The IT Reporting Initiative in the Netherlands

Reporting on the organization and control of IT in a standardized manner by NOREA

Alex van der Harst
is a member of NOREA's NRI working group and a partner at KPMG Advisory N.V.

Ronald van Langen
is a member of NOREA's NRI working group, senior manager at KPMG Department of Professional Practice and chair of NOREA's Professional Practice Committee.

Mariska de Kort
is a senior manager at KPMG Advisory N.V.

Tom Verharen
is a member of NOREA's NRI working group and a junior manager at CZ.

Jurgen Pertijs
is a senior manager of internal audit at CZ.

In this article, we outline the contours of the NOREA Reporting Initiative (NRI) ([NORE24]). This initiative arose because of the need to report and be able to account for IT controls in a standardized manner. A public consultation on the so-called "IT report" took place in March 2023 and responses are currently being processed ([NORE23b]). We describe the reason for this initiative and the evolution it has undergone over the past two years. Of course, we also discuss the content of the reporting standard. In addition to the "IT report," an "IT statement" is also being considered. We will also discuss this in more detail.

Drafting a reporting standard is one thing, but its use is obviously something that must be demonstrated in practice. This is why we also outline the experiences that CZ gained during one of the pilots in which the reporting standard was applied.

BACKGROUND

By now, it is evident that Information Technology (IT) holds paramount significance across virtually all organizations. The integration of IT is indispensable for maintaining financial accounts, and in numerous instances, it assumes a pivotal role in driving operational activities for organizations. This may include administrative aspects in operations such as the import and distribution of cars, for example, as well as the control of production lines. Of course, IT also plays a crucial role in public tasks. Think of the control of our water flood defenses or the coordination in the emergency services.

When IT plays a role in operations, it is often a means for an organization to achieve strategic goals and is partly what determines an organization's valuation. In a critical scenario where an organization's viability is contingent on IT infrastructure, a poorly maintained system reliant on a limited pool of individuals for expertise can substantially diminish the organization's valuation. Conversely, a high-quality IT organization equipped to adapt swiftly to evolving circumstances would enhance the organization's overall value.

What is striking is that there are many specific accountability requirements for organizations in IT, but there is still a lack of integrated accountability. A bottleneck emerges as a result of diverse reporting formats varying in depth and scope, resulting in redundancy, increased burdens, incomparability, and ambiguity for stakeholders.

Specific obligations exist in the areas of DigiD, ENSIA and, for example, NEN 7510. Regulators such as DNB and AFM have also instituted specific accountability obligations. Internationally, the SEC recently announced a cybersecurity disclosure obligation. This is the first obligation where public disclosure is expected. In addition, a specific part of IT control – namely IT risks related to the financial reporting process and the management of those risks – is also a regular part of the audit.

Dutch Civil Code book 2 title 9 article 393 paragraph 4 is an important piece of legislation when we talk about IT within the financial statement audit:

The auditor will report on his audit to the supervisory board and the management board. He will at least report his findings with respect to the reliability and continuity of automated data processing.

Traditionally, accountants have conducted audits of financial statements with a substantive approach, employing detailed checks and numerical analysis to ensure that the information aligns with the true and fair view intended by the financial statements. During this audit, the auditor will also gain insight into IT.

Increasingly, we are seeing auditors take a "systems-oriented" approach to the financial statement audit, making use of the internal controls that have been established around IT systems. This usually leads to a combination of a system-oriented and a substantive audit approach. The auditor may report to a limited extent on the reliability and continuity of automated data processing in the report to the board and those charged with governance. The focus is only on those systems that are relevant to the financial statements and to the extent they are in scope for the financial audit. In short, the information about the "quality" – if it can be defined at all – of the automated data processing is retrieved to a limited extent as part of the financial statement audit, while it may be pertinent to conduct this assessment in a broader context for various reasons.

The identification of the gap between the critical importance of IT in a broad sense, on the one hand, and the limited provision of information about IT to supervisory bodies, such as those charged with governance and possibly other stakeholders, on the other, led to the NOREA Reporting Initiative (NRI). The aim of the NRI is to systematically illuminate how an organization has structured its IT framework to ensure that IT actively contributes to the achievement of the organization's strategic objectives. This fits in with NOREA's manifesto "Towards a digitally resilient society" ([NORE23a]), which was presented in April 2023 to State Secretary for Kingdom Relations and Digitalization Alexandra van Huffelen and to Nicole Stolk, board member of De Nederlandsche Bank. It includes the recommendation for external accountability for IT control within an organization which will boost accountability in IT control.

