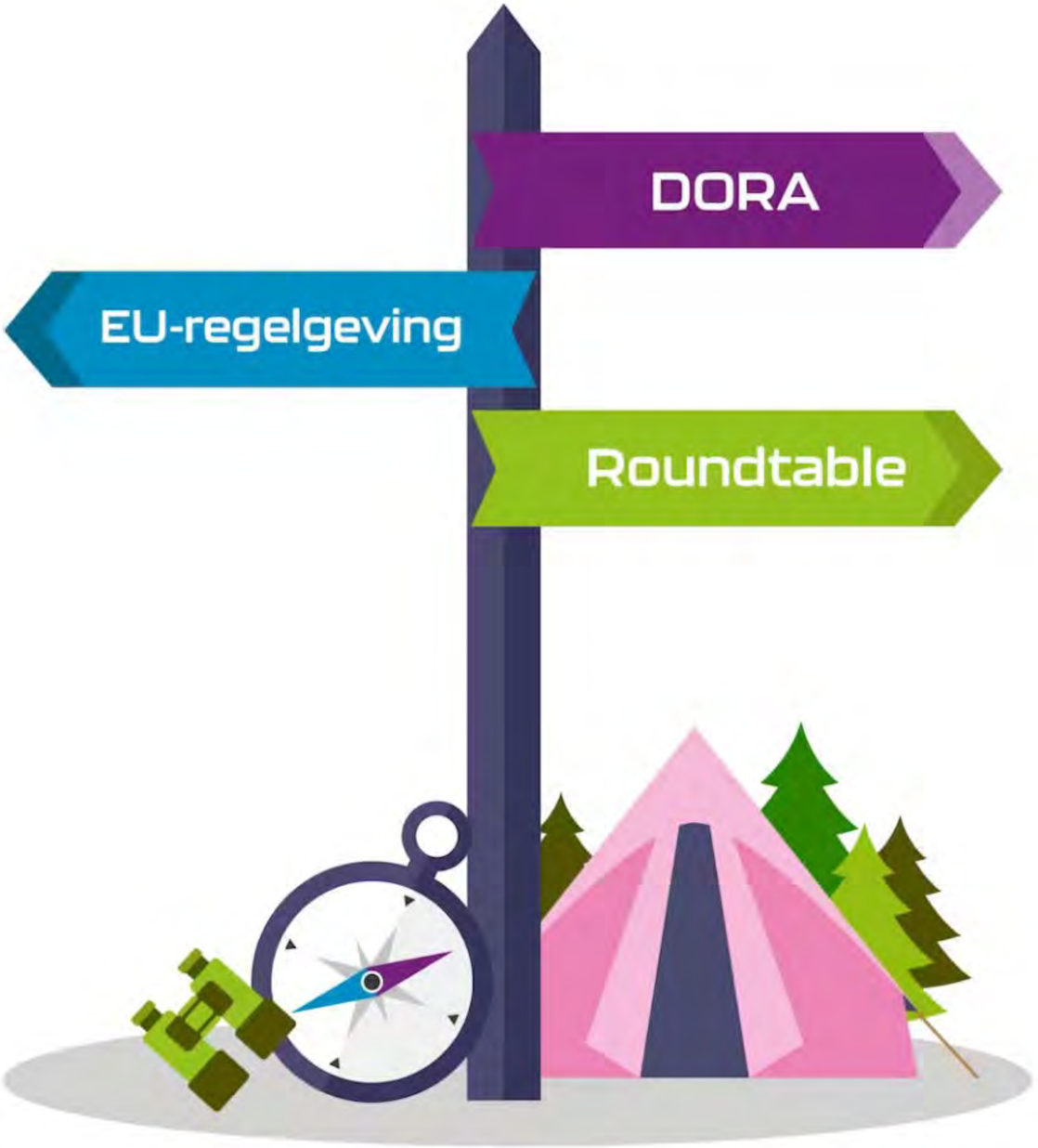
# Instructions

# DORA Explored

26 oktober 2023



## CYBERSECURITY AND DATA SECURITY

### Auditing at the speed of crime

**With hackers now able to threaten critical infrastructure and people's lives, internal auditors must move faster than ever to combat threats.**

Cybersecurity and data security retained its hold as the number one threat in the Risk in Focus 2023 survey – with 82% of respondents saying it was a top five risk (the same as in 2022). It is also the area in which internal auditors say they spend most time and effort. In three years' time, internal auditors expect the risk to still rank highest as a threat to their organisations but with slightly fewer ranking it a top five risk (79%).

In fact, the threat landscape has become more dangerous – not least because of the war in Ukraine. Survey respondents said cybercrime and data security was their second biggest risk from the conflict. In addition, ransomware attacks increased by 80% in 2022, according to cyberthreat analyst Sophos[1]. That growth was driven in part by hackers taking advantage of the burgeoning ransomware-as-a-service industry. The average price for recovering stolen data soared from $170,000 per infringement to $812,360, according to the survey. Hackers are also moving into the more ominous area of so-called "killware" to put pressure on organisations to pay up – those attacks target critical infrastructure, such as hospitals or energy supplies, which could result in actual deaths.

Chief audit executives at the Risk in Focus 2023 roundtable on cyber and data security agreed that ransomware risk continues to be difficult to mitigate and poses a potential existential threat to businesses. "A major data breach can impact on the quality of our services, trust and reputation, our financials and, if our clients lose money, we have to compensate them," said one chief audit executive. "But the biggest threat we are scared of is that we cannot keep our business running."





## CYBERSECURITY AND DATA SECURITY

### Cybercrime business models maturing

"The maturation of business models around cybercrime is becoming a major threat," the chief audit executive of an international IT company says. He says that the ability of low-skilled hackers to buy sophisticated off-the-shelf attacks should be on every internal audit team's radar. "It is now an open battlefield and auditors should ensure they keep up-to-date on the main evolutions in cyber-attack strategies." While technicians are best placed to develop and deploy defences, he says, internal auditors should help to effectively spread new counter measures and advice from those teams throughout the organisation.

"Every day, this issue becomes more rather than less important," said another chief audit executive at the Risk in Focus 2023 roundtable on the issue. "It has all the characteristics of an emerging risk, which are often the most difficult to tackle. This year, for example, we could face increased Russian cyber-attacks, next year it could be something else. It is the biggest risk we have."

### Raising board awareness

Auditors must help to connect the dots between what is going on in the business and the board. A qualitative survey by the UK government earlier this year uncovered limited board understanding of cybersecurity risk[2]. This had led, it said, to efforts to pass on the risk to outsourced cyber providers, insurance companies or even non-board level colleagues.

Risk in Focus 2023 roundtable participants agreed it could be difficult to find board time for IT-related topics, including cybercrime, despite the fact the pandemic had pushed digitalisation efforts further up the agenda. In last year's Risk in Focus survey, for example, the threat from digitalisation ranked third – compared with fifth this year.

"I participate in both risk and audit committees," said one chief audit executive at a financial services firm, "and while we talk a lot about lending, compliance and credit risk, we don't discuss IT." That was left to a separate meeting with the chief information officer and those in the second lines.

An internal audit presence at IT security committees, or with chief information and security officers[3], is effective for driving better security, but board-level engagement is key. Chief audit executives can play a major role in raising awareness of cyberthreats in board rooms. They should explain how much money their organisations stands to lose when specific risks crystallise – and avoid cloaking the topic in technical jargon.





## CYBERSECURITY AND DATA SECURITY

### Third parties create weak links

While many large organisations are relatively well-protected by strong cyber defences and regular up-to-date training, this year has seen more of a shift to hackers targeting third-party suppliers with less mature security systems. Yet European legislation such as the General Data Protection Regulation[4] and, more recently, guidance by the European Banking Authority, place responsibility squarely on the shoulders of the organisation that owns the data[5]. This trend is likely to continue to grow under Europe's revised cybersecurity directive, NIS2[6]. Like many new emerging risks, identification, control and mitigation lies partly outside of the business' remit.

Those concerns extended to cloud service providers, especially since many organisations have signed up to the same few major businesses to accelerate their digitalisation plans. Given that the levels of service are standardised by each provider, chief audit executives said that organisations often had little negotiating power to agree or force controls on those suppliers. "Everything becomes a bit too far from our site from an internal audit point of view and it can be hard to assess and mitigate risk."

Greg Schlegel, founder of the Supply Chain Risk Consortium in the US and Adjunct Professor for teaching enterprise risk management for Villanova University's EMBA programme, says that internal auditors must focus on such third-party risks over the next twelve months – even though the time internal auditors spend on supply chain issues is likely to fall from sixth to nineth place, according to Risk in Focus 2023 survey. While he accepts that data security is a key issue in terms of protecting the organisation's digital assets and infrastructure, auditors should also ensure that the cloud service providers (and others who supply critical data infrastructure) are financially secure.

**"The biggest threat we are scared of is that we cannot keep our business running"**

"The business needs some methodology to assess the financial health of third-party suppliers because the world at the moment is a very uncertain place, especially with inflationary pressures and energy supply risk increasing," Schlegel says. He also advises internal auditors to ensure that the business knows where suppliers are located physically. While software security is often framed in terms of the cloud, if the sites where those services are based become subject to power outages – such as the one at Amazon Web Services in 2021[7] – that could bring an organisation's critical infrastructure to a halt.





## CYBERSECURITY AND DATA SECURITY

### Controls must be implemented

Not only did the pandemic weaken many organisations' cyber defences as staff were forced to work at home, the culture around data security also deteriorated. As online communication became the norm, one of the hacker's favourite weapons of choice – the spoof email – was less easy to detect as most correspondence moved online.

Foyle said that audit controls should include training and alerts so that people become more aware of the latest hacks. "Quite simple things, such as always hovering over email to make sure it is one that you recognise or would expect to see, can make a difference," she says.

Also, applying risk frameworks with policies and procedures, including ISO 27100, NIST and COBIT are a must. But they are not enough. "We have excellent IT policies and standards that follow best practice – but the simplest error is that people often fail to implement them," said one chief audit executive at the Risk in Focus 2023 roundtable event.

While larger organisations tend to have specialist cyber security expertise in-house, general internal auditors can make a big difference by refocusing on the basics. That includes the security culture of the organisation, which a Chartered IIA UK and Ireland study found was often a blind spot for internal auditors and businesses[8].

## CYBERSECURITY AND DATA SECURITY

### More dangerous

But the unfortunate truth is that the online world is now more dangerous. First, hacking has professionalised and commercialised and many attacks are more sophisticated - a trend discussed in Risk in Focus 2023. In the UK, for example, British Airways, Boots, and the BBC were among businesses infiltrated by a ransomware outfit through their payroll provider's software.[1] Second, state-sponsored actors are using so-called wiper attacks to breach cyber defences and destroy the affected organisations – these are rare but have increased in frequency since the war in Ukraine.

Third, as wars are increasingly waged both online and on battlefields, organisations must assess how geopolitical events could not only damage businesses, but also critical infrastructures. One Swedish CAE at the report's roundtable said cyberattacks spiked immediately after the government announced its intention to join NATO: another saw increased activity after a major product launch. In addition, threats to the global underwater network of cables that carry much of the internet could also increase, highlighting how cyberattacks have been weaponised.

