# NOREA Reporting Initiative

## NOREA Symposium 2023

How the ever-increasing digitization of our society requires a new form of accountability for the management of IT

10 May 2023

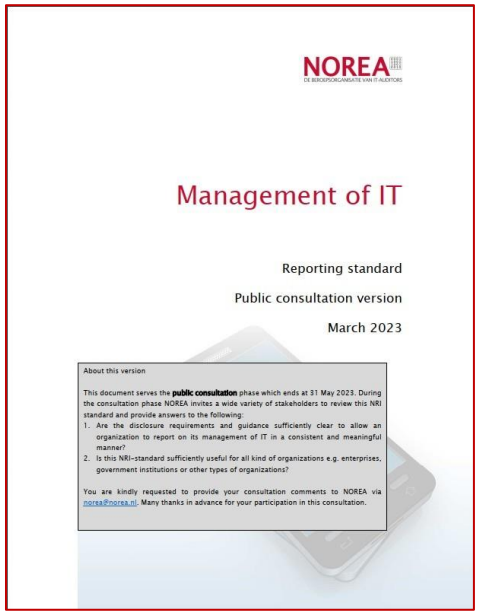
NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

# Agenda

1. Introduction – Why NRI
2. Positioning NRI
3. Drafting approach
4. Structure
5. Per topic
6. Next steps on the journey
7. Consultation questions

# 1. Introduction – Why NRI?

- NOREA vision and mission statement
  - Manifest
- IT resilience
  - Continuity
  - Cyber
  - Data
- Transparancy and accountability
- Role of IT-auditor

# 1a. Introduction to the topic

- Digitization advances at an unprecedented pace, and so are the risks…
- It happens as we speak, and more will follow…
  - Quantum computing, seems remote, but is it?
  - If ‘change is the new constant’, so are ‘new risks’
- If the industry calls for a break, regulators and supervisors need to speed up?
- NOREA view: Transparency and Accountability are a part of the puzzle, and need to get more structure

REUTERS® World Business Legal Markets Breakingviews Technology Investigations

3 minute read · March 29, 2023 3:33 PM GMT+2 · Last Updated 4 hours ago

## Elon Musk and others urge AI pause, citing 'risks to society'

By Jyoti Narayan, Krystal Hu, Martin Coulter and Supantha Mukherjee

March 29 (Reuters) - Elon Musk and a group of artificial intelligence experts and industry executives are calling for a six-month pause in developing systems more powerful than OpenAI's newly launched GPT-4, in an open letter citing potential risks to society and humanity.

Opinie • 14 apr 11:00

## Digitale weerbaarheid: een verplichte upgrade

Laura van Geest

Cyberveiligheid heeft de aandacht van bestuurders, maar volgens AFM-voorzitter Laura van Geest moeten zij zich dit thema veel intensiever toe-eigenen. Bestuurders kunnen het niet langer van zich afschuiven en overlaten aan de cyberexperts.

# 1b. (EU) Acts

- In EU new and tightened laws (e.g. NIS2, DORA, Digital Markets Act, Artificial Intelligence Act and Cyber Resilience Act).
- In NL updated Corporate Governance Code, Policy Response OVV Report 'vulnerable by software – lessons in response to vulnerabilities by Citrix software, Digital Government Act and Future of Pensions Act.