To ensure uniformity, it was decided to develop a reporting standard. NOREA has taken the initiative and produced a first draft and incorporated feedback received. It is important to note that this reporting standard is still under development and has no formal status yet. It is also recognized that the responsibility for and management of such a reporting standard should not lie with the professional group of IT auditors, but with an organization more appropriate for this purpose. This has not been further concretized at this stage. This reporting standard provides guidance and also identifies topics to be described that, if explained, contribute to the purpose of the IT report.

The current NRI has gone through several developments in its inception, which makes sense considering the complexity resulting from:

- a diverse landscape of types of organizations (large, small, national, international, IT-driven or not etc.);
- pre-existing standards and standards frameworks;
- the link to the financial statement audit;
- public or private distinction (public organizations should be more transparent);
- whether an organization is publicly traded (publicly traded organizations should be more transparent);
- the sector in which an organization operates (external accountability plays more of a role in highly regulated sectors such as banking and healthcare);
- different information needs of various stakeholders. Examples include understanding different aspects of IT, degree of depth, focus on past accountability or future-proofing et cetera.

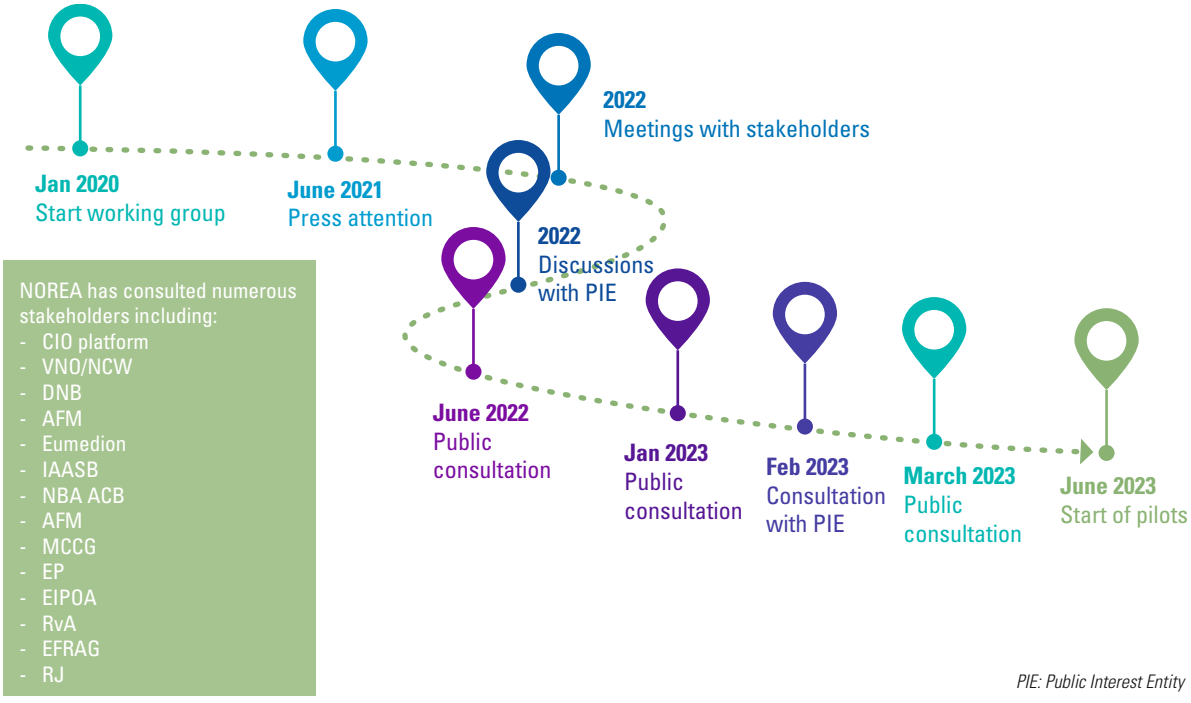
One of the first issues was whether the reporting standard should include a standards framework for minimum desired internal controls and/or control objectives. It quickly became clear that such a uniform standards framework could not be established because organizations are very different. In addition, there are already several standards frameworks on the market and an overlap with those standards frameworks did not seem a logical idea. Therefore, the NRI certainly does not include minimum required internal control objectives and internal control measures.