Fourth, many organisations have moved to the cloud, digitalised their operational technologies, and integrated with suppliers. The so-called "attack surface" of businesses is broader as a result – there are more ways in. Finally, emerging technologies, such as the generative AI program ChatGPT and blockchain offer both important new business opportunities at the same time as adding speed, complexity and additional risk exposures. For example, malware can test an organisation's security patching status and then request AI to generate an attack that targets specific vulnerabilities. Because such hacks can exploit legitimate software, they can be difficult to defend against. By 2027, CAEs said that digital disruption, new technology and AI would be their organisations' 4th biggest risk, potentially increasing cyber threats further.

### Fundamentals

"We invest a lot in making sure we keep the known risks under a tight grip with new controls and security measures," a CAE from a Swiss-based financial services firm said at the roundtable, "but the biggest challenge now is what we should invest in to identify and tackle the unknown cyber and data risk exposures." Given that cybersecurity and data security sit at the centre of the turbulent meeting place of many interconnecting risks – from geopolitical uncertainty to digital disruption – constant vigilance and control innovation is a must.

> "The biggest challenge now is what we should invest in to identify and tackle the unknown cyber and data risk exposures."





## CYBERSECURITY AND DATA SECURITY

### More regulation

Since COVID-19, organisations have got better at cyber risk fundamentals: strengthening perimeter defences, monitoring network activity, patching updates, penetration testing, and even employing ethical hacking on both internal systems and online services. Security automation means that AI programs can monitor threats by scanning patterns of activity rapidly and accurately across entire networks. To combat people risk – a huge challenge in a world of ubiquitous digital communication and social media – businesses regularly conduct awareness training and assess the maturity of their cybercultures by measuring response rates to spoof phishing campaigns.[2] Most organisations are also assuming that a major hack will occur. Advanced recovery solutions include ensuring that the systems that underpin critical activities can be rebuilt from scratch in case hackers have corrupted the organisation's backups.

> "Firms must address any 'reasonably identifiable' IT risk that could compromise enterprise networks"

The requirements mandated by legislation such as General Data Protection Regulation are being extended by rules such as the EU's Data Act, EU Cyber Resilience Act, NIS2, and Digital Operational Resilience Act (DORA)[3] – to name a few. These initiatives provide CAEs with a platform to reinforce the importance of good cyber security and data practices, and they are helping to create a common language of risk around the topic.

DORA, for example, which affects financial entities in the European Union, explicitly states that firms must address any "reasonably identifiable" IT risk that could compromise enterprise networks. That could include anything from updates from intelligence agencies to known shortcomings of ChatGPT-style apps – potential data leaks and inbuilt biases. CAEs at the roundtable were both experimenting with such apps and admitted not knowing whether staff in other parts of the enterprise used them. In addition, since DORA applies to suppliers too, financial organisations will have to reassess their due diligence processes around nth party cyber risk.





## CYBERSECURITY AND DATA SECURITY

More broadly, NIS2 Directive sets a new mandatory level of measures (effective October 2024) aimed at preventing cyber incidents. Those include policies on risk analysis, information security, cyber security training, multi-factor and continuous authentication solutions. The idea is to standardise measures across Europe at the same time as imposing fines for non-compliance.

### The role of internal audit

Boards and CAEs must both ensure they are ready for compliance across a wide spectrum of requirements and use those rules to further improve resilience. The Risk in Focus 2024 survey suggests some of that effort is going into business continuity, operational resilience, crisis management, and disaster response - which ranked in 4th place in terms of where internal audit spends its time this year - up from 5th place in 2023.

One CAE at the roundtable used the certification process for ISO 27001[4] to develop a very detailed business continuity plan for the specific cyber risks the organisation faced. "Behind the certification there is a strong focus on risk monitoring, risk management activities, and, in particular, identifying exactly which equipment, factory, operation, and application is vulnerable and how to fix it," he said. "From there, you can plan your BCP in detail and construct scenarios that you can test." The lessons learned from those scenarios can then be used to improve responses further.

> "Attracting and retaining people with the right technical and security expertise is a big, expensive problem to solve"

Securing operational technology from threats is key. Because of higher levels of digitalisation and automation, internal auditors must view their organisation's cyber and data risks through an IT lens. One CAE based at a German multinational healthcare company at the roundtable said that she had worked with the first and second lines to redefine in detail the company's risk domains by paying close attention to its digital infrastructure.[5] In each of these areas, CAEs are seeking as much detail and specificity as possible to identify gaps and strengthen controls. The board's strategy at one German media business, for example, has been to drive the three lines[6] to co-ordinate efforts on cyber and data security, said its CAE in an interview for this year's report. Given the switch to digital operating models, he said that in three years' time, most internal auditors should be trained IT security specialists at the business.

"But attracting and retaining people with the right technical and security expertise is a big, expensive problem to solve," he said.





## CYBERSECURITY AND DATA SECURITY

To do so, he has focused on building a team that concentrates more on hardcore technical issues and less on compliance – something smaller audit functions must co-source to achieve. But that has helped attract talent, such as new chief information security officer (CISO) (himself a former IT auditor), to the business – and to go more granular on recommendations. "The key is to go beyond your average compliance audit and provide actual risk-based technical assessments of the environment and engage in frank, technical discussions with the auditees in a language they understand," the CAE said.

Raising the profile of the CISO and working closely across all lines of assurance is crucial. But CAEs must ensure that risks identified by CISOs are clearly quantified in terms of business risk and communicated clearly to the board or its equivalent.

### How can internal audit help the business?

1. Assess how well the organisation complies with relevant cybersecurity laws, regulations and industry standards and is prepared for the impact of upcoming rules
2. Assess how far risk taxonomies and controls on cybersecurity and data security for digital operating systems are aligned across the three lines
3. Assess how effectively the three lines (including the CISO) are working together and with the board
4. Evaluate the effectiveness of cybersecurity controls in the first and second lines and for the organisation's key assets
5. Assess whether the organisation is conducting adequate vulnerability assessments to identify potential entry points for cyberattacks and weaknesses
6. Assess the effectiveness of the business' ongoing monitoring processes to track and assess its cybersecurity posture
7. Assess the effectiveness of the organisation's incident response and recovery plans and its capabilities to execute it
8. Evaluate the organisation's cybersecurity awareness and training programmes and assess whether those produce the desired outcomes
9. Assess how vulnerable backup data is to corruption and whether the organisation has the capability to rebuild its systems at speed from scratch
10. Assess whether senior management and the board are sufficiently informed and show serious commitment to cybersecurity

## Contents





# Looking ahead

## What are the top 5 risks you expect internal audit to spend the most time and effort addressing three years from now?

**Internal auditors expect to spend significantly more time on human capital, climate change and digital disruption, while organisational governance and business continuity are among the areas that will ease.**

# WARNING !!!

**'De volgende beelden kunnen als schokkend worden ervaren'**

## Annual cost of Cybercrime in 2023: $ 8 trillion

# WARNING !!!

Centraal Bureau voor de Statistiek

Waar ben je naar op zoek?