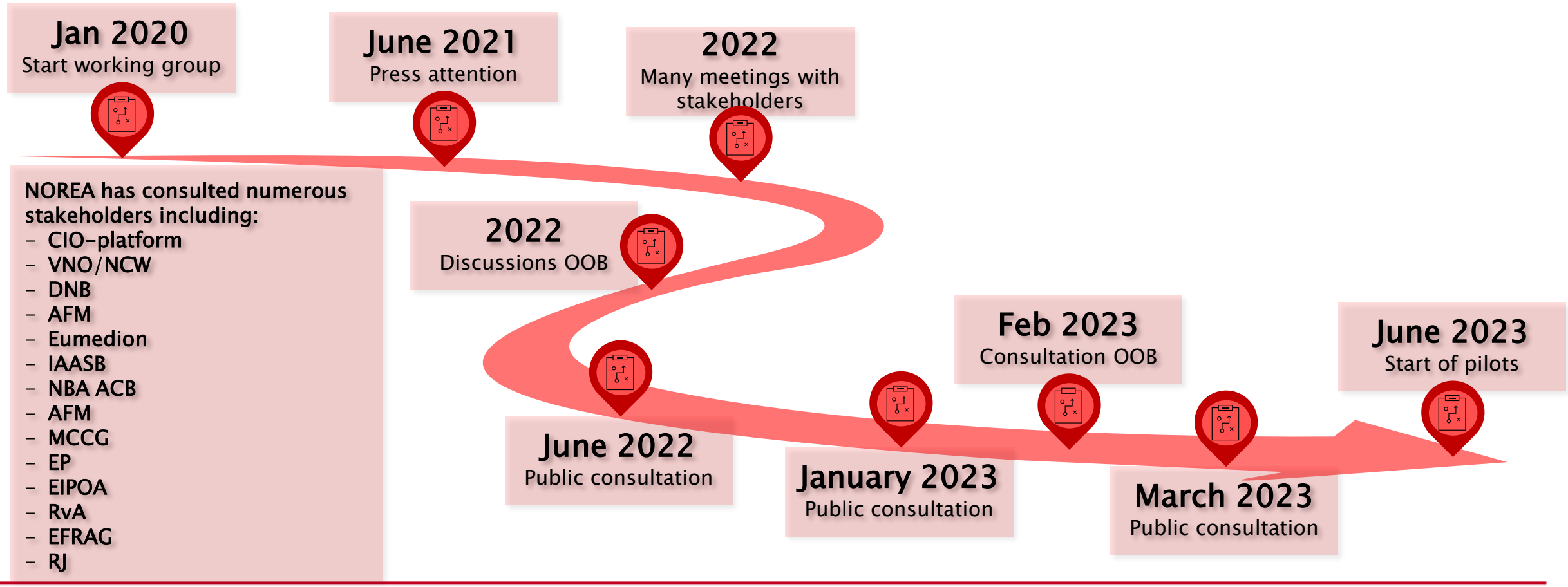

- All these laws and regulations mention IT-statements and audits that must determine that IT control is in order.



NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

# 1c. Our NRI road so far

**Over the past 3 years NOREA made relentless efforts to develop the NRI concept while consulting numerous stakeholders**






NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

# 2. Positioning the NOREA Reporting Initiative

Frameworks

Reporting

NRI

Stakeholders
e.g. Regulators

Legislation / regulations
Good practices

Industry

Policies / Procedures
(Organization specific)

Operational IT

ISO Standards
Best practices (e.g. TOGAF, Cobit, DAMA, DMBOK)

Much more to come…

Service levels
Incidents
Progress reports
Change requests

IT Management topics
Based on standards and best practices
Organization specific



NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

# 2a. Standards underlying NRI

- Transparency and accountability are main objectives
- It is crucial to base reporting on underlying standards
  - Common language
  - To measure / Maturity / Norm
  - Comparability
- And to maintain a mapping to regulatory frameworks, i.e. GDPR, DORA, DSA, etc.
- Therefore NRI based on a multitude of standards, see bibliography section




NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

# 2b. Why is it a good idea?

- Digitization just started… and society is too vulnerable
- Industry:
  - Increased need to answer to responsibilities re transparency and accountability (in line with sustainability topics)
  - Regulatory burden dilemma; more info needed against lower effort
- Regulators:
  - Framework for obtaining information based on proven standards
  - Convergence of frameworks (e.g. across industries), reduce ‘regulatory noise’
- Action is needed

# 3. The drafting approach we followed

- Analogy with GRI standards (2 and 3)
  - Identified as a topic standard
  - Separation of management of IT topic(s) and Material IT topics
  - Adoption of the GRI structure: disclosures → requirements → guidance
- Shall be a reporting standard not an audit standard
  - Audit guidance separate
  - Assurance report foreseen
- Structure
  - Starting with a scope paragraph per IT topic
  - Follows a generic structure
  - Shall be concrete but not prescriptive
  - Report should be auditable
  - Identified material topics for IT with the option to extend the set