As the development progressed, it became evident that the primary goal is not necessarily to generate an IT report for the general public interest. It soon ran into the understandable objection that an organization does not want to reveal confidential aspects of its IT organization. This ultimately resulted in the NRI aiming to produce an IT report primarily for the supervisory body, for example, leaving it to the supervisory body to decide whether the IT report should be made public. The NRI does not include any obligation to make an IT report public, but primarily aims to provide a reporting framework to help organizations understand the state of IT.

WHAT DOES AN IT REPORT IN ACCORDANCE WITH THE NRI LOOK LIKE?

As described earlier, the IT report is not a standards framework with internal control objectives and/or measures. That does not mean it is unstructured. A design and structure has been chosen in line with the GRI Sustainability Reporting Standards ([GRI]). On the one hand, this provides a modular structure, featuring the development of six IT themes. Any other (optional) IT themes can be added to this later. On the other hand, the NRI outlines what needs to be reported for each theme, without requiring an explicit assessment of whether the current IT environment meets a particular standard/requirement such as DORA, GDPR or the Cyber Resilience Act. As an illustration, *GRI 418: Customer Privacy 2016* ([GRI16]) includes one reporting requirement with no standard setting: "report the total number of substantiated complaints

Figure 1. NOREA Reporting Initiative development timeline.



PIE: Public Interest Entity

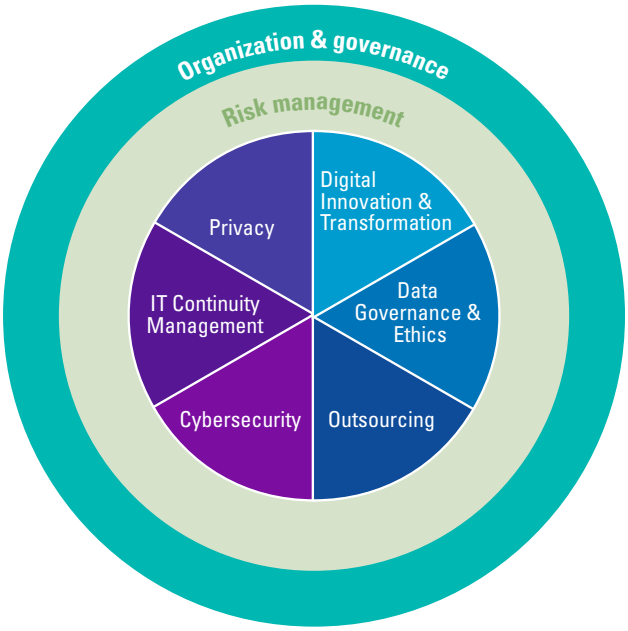


Figure 2. Coherence of generic and specific themes ([NORE23b]).

received about customer privacy breaches, and the total number of identified leaks, thefts or losses of customer data". Additionally, NOREA's Privacy Control Framework (PCF) can be used by entities to determine whether privacy protection measures are adequate in relation to the GDPR, for example, and includes 95 control measures. The PCF can lead to a Privacy Audit Proof statement.

The IT report takes a broad look at the organization of IT. In doing so, the NRI identifies two main sections. The first section deals with more general themes regarding the organization of IT and its governance, and risk management. The second section deals with specific themes that may be relevant to each organization.

In this process, the organization assesses six key IT themes by examining the existing level of IT control on one hand and juxtaposing it with the organization's aspirations in the respective theme on the other. The reporting standard pays specific attention to elements that are critical to an organization and can impact its stakeholders, including customers, suppliers, employees and other workers, regulators, investors and society. The standard currently identifies six themes:

- Digital Innovation & Transformation;
- Data Governance & Ethics;
- Outsourcing;
- Cybersecurity;
- IT Continuity Management;
- Privacy.

The reporting standard provides guidance by clarifying the scope for each theme and by describing specific reporting requirements with associated specifications to substantiate them. The reporting standard provides readers with a cohesive and standardized approach through a common framework for IT reporting. Consequently, the report enables a consistent depiction of various organizations, fostering clarity and uniformity in presenting a comprehensive picture.

Outsourcing

To paint a picture of the elaboration according to the NRI, we describe the theme of "Outsourcing" below.