Cijfers ▾ Arbeid en inkomen ▾ Economie ▾ Maatschappij ▾ Regio Over ons

Home

Deel deze pagina

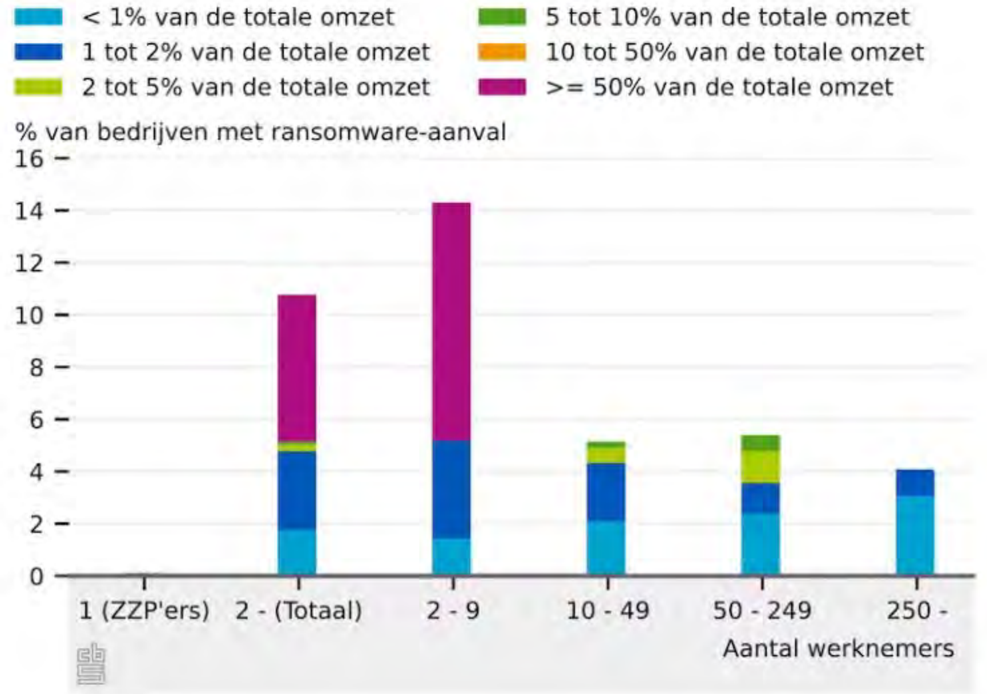
## Cybersecuritymonitor 2022

4-8-2023 00:00

© Hollandse Hoogte / Patricia Rehe

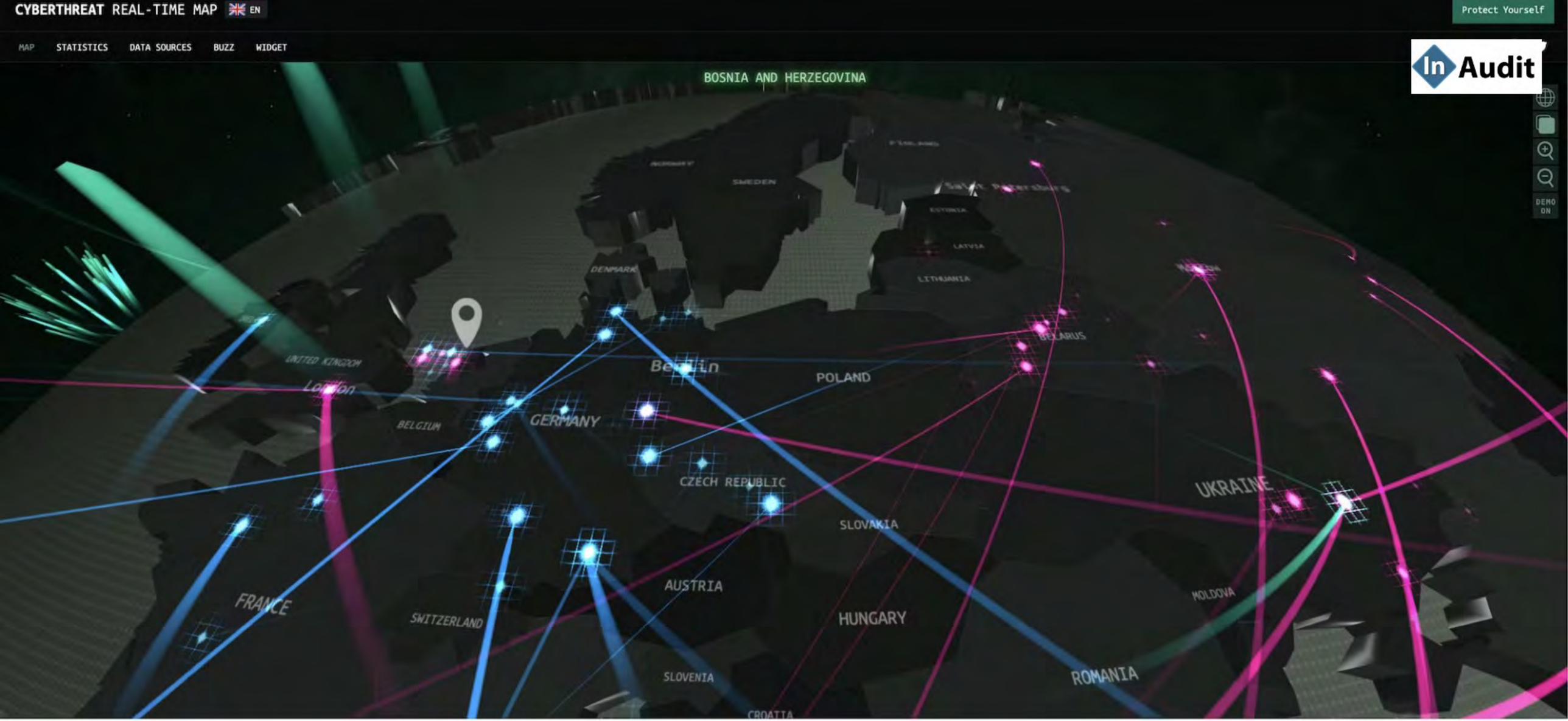
**3.1.11 Percentage van bedrijven met een ransomware-aanval die losgeld betaald hebben per grootteklasse (a) en bedrijfstak met 2 of meer werknemers (b). De percentages zijn opgesplitst naar de hoogte van het losgeld als percentage van de totale omzet.**

**(a) Grootteklasse**




In Audit
Audit Services


DORA
EU-regelgeving
Roundtable




https://cybermap.kaspersky.com

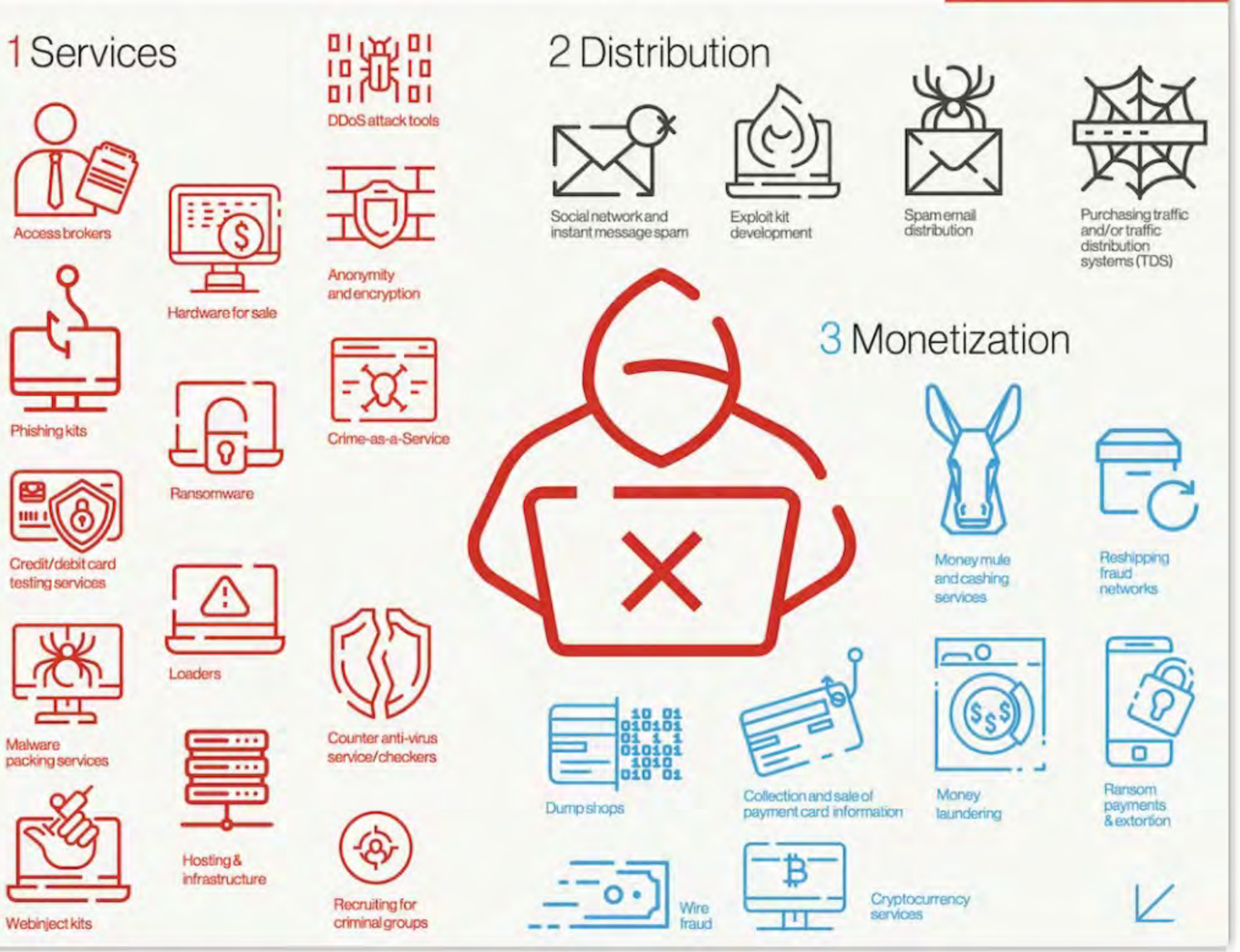
# eCrime ecosystem

A tectonic shift toward big game hunting has been felt across the entire eCrime ecosystem. Ransom payments and data extortion became the most popular avenues for monetization in 2020.

While many established criminal actors still operate out of Russia and Eastern Europe, the complete ecosystem is truly global, with newly uncovered marketplaces arising and maturing in Latin America, Asia, Middle East and Africa.

Many criminal actors develop relationships within the ecosystem to acquire access to essential technology that enables their operations or maximizes their profits.

Although the methods used for malware distribution largely remain the same, criminal actors are finding novel ways to bypass security measures.



NOS Nieuws Sport Live Programma's


NOS Voetbal • Dinsdag 12 september, 09:09

## KNVB betaalt losgeld aan hackers om vertrouwelijke gegevens te beschermen

De KNVB heeft losgeld betaald aan cybercriminelen die in april persoonsgegevens hebben gestolen van de voetbalbond. De hackersgroep LockBit gebruikte hierbij gijzelsoftware. Volgens RTL Nieuws was de eis ruim 1 miljoen euro. De KNVB wil niet zeggen om hoeveel geld het gaat.

De KNVB deelt het nieuws in een advertentie in twee landelijke kranten en in een bericht, waarin ze mensen waarschuwen dat hun gegevens mogelijk in handen zijn van die criminelen. De bond zegt het betalen van losgeld een moeilijke keuze was, maar dat er uiteindelijk "onder deskundige begeleiding afspraken" met de hackers zijn gemaakt. De bond is er nog niet helemaal gerust op dat de criminelen na het krijgen van het losgeld de gegevens ook echt niet zullen verspreiden en roept mogelijke gedupeerden op om extra alert te blijven op misbruik van hun gegevens.

"Mogelijk buitgemaakte bestanden bevatten persoonsgegevens waarvan de verspreiding gevolgen kan hebben voor de persoonlijke levenssfeer van betrokkenen. Het voorkomen van een dergelijke verspreiding weegt voor de KNVB uiteindelijk zwaarder dan het principe om ons niet te laten afpersen", licht de bond toe.

https://nos.nl/artikel/2490181-knvb-betaalt-losgeld-aan-hackers-om-vertrouwelijke-gegevens-te-beschermen

MENU De Telegraaf Abonneer

NIEUWS / BINNENLAND

Lees voor

## Alkmaar trapt in mail met neprekening en betaalt ruim 2 ton

14 sep. 2023 in BINNENLAND

**DEN HAAG - De gemeente Alkmaar is opgelicht door een cybercrimineel. Die deed zich voor als directeur van een organisatie en stuurde een rekening. De gemeente trapte erin en betaalde ten onrechte een bedrag van 236.000 euro. Andere valse rekeningen zijn na de ontdekking meteen tegengehouden, waardoor de schade niet nog verder opliep.**

fd. Mijn nieuws Net binnen Beurs Krant Podcasts

29 aug 11:12

## Kendrion doelwit van beruchte cyberbende LockBit

Heiko Jessayan


Het kantoor van Kendrion, producent en leverancier van hoogwaardige elektromagnetische systemen en componenten voor de industrie, in het Vesta-gebouw in Amsterdam-Zuidoost. Foto: Dijkstra/ANP

**In het kort**

- Industrieel technologieconcern Kendrion is doelwit van gijzelsoftware van cyberbende LockBit.
- De cybercriminelen dreigen op 2 september gevoelige bedrijfsinformatie te publiceren.
- Onbekend is nog wat LockBit precies van Kendrion eist.

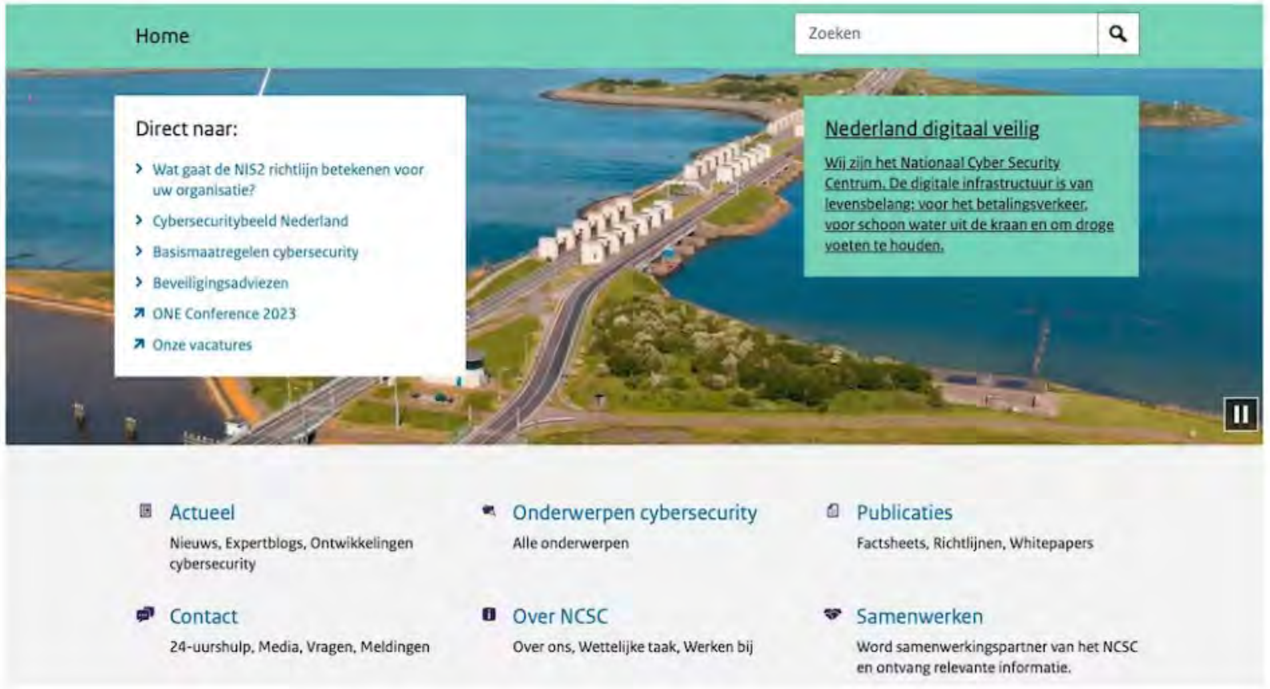
Kendrion KENDR: €13,22 +0,15% , de Nederlandse industrieel toeleverancier van hoogwaardige technologische componenten, is sinds zondag doelwit van gijzelsoftware van de beruchte cyberbende LockBit. Dat bevestigt de ceo van Kendrion, Joep van Beurden, dinsdag desgevraagd nadat de onderneming een persbericht had doen uitgaan over een 'cyber security-incident' door een 'ongeautoriseerde derde partij' die zich toegang heeft verschaft tot de computersystemen van de onderneming.

https://fd.nl/bedrijfsleven/1487239/kendrion-doelwit-van-beruchte-cyberbende-lockbit

In Audit

In Audit
Audit Services

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid




digital trust center.