# 4. Resulting setup of the standard

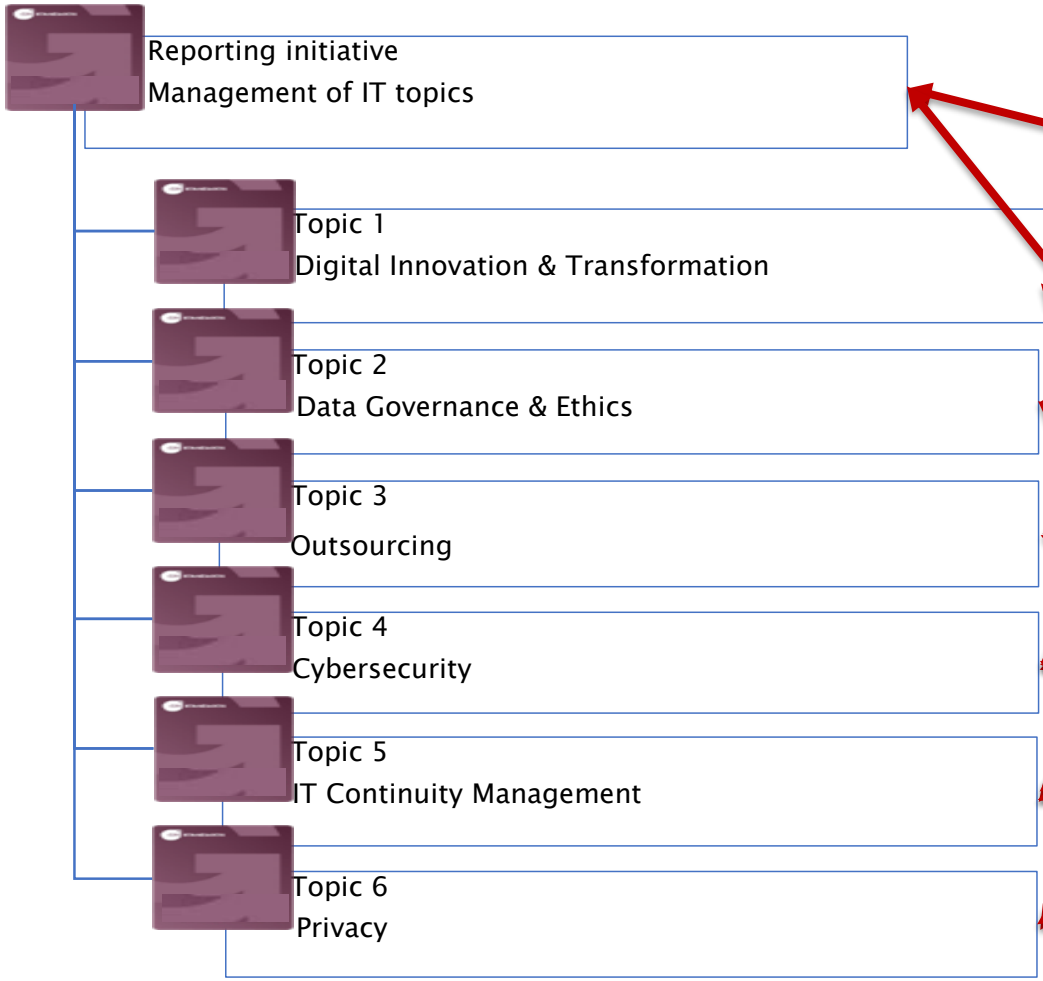
Introduction
- What, Why, Relations enterprise level and GRI, sustainability, 'likely' material IT topics

Management of IT
- Organization and governance
- Risk management

Identified generic IT material topics
- IT Innovation and Transformation
- Data governance & Ethics
- Outsourcing
- Cybersecurity
- IT Continuity Management
- Privacy


Based on international acknowledged standards and best practices (ISO standards or equivalent), see bibliography.