Ministerie van Economische Zaken en Klimaat

In Audit


*Digital Trust Center helpt jouw organisatie met advies en tools om veilig digitaal te ondernemen.*

### De 5 basisprincipes

Volg de 5 basisprincipes van veilig digitaal ondernemen om de cyberweerbaarheid van je bedrijf te vergroten.

### Informatie & Advies

Informatie en adviezen om zelf aan de slag te gaan met de cyberweerbaarheid van je onderneming.

### Samenwerkingen

Een landelijk dekkend stelsel van samenwerkingen op gebied van cyberweerbaarheid.

In Audit
Audit Services

An official website of the European Union How do you know?

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Search for resources, tools, publications and more

English (en)

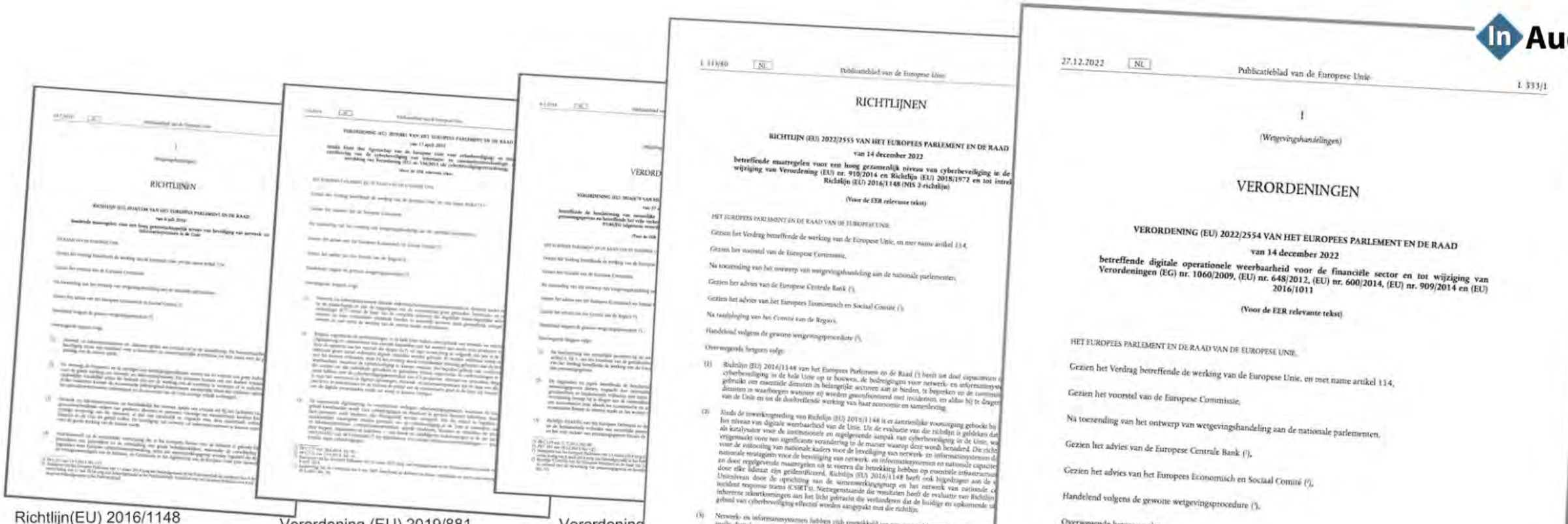
TOPICS PUBLICATIONS TOOLS NEWS EVENTS ABOUT WORK WITH ENISA CONTACT

Home › About ENISA › About › Over Enisa – het Agentschap van de Europese Unie voor cyberbeveiliging

# Over Enisa – het Agentschap van de Europese Unie voor cyberbeveiliging

Naar een betrouwbaar en cyberveilig Europa

*Het Agentschap van de Europese Unie voor cyberbeveiliging, Enisa, streeft ernaar **een hoog niveau van cyberbeveiliging in heel Europa te bereiken.***




Richtlijn(EU) 2016/1148
(NIS Directive)

Verordening (EU) 2019/881
(Cybersecurity Act)

Verordening
(AVG – Algemene Verord

Richtlijn (EU) 2022/2555
(NIS2 Directive)

- ✓ Digital Markets Act
- ✓ Digital Services Act
- ✓ EU Data Governance Act
- ✓ EU Data Act

Verordening (EU) 2022/2554
(Digital Operational Resilience Act)

In Audit
Audit Services


Good practice
Informatiebeveiliging 2023
DeNederlandscheBank
EUROSYSTEEM

# DORA en Cyberrisico

Jan-Willem Zeijen

26 oktober 2023

TRIPLE A
RISK FINANCE

# Wat is DORA?

- Digital Operational Resilience Act
- Europese regelgeving
- Door 4 toezichthouders (ESAs)

- Bescherming van netwerken en informatiesystemen
- Weerbaarheid tegen cyber-dreigingen financiële sector
- Consumentenbescherming en financiële stabiliteit

- Hoe ziet dat er uit?

# Tijdslijn DORA

- Level 1: Verordening van kracht sinds 16 januari 2023
- <11 september 1e batch consultatie (4-tal RTS + 1 ITS)
- Submissie EC per 17 januari 2024
- Eind 2023 2e batch consultatie
- Submissie EC per 17 juli 2024
- Implementatie 17 januari 2025

VERORDENINGEN

VERORDENING (EU) 2022/2554 VAN HET EUROPEES PARLEMENT EN DE RAAD

van 14 december 2022

| ICT risk framework (Chapter II) | ICT related incident management classification and reporting (Chapter III) | Digital Operational Resilience Testing (Chapter IV) | Third-party risk management (Chapter V.I) |
|---|---|---|---|
| • **RTS on ICT Risk Management framework (Art.15)**<br>• **RTS on simplified risk management framework (Art.16.3)**<br>• Guidelines on the estimation of aggregated costs/losses caused by major ICT related incidents (Art. 11.1) | • **RTS on criteria for the classification of ICT related incidents (Art. 18.3)**<br>• RTS to specify the reporting of major ICT-related incidents (Art. 20.a)<br>• ITS to establish the reporting details for major ICT related incidents (Art. 20.b)<br>• Feasibility report on further centralisation of incident reporting through the establishment of a single EU hub for major ICT-related incident reporting (Art. 21) | • RTS to specify threat led penetration testing (Art. 26.1) | • **ITS to establish the templates of register of information (Art.28.9)**<br>• **RTS to specify the policy on ICT services performed by third-party (Art.28.10)**<br>• RTS to specify the elements to determine and assess when sub-contracting ICT services supporting a critical or important function (Art.30.5) |
| | | | **Oversight framework (Chapter V.II)**<br>• Call for advice on criticality criteria (Art. 31.8) and fees (Art. 43.2) DL: 30 Sept 2023<br>• Guidelines on cooperation ESAs – CAs (Competent Authorities) regarding DORA oversight (Art. 32.7)<br>• RTS on harmonisation of oversight conditions (Art. 41) |

**Bold = policy mandates with deadline 17 January 2024 (first batch)**

# Is DORA noodzakelijk? – Invalshoeken

**Ekelmans Advocaten (interview VvV):**
"Vergis je niet, als je ziet hoeveel schade cyberincidenten berokkenen, dan schrik je je kapot. Dat loopt wereldwijd echt in de miljarden en dan heb ik het nog niet eens over de bedrijfsschade, omdat het bedrijf dagen of weken platligt. Reken maar eens uit wat het kost als een verzekeraar een compleet nieuw ICT-systeem moet bouwen, omdat het oude na een hack niet meer kan worden hersteld. Ieder bedrijf moet zijn eigen systemen op orde hebben.

Dora is niets meer of minder dan een logische reactie op alle dreigingen die er zijn."

**VvV (reactie op consultatie):**
"Zorg voor proportionele en op risico's gebaseerde DORA-regelgeving die past bij de specifieke omvang en risico's van verzekeraars"
"maatregelen die operationeel én financieel uitvoerbaar zijn"

**DNB:**
"DORA bevat stringentere normen dan de huidige Guidelines en Good Practices"
"DNB vraagt instellingen en hun uitvoeringsorganisaties de ontwikkelingen rondom DORA adequaat te vertalen naar impact op haar eigen organisatie en die van haar uitbestedingspartners en zich tijdig op DORA voor te bereiden."

# EIOPA – Financial Stability Report (juni 2023)

- **EIOPA (Financial Stability Report juni 2023):**
  - "Digitalisation has become a major trend in the insurance industry. Despite its benefits it also creates potential risks for insurers, particularly in the form of cyber-attacks."
  - "The results of the January 2023 EIOPA Risk Dashboard show digitalisation and cyber risks at a medium level with no change in the last 3 months. The materiality assessment of these risks for insurance by supervisors remains unchanged with cyber security and hybrid geopolitical conflict as main concerns"
  - "When considering the expected developments in terms of risk materiality over the next year, digitalization and cyber risks are ranked first."
  - "Until the DORA rules apply , EIOPA will continue to promote an effective exchange of information with national supervisors on cyber security and cyber-incidents"
- **EIOPA Methodological principles of insurance stress testing of cyber risk:**
  - Operational resilience testing, as required under the Digital Operational Resilience Act (DORA), is not in the scope of the current paper.

# Enkele voorbeelden

- "Cloud outage"
  - Outage time: Intern of extern data center?
- Ransomware
  - Business processes: buiten werking en herstel nodig
  - Hersteltermijn
- Denial of Service (DoS)
  - Business processes
  - Outage time
- Data breach (vb. Australische zorgverzekeraar)
  - % gevoelige data die is kwijtgeraakt
- Power outage (aanval energie centrale)
  - Outage time

- Allianz Risk Barometer 2023:
  - Top risks for small- and mid-size companies:
  - "Many smaller companies continue to be under the misconception that cyber-attacks won't happen to them but as many large businesses ramp up their cyber security investments the opposite is true."


Bron: Allianz Risk Barometer 2023

# Risico’s gelinkt aan cybercrime

- Directe impact:
  - Losgeld (ca. 0,4%-2% van jaaromzet)
  - Boete Autoriteit Persoonsgegevens (AP)
  - Lengte “downtime”
  - Kosten “downtime”
  - Systeem-onderhoud / herstel

- Indirecte impact:
  - Reputatieschade → Anti-selectie

- ORSA:
  - Impact op eigen vermogen
  - Impact op SCR
  - Mogelijk significante impact op SII-ratio!
  - Herstelmaatregelen?

# Testen van digitale weerbaarheid 1/2


- Komt expliciet terug in DORA :
  - Threat Led Penetration Testing (TLPT)
- Jaarlijks passende testen uitvoeren op ICT-systemen die kritieke of belangrijke functies ondersteunen.
- Ook hierop rapporteren
- Precieze vereisten in 2e consultatiebatch
- DNB doet al TIBER testen

# Testen van digitale weerbaarheid 2/2


- DNB doet al TIBER testen:
  - Threat Intel Based Ethical Redteam
  - Vooral banken, grote verzekeraars
  - Échte hacks met ingehuurde professionals
  - Zijn er maatregelen? Is er een draaiboek?
  - DNB: “We hebben op dit moment in het TIBER-programma alleen de vitale instellingen in scope. […] Het is van belang dat ook middelgrote verzekeraars en belangrijke toeleveranciers zich voorbereiden op een echte aanval. Want ondanks alle voorbereiding kan het gebeuren dat een echte cyberaanval op een organisatie succesvol is. Samen kunnen we eraan werken om de impact dan zo minimaal mogelijk te laten zijn”

# Samenvattend

- DORA
  - Europese regelgeving
  - Verplicht
- Nodig gegeven omvang en toename  cyber risico
- Cyber risico
  - Componenten
  - Impact financieel → ORSA
  - Impact operationeel → TLPT
- Inzicht:
  - DORA bestuderen
  - GAP Analyse ten opzichte van DORA
  - Maatregelen nemen!

# Bedankt voor uw aandacht


Hoogoorddreef 54

1101 BE  Amsterdam Zuidoost

www.aaa-riskfinance.nl

info@aaa-riskfinance.nl

Jan-Willem Zeijen  06 2133 8091

jan-willem.zeijen@aaa-riskfinance.nl


DORA
EU-regelgeving
Roundtable


DORA

# Waarvoor staat de 'R' in DORA ?


# Uit hoeveel pijlers bestaat DORA ?


| 4 pijlers | 5 pijlers | 6 pijlers | 7 pijlers | 8 pijlers |
|---|---|---|---|---|
| ✗ | ✓ | ✗ | ✗ | ✗ |

# Vanaf wanneer treedt DORA in werking?


| 17 januari 2023 | 19 januari 2024 | 19 januari 2023 | 17 januari 2025 |
|---|---|---|---|
| ✓ | ✗ | ✗ | ✗ |

# Hoeveel organisaties gaan te maken krijgen met DORA ?


| ✗ | ✗ | ✗ | ✓ | ✗ |
|---|---|---|---|---|
| meer dan 5.000 | meer dan 12.000 | meer dan 17.000 | **meer dan 22.000** | meer dan 27.000 |

# Leaderboard

## No results yet

Top Quiz participants will be displayed here once there are results!

# Introductie DORA *(overweging 1)*

In het digitale tijdperk ondersteunt informatie- en communicatietechnologie (ICT) complexe systemen die worden gebruikt voor dagelijkse activiteiten.

ICT houdt belangrijke sectoren van onze economie draaiende, waaronder de financiële sector, en verbetert de werking van de interne markt.

Meer digitalisering en onderlinge verwevenheid vergroten ook het ICT-risico, waardoor de samenleving als geheel, en het financiële stelsel in het bijzonder, kwetsbaarder wordt voor cyberdreigingen of ICT-verstoringen.

Hoewel het alomtegenwoordige gebruik van ICT- systemen en een hoge mate van digitalisering en connectiviteit tegenwoordig belangrijke kenmerken zijn van de activiteiten van financiële entiteiten in de Unie, **moet hun digitale weerbaarheid nog beter worden aangepakt** en in hun ruimere operationele kaders worden ingebouwd.

# Doelstelling DORA *(artikel 1)*

Om een hoog gemeenschappelijk niveau van **digitale operationele weerbaarheid** te bereiken, worden in deze verordening uniforme vereisten vastgesteld met betrekking tot de beveiliging van netwerk- en informatiesystemen ter ondersteuning van bedrijfsprocessen van financiële entiteiten, te weten:

a) vereisten die van toepassing zijn op financiële entiteiten met betrekking tot:

- i) het **risicobeheer** op het gebied van informatie- en communicatietechnologie (ICT);
- ii) de **melding van ernstige ICT-gerelateerde incidenten** en, op vrijwillige basis, van **significante cyberdreigingen** aan de bevoegde autoriteiten;
- iii) de **melding van ernstige betalingsgerelateerde operationele of beveiligingsincidenten** aan de bevoegde autoriteiten door de financiële entiteiten als bedoeld in artikel 2, lid 1, punten a) tot en met d);
- iv) het **testen van de digitale operationele weerbaarheid**;
- v) de **uitwisseling van informatie** en inlichtingen met betrekking tot cyberdreigingen en -kwetsbaarheden;
- vi) maatregelen voor **het goede beheer van het ICT-risico van derde aanbieders**;

b) vereisten met betrekking tot de contractuele overeenkomsten tussen derde aanbieders van ICT-diensten en financiële entiteiten;

c) regels voor de vaststelling en het beheren van het oversightkader voor **kritieke derde aanbieders** van ICT-diensten bij het verlenen van diensten aan financiële entiteiten;

d) regels inzake **samenwerking tussen bevoegde autoriteiten** en regels inzake toezicht en handhaving door bevoegde autoriteiten met betrekking tot alle aangelegenheden die onder deze verordening vallen.

# De 5 pijlers van DORA

## ICT risico management

- Governance
- Risico management raamwerk
- Preventie & detectie
- Respons en herstel
- Communicatie
- etc

## ICT incident rapportage

- Classificatie van incidenten
- Classificatie van dreigingen
- Criteria en drempels
- Verplichte melding
- Geanonimiseerde EU-brede rapportages

## Testen van digitale weerbaarheid

- Testprogramma
- Interne of externe onafhankelijke partijen
- (TLPT) - Threat-led penetration testing (dreigingsgestuurd)
- eens in de drie jaar (extern)
- Rapportage aan toezichthouder

## ICT risicobeheer ketenpartners

- Kritieke of belangrijke functies
- Pre-contract toetsing
- Realistische exit opties
- Centraal toezicht op de ICT reuzen
- Bevoegdheden en boete-bepalingen

## ICT informatie uitwisseling

- Juridisch kader om informatie over dreigingen en kwetsbaarheden te delen
- Vertrouwens-gemeenschappen (Trusted communities)

*Van toepassing met ingang van 17 januari 2025*

In Audit
Audit Services

# Toepassingsgebied van DORA

## Bancaire instellingen

- Kredietinstellingen
- Betalingsinstellingen
- Rekeninginformatie diensten
- Instellingen voor electronisch geld
- Aanbieders van crypto (met vergunning)
- Centrale tegenpartijen

## Vermogens-beheer

- Handelsplatformen
- Transactieregisters
- Beleggings-ondernemingen
- Beheermaatschappijen
- Beheerders van alternatieve beleggings instellingen
- Centrale effecten-bewaarinstellingen

## Verzekeraars & pensioenfondsen

- Verzekeraars
- Herverzekeraars
- Assurantie-tussenpersonen
- Instellingen voor bedrijfspensioen-voorziening (IORP II)

## Overige gereguleerde organisaties

- Rating bureaus
- Aanbieders data-rapporteringsdiensten Beheerders kritische benchmarks
- Securitisatieregisters
- Aanbieders crowdfunding diensten

## Aanbieders ICT diensten

- Derde aanbieders van kritieke of belangrijke ICT diensten:

1. *Cloud services*
2. *Software*
3. *Datacenters*
4. ...

In Audit
Audit Services

# Van BIV criteria naar BAIV


# Evenredigheidsbeginsel *(artikel 4)*

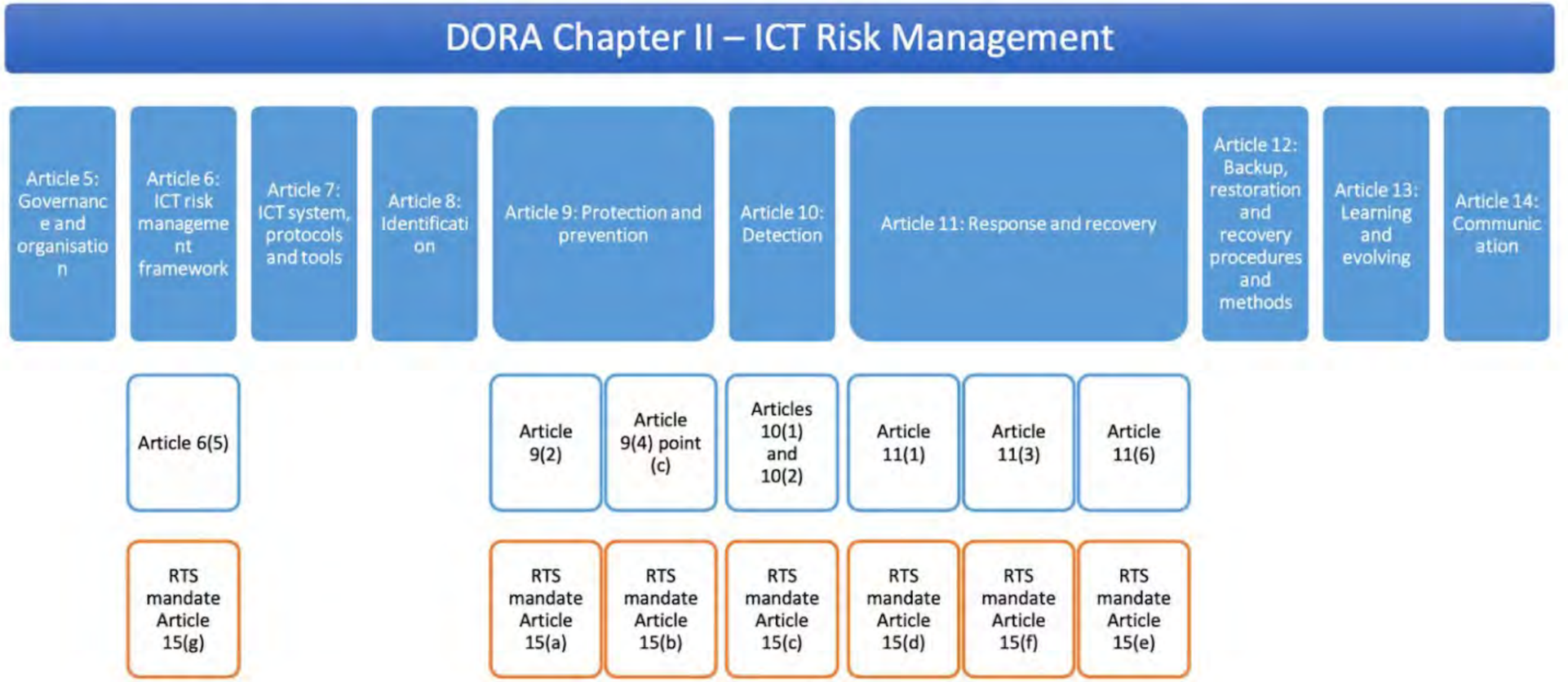
1. Financiële entiteiten passen de bij **hoofdstuk II** ingevoerde regels toe overeenkomstig het evenredigheidsbeginsel, rekening houdend met
   - omvang,
   - algehele risicoprofiel en
   - de aard, schaal en complexiteit van hun diensten, activiteiten en verrichtingen.