# 4a. Visualized structure



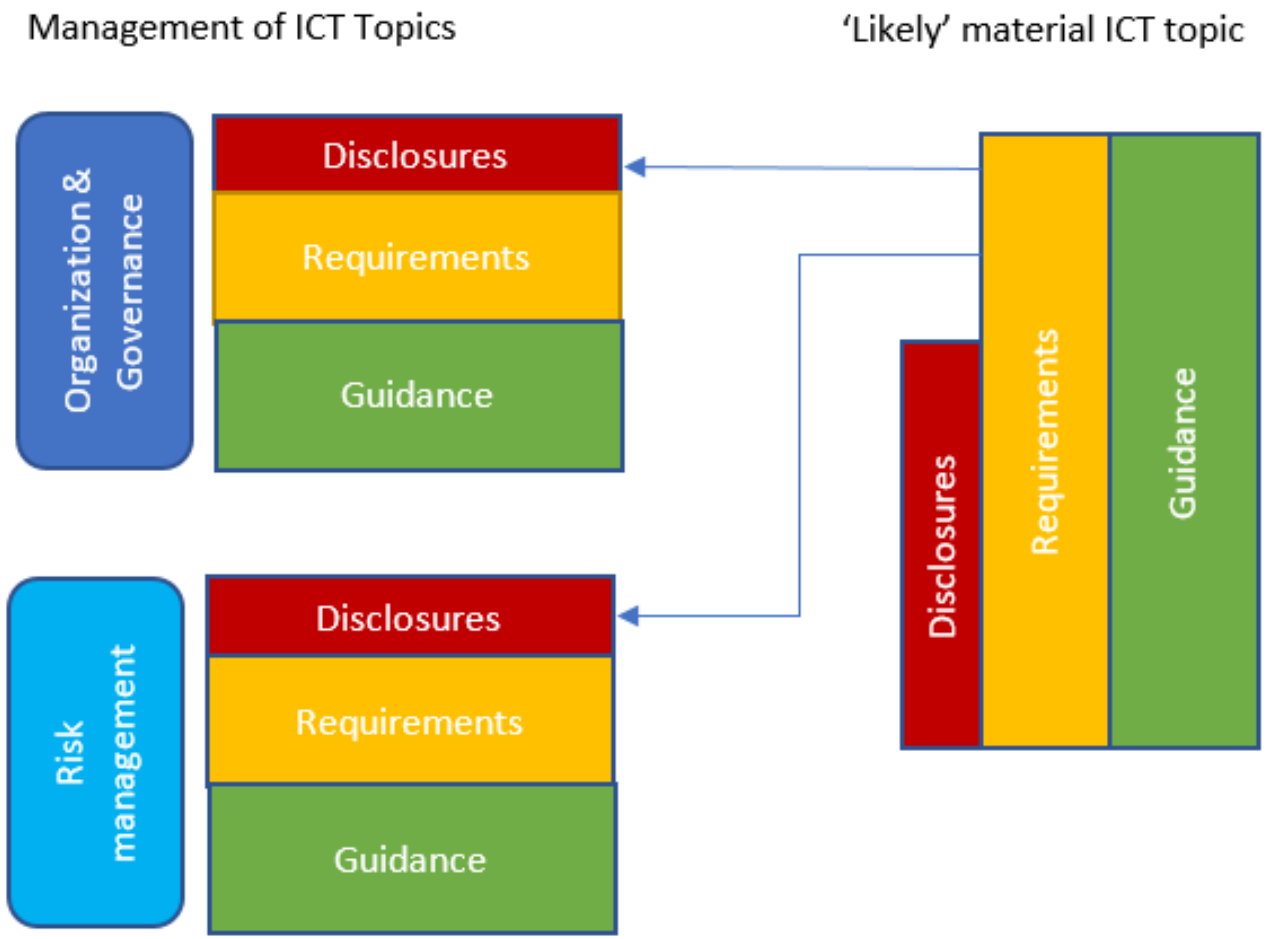

**Example of relevance: DORA**

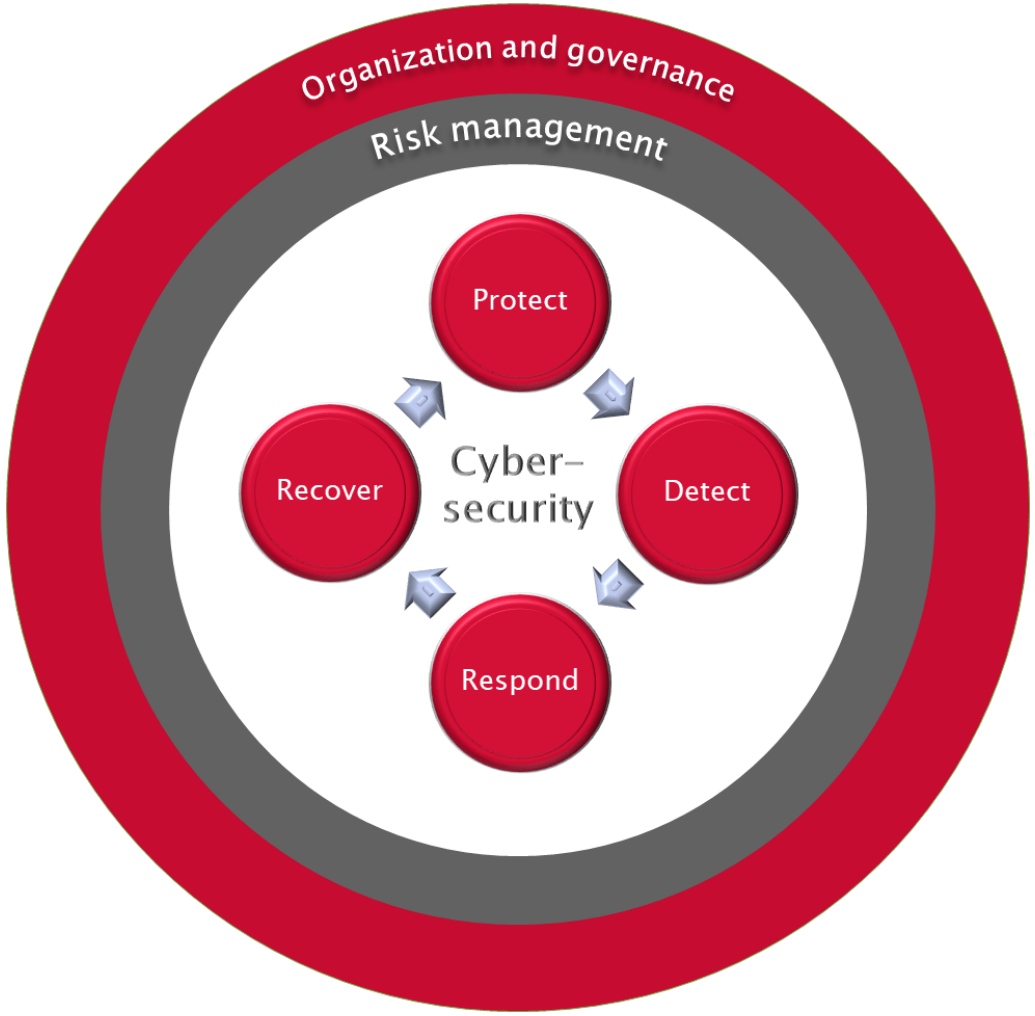
1. IT Risk Management
2. Incident reporting
3. Operational resilience testing
4. Management of IT third party risk
5. Information sharing