2. Daarnaast staat de toepassing door financiële entiteiten van de **hoofdstukken III en IV en hoofdstuk V**, afdeling I,
   - in verhouding tot hun omvang en algehele risicoprofiel en
   - tot de aard, schaal en complexiteit van hun diensten, activiteiten en verrichtingen,
   - zoals specifiek bepaald in de desbetreffende regels van die hoofdstukken.

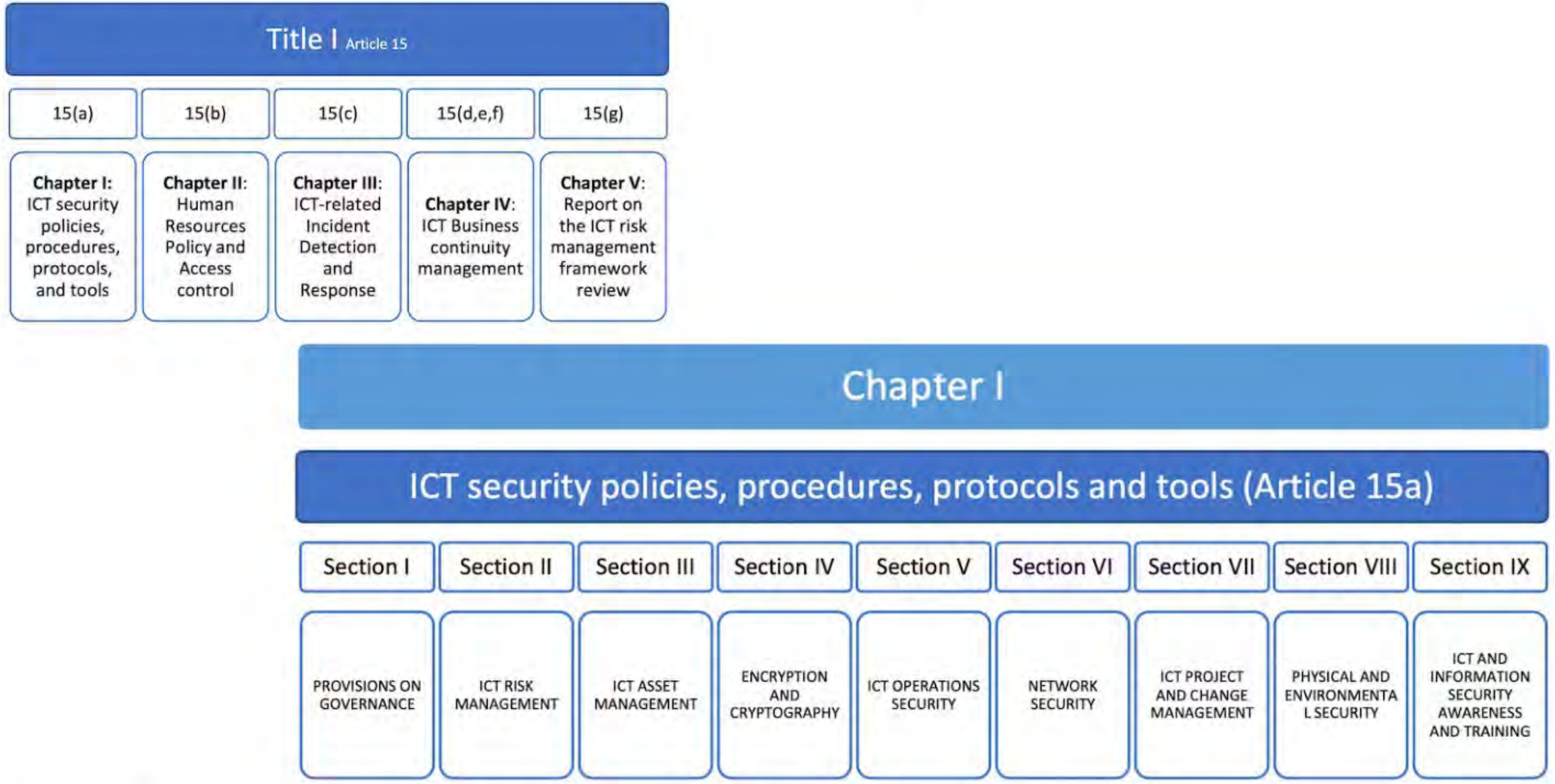
# Omvang criteria

| Omvang | Definitie | Werknemers | Jaaromzet / Balanstotaal |
|---|---|---|---|
| Micro | artikel 3 lid 60 (én/én criterium) | Minder dan 10 | Minder dan € 2 miljoen |
| Klein | artikel 3 lid 63 (én/én criterium) | 10 of meer, maar minder dan 50 | Meer dan € 2 miljoen, maar minder dan € 10 miljoen |
| Middelgroot | artikel 3 lid 64 (én/én criterium) | Minder dan 250 | Jaaromzet, maximaal € 50 miljoen<br>Balanstotaal, maximaal € 43 miljoen |
| Groot (volledig in scope) | | Meer dan 250 | Meer dan € 50 miljoen jaaromzet<br>Meer dan € 43 miljoen balanstotaal |

# Hoofdstuk 2 - Risicobeheer



# Hoofdstuk 2 - Risicobeheer



# Hoofdstuk 2 - Toezichthouder

*Artikel 6*

**Kader voor ICT-risicobeheer**

1. Financiële entiteiten beschikken over een solide, alomvattend en goed gedocumenteerd kader voor ICT-risicobeheer, als onderdeel van hun algemeen risicobeheersysteem, dat hen in staat stelt ICT-risico snel, efficiënt en zo volledig mogelijk aan te pakken en een hoog niveau van digitale operationele weerbaarheid te waarborgen.

2. Het kader voor ICT-risicobeheer omvat ten minste strategieën, beleidslijnen, procedures, ICT-protocollen en instrumenten die nodig zijn om alle informatie- en ICT-activa, met inbegrip van computersoftware, hardware, servers naar behoren en toereikend te beschermen, en om alle relevante fysieke elementen en infrastructuur, zoals gebouwen en terreinen, datacentra en als gevoelig aangewezen gebieden te beschermen, teneinde te waarborgen dat alle informatie- en ICT-activa toereikend worden beschermd tegen risico's, waaronder schade, ongeoorloofde toegang en ongeoorloofd gebruik.

3. Overeenkomstig hun kader voor ICT-risicobeheer beperken financiële entiteiten de impact van ICT-risico tot een minimum door passende strategieën, beleidslijnen, procedures, ICT-protocollen en instrumenten in te zetten. Op verzoek van de bevoegde autoriteiten verstrekken zij aan die autoriteiten volledige en geactualiseerde informatie over ICT-risico en over hun kader voor ICT-risicobeheer.

4. Andere financiële entiteiten dan micro-ondernemingen wijzen de verantwoordelijkheid voor het beheer van en toezicht op ICT-risico toe aan een controlefunctie en waarborgen een passend niveau van onafhankelijkheid van die controlefunctie om belangenconflicten te voorkomen. Financiële entiteiten waarborgen een passende scheiding en onafhankelijkheid van ICT-risicobeheerfuncties, controlefuncties en interne auditfuncties, overeenkomstig het model van de drie verdedigingslijnen of een model voor intern risicobeheer en -controle.

5. Het kader voor ICT-risicobeheer wordt ten minste eenmaal per jaar, of periodiek in het geval van micro-ondernemingen, gedocumenteerd en geëvalueerd, alsook wanneer zich ernstige ICT-gerelateerde incidenten voordoen en na toezichtinstructies of -conclusies die voortvloeien uit relevante tests of auditprocessen op het gebied van digitale operationele weerbaarheid. Het wordt voortdurend verbeterd op basis van de lessen die uit de uitvoering en de monitoring naar voren komen. Aan de bevoegde autoriteit wordt een verslag bezorgd over de evaluatie van het kader voor ICT-risicobeheer indien zij daarom verzoekt.

Toenemende informatieplicht aan de toezichthouder
*(indien zij daarom verzoekt)*

ICT-risico controlefunctie
*(de CISO)*

In Audit
Audit Services

# Hoofdstuk 2 – Inhoud review rapport

CHAPTER V

REPORT ON THE ICT RISK MANAGEMENT FRAMEWORK REVIEW

*Article 28*

**Format and content**

- 1. **Inleiding** (organisatie, doel van het rapport, context, belangrijkste wijzigingen)
  plus een 'executive level' samenvatting van het ICT risicoprofiel, het dreigingsbeeld, de (vastgestelde) effectiviteit van het informatiebeveiliging
- 2. Datum goedkeuring
- 3. Reden update review rapport (indien agv incidenten, een overzicht met root-causes)
- 4. Start- en einddatum review periode
- 5. De verantwoordelijke voor de review
- 6. Belangrijkste veranderingen en verbeteringen sinds de vorige review
- 7. Samenvatting van de review uitkomsten
- 8. Opsomming van de beheersmaatregelen, inclusief:
  (a) de control, (b) de verwachte implementatiedatum, (c) middelen, (d) indicatie impact in termen van kosten en tijd voor de implementatie (e) communicatie aan toezichthouder in geval van tekortschietende beheersing (f) indien tekortkomingen niet worden opgelost: hoe groot is het risico en wat doe je er aan ?
- 9. informatie over geplande ontwikkelingen
- 10. overall conclusies
- 11. informatie over afgelopen reviews (overzicht, follow-up, evaluatie ervan)

# Hoofdstuk 2 – rol voor interne audit

6. Het kader voor ICT-risicobeheer van andere financiële entiteiten dan micro-ondernemingen wordt regelmatig onderworpen aan een interne audit door auditors, in overeenstemming met het auditplan van de financiële entiteiten. Deze auditors beschikken over voldoende kennis, vaardigheden en deskundigheid op het gebied van ICT-risico en over de nodige onafhankelijkheid. De frequentie en de focus van de ICT-audits staan in verhouding tot het ICT-risico van de financiële entiteit.

7. Op basis van de conclusies van de interne audit stellen financiële entiteiten een formeel follow-upproces vast, met regels voor de tijdige verificatie en remediëring van kritieke ICT-auditbevindingen.

# H3 – Melding ICT gerelateerde incidenten

Financiële entiteiten omschrijven een beheerproces voor ICT-gerelateerde incidenten, stellen dit vast en leggen dit ten uitvoer om ICT-gerelateerde incidenten:

- te detecteren,
- te beheren en
- te melden

Uitdaging: classificatie (artikel 18) (o.a. 'ernstig' en 'significant')

Meldingsplicht voor 'ernstige' ICT gerelateerde incidenten

Vrijwillige melding van 'significante cyberdreigingen'

In het geval van een significante cyberdreiging stellen financiële entiteiten, in voorkomend geval, hun cliënten die mogelijk getroffen zijn in kennis van passende beschermingsmaatregelen die zij kunnen nemen.

# H3 – Classificatie incidenten

| Omvang | Definitie | Toelichting |
|---|---|---|
| ICT gerelateerd incident | artikel 3 lid 8 | één gebeurtenis of een reeks gekoppelde gebeurtenissen die:<br>- niet door de financiële entiteit zijn gepland en<br>- die de beveiliging van de netwerk- en informatiesystemen in gevaar brengen en<br>- een nadelig effect hebben op de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens of<br>- op de door de financiële entiteit verleende diensten |
| Betalingsgerelateerd operationeel of beveiligingsincident | artikel 3 lid 9 | één gebeurtenis of een reeks gekoppelde gebeurtenissen die niet door de [...] bedoelde financiële entiteiten zijn gepland, die al dan niet ICT- gerelateerd zijn, en [...] |
| Ernstig ICT-gerelateerd incident | artikel 3 lid 10 | een ICT-gerelateerd incident met grote nadelige gevolgen voor de netwerk- en informatiesystemen die kritieke of belangrijke functies van de financiële entiteit ondersteunen |
| Ernstig betalingsgerelateerd operationeel of beveiligingsincident | artikel 3 lid 11 | een betalingsgerelateerd operationeel of beveiligingsincident dat een groot negatief effect heeft op de verleende betalingsgerelateerde diensten |

# H3 – Classificatie dreigingen

| Omvang | Definitie | Toelichting |
|---|---|---|
| Cyberdreiging | artikel 3 lid 12 | Cyberdreiging in de zin van […] van Verordening (EU) 2019/881<br>(lees: De CyberSecurity Act – ENISA)<br><br>*"elke potentiële omstandigheid, gebeurtenis of actie die netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen kan schaden, verstoren of op andere wijze negatief kan beïnvloeden"* |
| Significante cyberdreiging | artikel 3 lid 13 | Een cyberdreiging waarvan de technische kenmerken erop wijzen dat zij kan leiden tot een ***ernstig*** ICT-gerelateerd incident of een ***ernstig*** betalingsgerelateerd operationeel of beveiligingsincident. |
| Cyberaanval | artikel 3 lid 14 | cyberaanval": een kwaadwillig ICT-gerelateerd incident dat het gevolg is van een door een dreigingsactor gepleegde poging om een actief te vernietigen, bloot te stellen, te veranderen, buiten werking te stellen, te stelen of er ongeoorloofde toegang toe te verkrijgen of er ongeoorloofd gebruik van te maken |
| | | |

# H4 – Testen digitale operationele weerbaarheid

Testprogramma verplicht onderdeel ICT risicobeheer

Door interne of externe onafhankelijke partijen *(kwalificeert de IAD ?)*

Ten minste éénmaal per jaar

**TLPT – Threat-led-Penetration-Testing** (dreigingsgestuurde penetratietest)

Ten minste éénmaal in de drie jaar geavanceerde tests

Financiële entiteiten beoordelen voor welke kritieke of belangrijke functies TLPT moeten worden verricht.
Het resultaat van die beoordeling bepaalt het exacte toepassingsgebied van TLPT
en wordt door de bevoegde autoriteiten gevalideerd.

Gebundelde test bij 'derde aanbieders' (met één lead financiële entiteit)

# H5 – Risicobeheer 'derde' aanbieders

"financiële entiteiten die contractuele overeenkomsten voor het gebruik van ICT-diensten voor hun bedrijfsactiviteiten hebben getroffen, **blijven te allen tijde volledig verantwoordelijk voor de naleving** en de verantwoording van alle verplichtingen uit hoofde van deze verordening en het toepasselijke recht inzake financiële diensten"

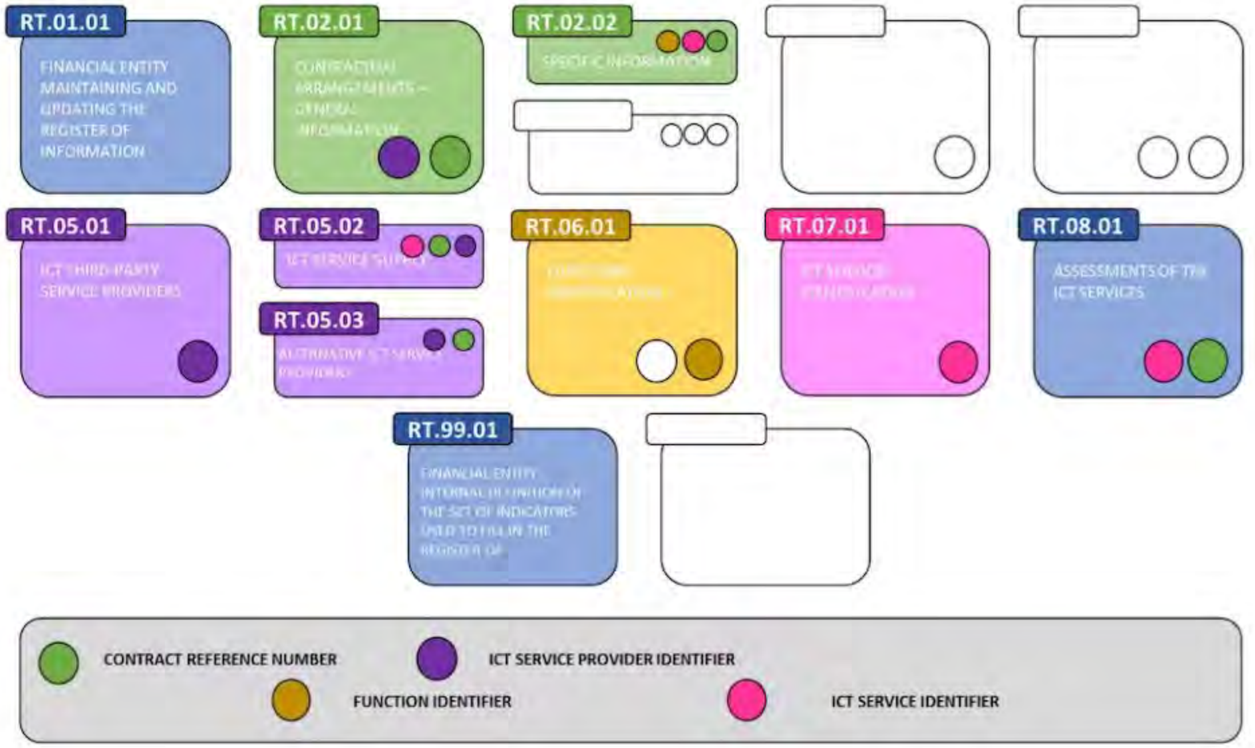
Jaarlijkse rapportage aan de toezichthouder van gebruik van 'derde' aanbieders
(zie volgende slide)

- Formele criteria voorafgaand aan contracteren
- Infomeren toezichthouder
- Beoordeling ICT-concentratierisico
- Beoordeling subcontractering
- Naleving en handhaving GDPR in derde landen
- Belangrijke contractuele bepalingen (2 pagina's !) → https://www.dirkzwager.nl/kennis/artikelen/checklist-voor-it-contracten-onder-dora/

# Rapportage aan de toezichthouder

8. The register of information at entity level is composed of 10 templates. Illustration 1 shows the relational structure between the templates highlighting the relational keys used to link one template to another.

**Illustration 1: Structure of the Register of Information maintained and updated at entity level**



# H5 – Oversight kader kritieke aanbieders

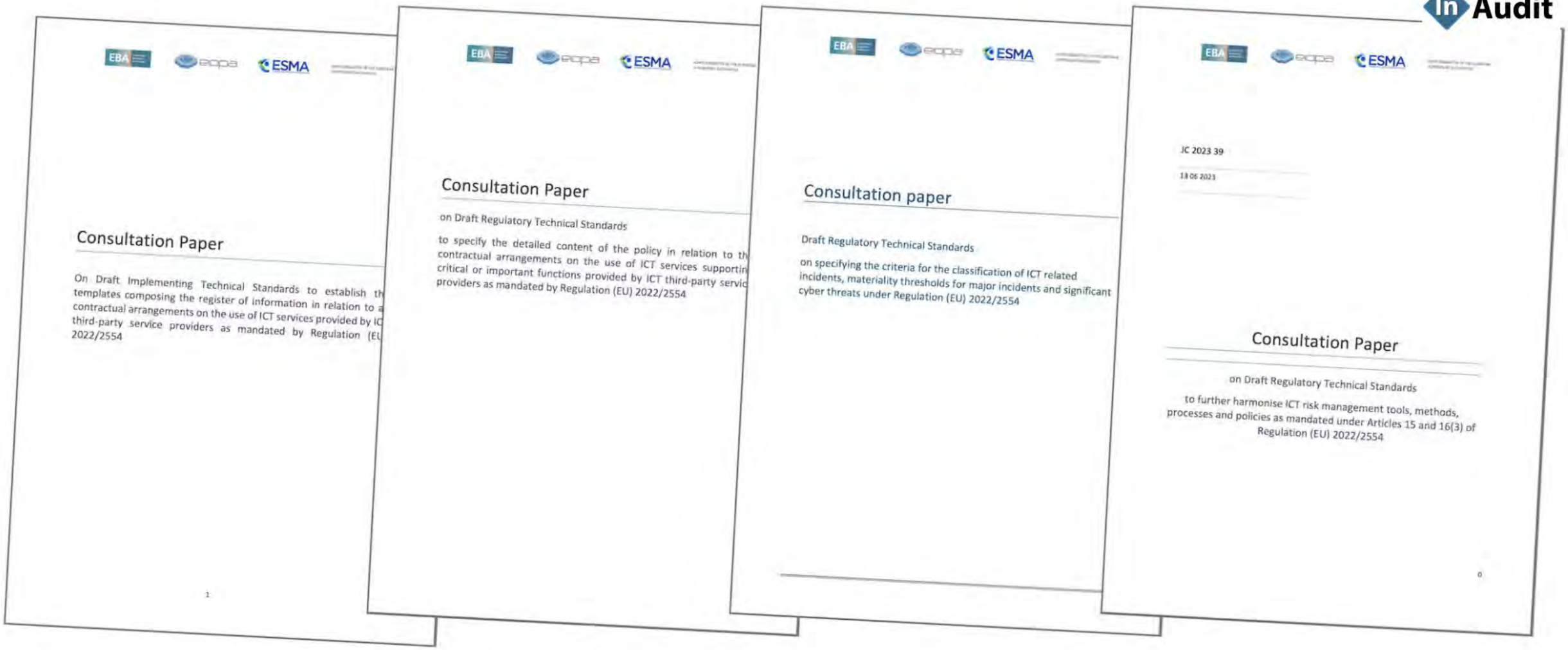
Toezicht op kritieke derde aanbieder verschuift naar de Europese toezichthouders