# 5. Structure per 'likely' material IT topic


- Scope
  - Why material, what is it, relation with management of IT topics, cross relations with other IT topics
- Requirements "Organization and governance" and "Risk management" directly related to disclosures in the 'Management of IT topics'.
- GRI elements (relations in the numbering)
  - Disclosures (derived from principles defined in standards)
  - Requirements (Direct, Monitor, Evaluate)
  - Guidance (Policy, Process, Monitor and improvement, Occurrences, Communications, Review)
- Setup: Plan Do Check Act management cycle specific for IT topic
  - Following domain specific standards and best practices

# 5a. Connected layers



# 5b. Disclosures, requirements and guidance

**Disclosures**


Assertions /
Statements by management
of the organization

**Requirements**

**Guidance**

Shall = Requirement

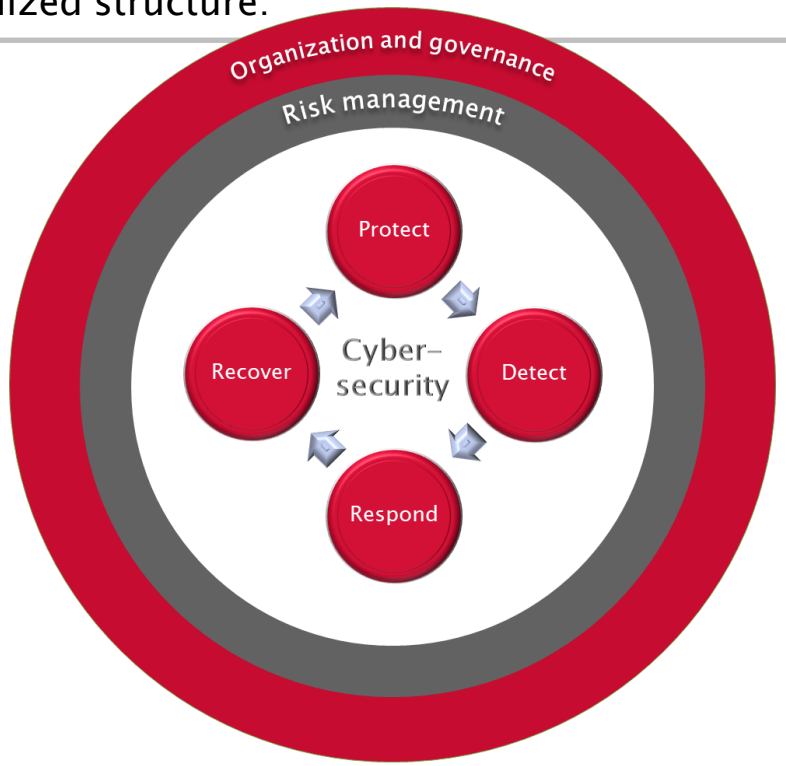
Should = Expectation/ Recommendation

Could = Possibility / capability

May = Permission

# 5c. Structure of the standard

- 6 identified generic IT material topics: cybersecurity, digital innovation and transformation, business contingency management, (out)sourcing, data governance & ethics and privacy.
- GRI-standard used as a starting point which structure is based upon: disclosures, requirements and guidance.
- Visualized structure:




| Disclosures IT topic cybersecurity | |
|---|---|
| CYBER-1 | Developed and implemented safeguards to ensure sufficient delivery of products and services that limit or contain the impact of a potential cybersecurity event. |
| CYBER-2 | Identified occurrence of cybersecurity events in a timely fashion. |
| CYBER-3 | Appropriate actions regarding detected cybersecurity events to sufficiently contain the impact of these events. |
| CYBER-4 | Maintained and tested plans for resilience and to restore any capabilities or services that were impaired due to cybersecurity events. |

| Requirements | |
|---|---|
| **IT Topic Cybersecurity** | |
| CYBER-1-1 | The reporting organization shall report the status of, and the activities for, protection safeguards that limit cyber risks. |
| CYBER-2-1 | The reporting organization shall report the activities for detecting cyber risk events timely. |
| CYBER-3-1 | The reporting organization shall report the activities with regards to the response on cyber risk incidents. |
| CYBER-4-1 | The reporting organization shall report the activities to recover from cyber risk incidents and the impact on :<br>• business partners;<br>• economy;<br>• environment and /or ;<br>• people, including impacts on their human rights. |

| Guidance | |
|---|---|
| **Example: Topic Cybersecurity** | |
| CYBER-1-1e | The reporting organization should report on the patch management process.<br><br>The organization could report about:<br>• identification of patch sensitive software and assets;<br>• routine patching;<br>• emergency patching;<br>• emergency mitigation;<br>• unpatchable assets (if any);<br>• patch management security impact and controls;<br>• impact for maintenance plans. |



NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

# 6. Next steps on the journey

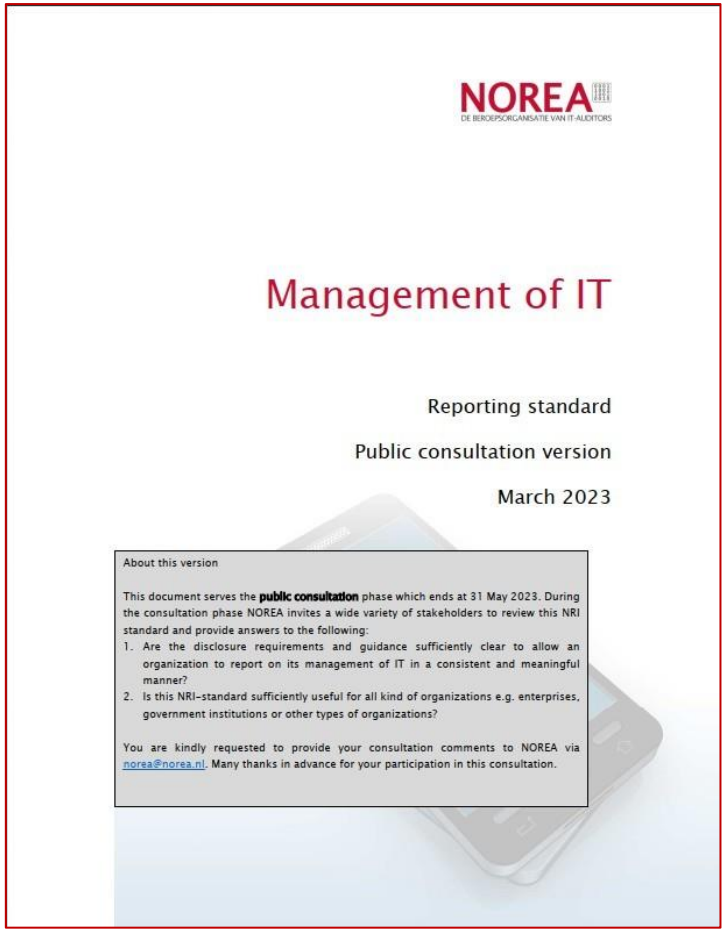
- Public Consultation
  - Ending 31 May 2023
- Pilot projects
  - 1 completed in 2022 (healthcare insurance)
  - Public sector: Government agencies, Community, Water management district
  - Private sector: various pilots, including Finance sector
- Further socialization of the NRI concept
  - National
  - International
- New version (2024 use)
  - Ready to go…

# 7. Some questions to you…

**Public Consultation ending 31 May 2023**

1. Are the disclosure requirements and guidance sufficiently clear to allow an organization to report on its management of IT in a consistent and meaningful manner?
2. Is this NRI-standard sufficiently useful for all kind of organizations e.g. enterprises, government institutions or other types of organizations?
3. Which body should ideally be responsible for issuing and maintaining such reporting standard?

- You are very much invited to respond!!




Any Questions?

# Thank you

Please contact Marc Welters or Rob Polderman if you require more information

norea@norea.nl



NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

# NOREA Reporting Initiative

## NOREA Symposium 2023

Backup slides – further detailed information

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

# Status quo

**Commissie Franken**

- Article 2:393 paragraph 4 of the Dutch Civil Code indicates that the accountant must give an opinion on the reliability and continuity of the automated data processing in connection with the audit of the annual accounts. In Pracitce, this leads to:
  i) diversity in the implementation of this obligation, in which cyber and IT contingency are not taken into account;
  ii) automated data processing to the extent relevant for the audit of the annual accounts is in scope and not broader

**Europe**

- In Europe, new and tightened laws are being issued to boost the general level of security within the EU, referring to monitoring, testing and auditing of measures taken (e.g. NIS2, DORA, Digital Markets Act, Artificial Intelligence Act and Cyber Resilience Act).
- In Dutch legislation and policy notes, there is a growing need to anticipate developments in new technologies with associated (IT) risks (e.g. updated Corporate Governance Code, Policy Response OVV Report 'vulnerable by software – lessons in response to vulnerabilities by Citrix software, Digital Government Act and Future of Pensions Act.
- All these laws and regulations mention IT-statements and audits that must determine that IT control is in order.

**Digital society**

- Digital society is experiencing increasing dependence on IT and the associated (cyber) risks and chain vulnerabilities.
- Emergence of new revenue models partly as a result of developments in the field of sustainability and digitization (including: Artificial Intelligence (AI), Internet of Things (IoT), Blockchain and Quantum).
- In short: being in control over IT is an increasing necessity and knowing that the Netherlands is one of the most digitalised countries in the world this becomes even more important.