# H6 – Uitwisseling informatie

Financiële entiteiten kunnen **onderling informatie en inlichtingen** over cyberdreiging **uitwisselen**, zoals indicatoren voor aantasting, tactieken, technieken en procedures, cyberbeveiligingswaarschuwingen en configuratie-instrumenten, voor zover dit:

- Bedoeld is om de digitale operationele weerbaarheid te versterken;
- Plaatsvindt binnen 'vertrouwensgemeenschappen' (trusted communities)
- Met inachtname van regelingen om potentieel gevoelige informatie te beschermen

Toezichthouders worden geïnformeerd




DORA wordt nader uitgewerkt in diverse technische standaarden

# Wat gaat er "veranderen"?

- Van "beheerste en integere bedrijfsvoering" naar wettelijke normeringen.
  - DORA bevat stringentere normen dan de huidige Guidelines en Good Practices.
  - Noodzaak tot (geavanceerde, dreiging gestuurde) testen (waarbij TIBER als raamwerk wordt onderschreven).
- Inzicht in de gehele uitbestedingsketen (en de beheersing daarover) wordt nog belangrijker en is een verplichting.
- Formalisatie van de Meldplicht ICT-incidenten bij de toezichthouder(s)


DeNederlandscheBank
EUROSYSTEEM


DORA
EU-regelgeving
Roundtable

# De Europese toezichthoudende autoriteiten worden de ETA's genoemd. Welke zijn dat ?


| ENISA, ECB en EIOPA | ECB, EBA en EIOPA | EBA, ENISA en EIOPA | EBA, ESMA en EIOPA |
|---|---|---|---|
| ✗ | ✗ | ✗ | ✓ |

# Waarvoor staan de letters TLPT?


| ✗ | ✗ | ✗ | ✓ | ✗ |
|---|---|---|---|---|
| Tactical Network Penetration Test | Threat Landscape Proficiency Test | Top Level Security Posture Test | **Threat Led Penetration Test** | Technology Lifecycle Protection Test |

# Wat is geen (onderdeel van) de verplichte rapportage aan de toezichthouder ?


| ICT risico beheersings-kader | Evaluatie ICT risico beheersings-kader | Overzicht derde ICT aanbieders | Uitkomsten TLPT testen incl correctie plannen | Overzicht significante cyber-dreigingen |
|---|---|---|---|---|
| ✗ | ✗ | ✗ | ✗ | ✓ |

# In pijler 3 worden voorbeelden genoemd van passende tests. Welke wordt niet genoemd ?


| Prestatietests | Data-analyses | Gap-analyses | Open source analyses | Beoordeling broncodes |
|---|---|---|---|---|
| ✗ | ✓ | ✗ | ✗ | ✗ |

# Wat is geen pijler van de DORA ?


# Grootste uitdagingen per pijler

## ICT risico management

- Governance
- Risico management raamwerk
- Preventie & detectie
- Respons en herstel
- Communicatie
- etc

## ICT incident rapportage

- Classificatie van incidenten
- Classificatie van dreigingen
- Criteria en drempels
- Verplichte melding
- Geanonimiseerde EU-brede rapportages

## Testen van digitale weerbaarheid

- Testprogramma
- Interne of externe onafhankelijke partijen
- (TLPT) - Threat-led penetration testing (dreigingsgestuurd)
- eens in de drie jaar (extern)
- Rapportage aan toezichthouder

## ICT risicobeheer ketenpartners

- Kritieke of belangrijke functies
- Pre-contract toetsing
- Realistische exit opties
- Centraal toezicht op de ICT reuzen
- Bevoegdheden en boete-bepalingen

## ICT informatie uitwisseling

- Juridisch kader om informatie over dreigingen en kwetsbaarheden te delen
- Vertrouwens-gemeenschappen (Trusted communities)

In Audit
Audit Services

# Grootste uitdagingen per pijler

**ICT risico management**

- Governance
- Risico management raamwerk
- Preventie & detectie
- Respons en herstel
- Communicatie
- etc

- Voortgang op implementatie Good Practice document
  Het toezicht wordt meer 'rule-based'

- Expliciete onafhankelijke ICT controlefunctie (CISO)
- Leiding moet actief 'voldoende kennis en vaardigheden' onderhouden
- Expliciete aandacht voor respons en herstel *(nog een voorbereidend crisisplan)*

- Details & rapportages:
  - Regulatory Technical Standards
  - Ten minste eenmaal per jaar evaluatie en vastlegging
  - (Op verzoek) aan toezichthouder verstrekken


In Audit
Audit Services

# Grootste uitdagingen per pijler

**ICT incident rapportage**

- Classificatie van incidenten
- Classificatie van dreigingen
- Criteria en drempels
- Verplichte melding
- Geanonimiseerde EU-brede rapportages

- Verbeteren van issue- en incidentenregistratie
- Ontwikkelen van een incidenten-classificatiemethode
- Tijdige meldingen aan de toezichthouder

- Implementatie classificatiesysteem in RTS

# Grootste uitdagingen per pijler

**Testen van digitale weerbaarheid**

- Testprogramma
- Interne of externe onafhankelijke partijen
- (TLPT) - Threat-led penetration testing (dreigingsgestuurd)
- eens in de drie jaar (extern)
- Rapportage aan toezichthouder

- Eisen aan programma van penetratietesten
- De dreigingsgestuurde penetratietest (TLPT)
  *(Mogelijk al eind 2024 om in 2025 gereed te zijn)*

- Afstemming met **toezichthouder** vooraf *(art 26 lid 2)*
  Rapportage aan de toezichthouder achteraf *(art 26 lid 6)*
  *(mogelijk één toezichthouder – art 26 lid 9)*

- Gebundelde tests bij derde-aanbieders

- Nadere technische reguleringsnormen volgen nog (uiterlijk 17 juli 2024) *(gebaseerd op Tiber-EU kader)*

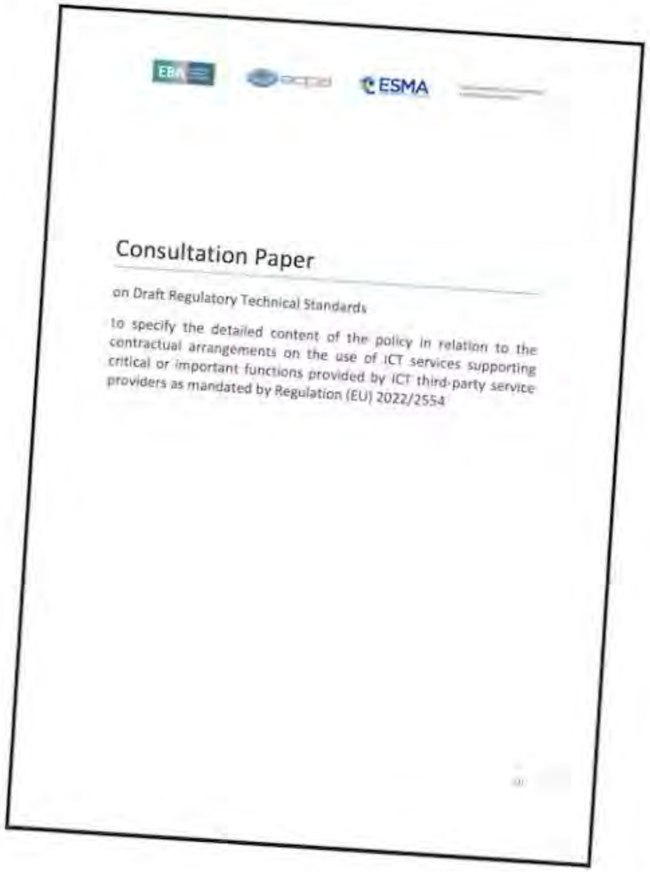
# Grootste uitdagingen per pijler

## ICT risicobeheer ketenpartners

- Kritieke of belangrijke functies
- Pre-contract toetsing
- Realistische exit opties

- Centraal toezicht op de ICT partijen
- Bevoegdheden en boete-bepalingen

- Overzicht (Informatieregister) van derde partijen die (kritieke of belangrijke) ICT diensten leveren
- Jaarlijkse rapportage aan toezichthouder
- Vooraf informeren van toezichthouder van voorgenomen contractuele overeenkomsten inzake het gebruik van ICT diensten die *kritieke* of *belangrijke* functies ondersteunen
- Service providers betrekken in de voorbereidingen op DORA
- Nieuwe contracten met ICT dienstverleners ?



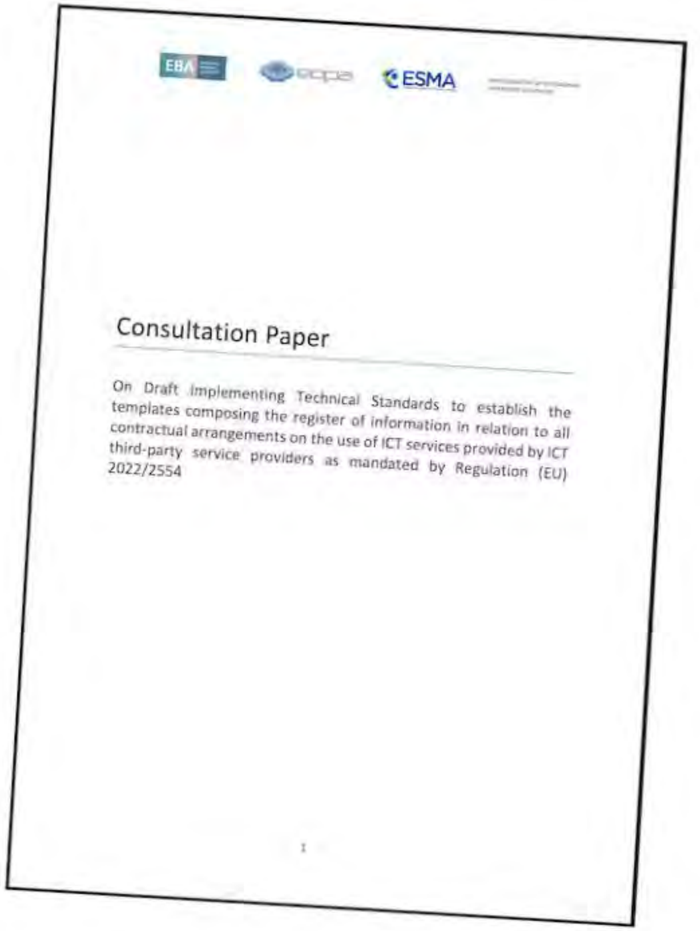

In Audit
Audit Services

# Grootste uitdagingen per pijler

## ICT informatie uitwisseling

- Juridisch kader om informatie over dreigingen en kwetsbaarheden te delen
- Vertrouwens-gemeenschappen (Trusted communities)

- Is de organisatie al aangesloten bij een 'trusted community' ?
- Regelingen voor informatie-uitwisseling
- Melden aan de toezichthouder


EBA ESMA

Consultation Paper

On Draft Implementing Technical Standards to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554

# Samenvattend

- Implementatie van DORA vereist een plan van aanpak:
    - Organisatie, verantwoordelijkheid, team
    - Planning op basis van prioriteiten
    - Samenloop met Good Practice ‘19 / ‘23 verbeterprocessen
    - Betrokkenheid van bestuur / RvC



We zijn er om u te helpen !