# Growing need for more insight

**Desire for insight**

- Among stakeholders (directors, supervisory directors and audit committee, supervisors, government) there is a growing need for insight into digital resilience against cyber attacks, data breaches, continuity of IT (and thus the continuity of organizations). This requires obtaining an integral picture of the control of IT within and by organizations

**Diversity of reporting**

- <u>Bottleneck:</u> diversity of forms of reporting with differences in depth/scope, which leads to redundancy, extra burdens, incomparability and ambiguity towards society.

Internal Control Statement

- Does not have a predetermined norm/standard that is tested against
- Drawn up internally without external assurance statement
- Hardly released to society
- Limited valud can be derived from this (comparison difficult due to lack of common standard as well as depth/scope/norm often not clear)

Key Audit Matters in auditor's report

- Scope includes key points in the audit (with regard to information security)
- The aim of Key Audit Matters is to break the uniformity of the audit report, to make it organisation-specifi, more informative and to increase transparancy about the audit

Assurance rapport

- Current assurance reports (SOC1/2-reports, ISAE 3000/3402-reports) play an important role, but focus exclusively on the past.
- The IT-scope is limited and focuses mainly on the General IT Controls regarding the financial accounting processes

ISO -certificates (e.g. 27001 and 22301)

- The scope is exclusively about information security
- The report is only focussed on the design (and not on testing the existences and operational effectiveness over a longer period of time) of the processes

Other reports (not exhaustive)

- IT Risk questionnaire self-assessment in financial sector
- NEN7510 in the healthcare sector
- SURF in de education sector
- BIO within the government

**Diversity of assurance**

- The diversity of accounts, certificates and reports has also led to various auditors and experts making an assessment of (parts of) IT control, which has led to uncertainty about the degree of IT control among stakeholders.

# What do we want to achieve?

**Increase resilience**

- Stimulate dialogue in the Boardroom and other stakeholders about having and maintaining IT in order, which is an impulse for long-term value creation.
- Ensuring that we are digitally resilient. As a society, but also at the level of individual organizations.
- Importance of adequate IT control of organizations in order to maintain competitiveness. Not only as an organization, but also as a country.

**Statement of accountability for IT control**

- Giving (externa) accountability for IT control within an organisation gives an impulse to the fulfillment of legal responsibility.
- Organisation obtains overarching coherent insight in key challenges and opportunities regarding IT, in its broadest sence (including the value-chain).
- Reduction administrative burden for organisation by preventing that each individual (new) EU/NL regulation asks for another report documenting compliance.
- Supervisors and regulators obtain sector-wide insight in key risk areas across our eco-system.
- Qualified IT-auditors who provide a standardized statement of accountability for IT control for all (vital) sectors ensures greater certainty for all stakeholders.

**How?**

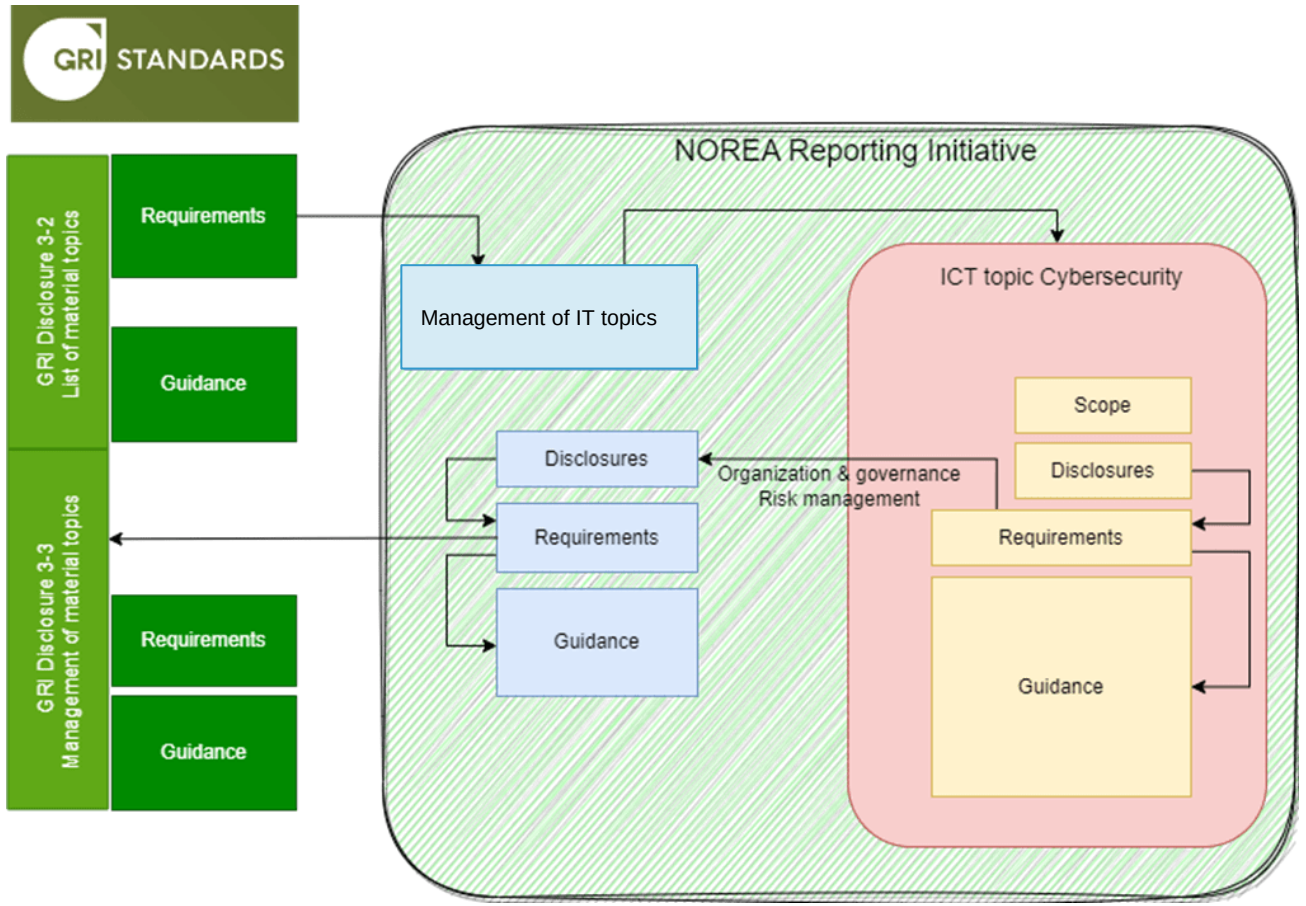
- *Reporting standard to account for IT control by management of the organisation*, in short: IT report.
- Accountability will be looking back and looking forward.
- The scope of the IT report will be broader than the IT scope in the audit of the financial statements. It contains: cybersecurity, digital innovation and transformation, business contingency management, (out)sourcing, data governance & ethics and privacy. To be used by SMEs and multinationals.
- No new control framework, but making use of the frameworks that organisations already have to comply with (e.g. NEN750, BIO, SURF, EBA). Based on the current GRI-standard (as is also used for sustainability reporting).

# How is this reporting standard compiled?

Structure reporting-standaard

- 6 IT Topics: cybersecurity, digital innovation and transformation, business contingency management, (out)sourcing, data governance & ethics and privacy.
- Making use of frameworks organisations already need to comply with (e.g. NEN750, BIO, SURF, EBA).
- Starting point used is GRI-standard including its structure: disclosures, requirements and guidance. Also based on e.g. ISO TS 27100/27103 [2020/2021], ISO 27035/27036, NISTIR 8286 [2020], NIST SP 800-40/800-161r1/NIST CSF v1.1 [2018], ISO 27001, ISO 27002, 'Basismaatregelen cybersecurity NCSC'.

- Structure:




.



NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

# Next steps

**Consultation**

- NOREAs reporting standard has been reviewed by the professional practices departments of the 6 OOB-audit offices in the Netherlands.
- Medio March the reporting standard will be lauchned for a formal consutation via the website of NOREA and social media channels as well as shared with individual stakeholders who have been in contact with NOREA during the recent months. This consultation period will take place untill the end of June 2023.

**Pilots**

- The outcome of the first pilot, taken place by a health insurance company, provided the managing board and supervisory board an integral insight in the key (overarching) challenges and opportunties regarding the IT, in its broadest sence. This outcome supported a dialog on 'IT in control' between all involved parties across the organisation and management levels.
- Performing more pilots within organisations, regulators and government the added value of the IT reporing standard can be further explored.
- Based on the experience acquired as regards a variety of pilots, NOREA will be able to draft an audit-guideline. This guideline will be used by IT-auditors if they will be asked to provide an assurance statement regarding the IT report.

**Involvement of EU**

- Although NOREA is taking a pioneering role in Europe, this initiative must be supported internationally. NOREA has the following route in mind:
  i) international acceptance through the major accounting firms that can roll it out globally
  ii) through European bodies such as Accountancy Europe for adoption at accounting firms
  iii) in context of integrated reporting through EFRAG (European Financial Advisory Group) & through GRI (Global Reporting Initiative) for reporting standards
- To avoid proliferation of reportings and confusion by stakeholders, NOREAs designed reporting standard could become a norm for reporting on IT control by management in the Netherlands with the possibilities for further roll-out in the EU.

# Ask

- Society asks for more transparency in accountability. In todays and future laws and regulations organisations are asked to provide an IT-statement and/or to perform audits that must determine that IT control is in order. Please, we would like to ask you to join us in creating a basis for NOREAs IT-reporting initiative so that this could become an EU-norm. This to avoid an administrative burden, proliferation of reportings and confusion for stakeholders.