According to the standard, managing outsourcing is generally addressed in Chapter 1 of the "Management of IT" report, which outlines both the organization of outsourcing and risk management as a result of disclosure "MGT-1.1: IT organization and governance".

There are also two more specific disclosures related to managing outsourcing:

MGT-OUTS-1.1 - The reporting organization shall report how it manages outsourcing using requirements and the context and scope of the outsourcing in addition to "Management of IT topics".

MGT-OUTS-1.2 - The reporting organization shall describe how it manages risks related to its outsourcing of processes and services in addition to "Management of IT topics".

An organization that has determined that the outsourcing of processes and services is material is required by the standard to report how it is being handled. Organizations describe the impact of outsourcing on their own organization and on the chain of supply and demand in which the organization finds itself.

An organization describes the establishment of outsourcing along three relevant disclosures as described in the standard:

- *OUTS-1 Outsourcing is governed and managed and the value and other overall objectives of outsourcing are monitored and evaluated.*
- *OUTS-2 Candidate providers for outsourcing of processes and services are selected, evaluated (to determine preferred candidate) and services*

are contracted, implemented and (eventually) terminated based on identified requirements.
- *OUTS-3 The delivery of services is managed based on identified requirements, including the connections (interfaces and handovers) with the rest of the organization, and service management.*

To ensure uniform reporting, the following requirements are embedded in the NRI:
- *OUTS-1.1 The organization shall report how it conducts ongoing oversight over its outsourcing portfolio, including the ongoing evaluation of the overall outsourcing performance against objectives.*
- *OUTS-2.1 The reporting organization shall report on its processes, policies and procedures for the initiation, implementation and termination of outsourcing.*
- *OUTS-3.1 The reporting organization shall report on its policies and procedures on the ongoing monitoring of the performance of outsourced processes and services. This includes responding to occurrences (e.g. incidents) and other service management aspects.*

The NRI then provides further guidance for each disclosure to achieve a proper description. By way of illustration, below is an example of guidance in relation to the second disclosure:
OUTS-2.1e The organization could describe how it handles the following topics:
- *the (re-)transfer of assets and data;*
- *documentation and archiving of the results of the termination efforts;*
- *fulfillment of contractual, compliance and regulatory obligations.*

AT WHAT LEVEL IS REPORTING PERFORMED?

The IT report is prepared by the organization and is emphatically not an audit or assurance report that, as is well known, is prepared by an independent external auditor. The organization describes the current situation in the organization at one moment in time, looking back 18 months in the description as well as 18 months ahead. As a result, choices and ambitions are explained in the report.

The report, as mentioned earlier, does not describe the design, implementation and operational effectiveness[1] of controls, but aims to provide insight into the organization of IT to relevant stakeholders. There is an explicit distinction between the IT report and standards frameworks such as NIST or ISO 27001 and between the IT report and assurance reporting standards such as SOC1, 2 and 3 and NOREA Guideline 3000. In addition, confidential detail about cyber incidents, for example, also have no place in the report.

THE ORGANIZATION DESCRIBES ITS IT ORGANIZATION AND IT CONTROLS

The purpose of the NRI, as mentioned, is to provide insight in a standardized uniform manner into how an organization has organized IT and how IT contributes to the organization's strategic goals. The organization's management is the appropriate body to report based on the NRI. Of course, the organization can also use external parties for this purpose, but the basic principle is that the organization itself is responsible for preparing the IT report.

It is relevant to circle back to the earlier assertion that the NRI is not a standards framework. For example, the NRI does not require an organization to comply with NIST or ISO 27001/2. What the NRI does ask is to describe whether, and if so, what information security standard the organization meets or intends to meet. If there are specific accountability requirements within the realm of IT, such as DORA, BIO, or NEN 7510, they will be explicitly addressed. At the same time, if the organization does not have a formal information security standard and reports it as such, this is appropriate in the spirit of the IT report.

PROVIDING ASSURANCE ABOUT THE IT REPORT

Drawing a parallel to financial statements, wherein an organization compiles financial information adhering to specific reporting standards, and an auditor subsequently reviews these statements in accordance with auditing standards, a similar process can be applied to IT reports. Herein lies the opportunity for the internal auditor or an external accountant/IT auditor to scrutinize the IT report. In this context it is possible to issue an assurance statement to the IT report, or IT statement. An IT statement is an assurance report based on NOREA

1 The design of a control measure refers to the extent to which it covers an identified risk. Implementation refers to the actual functioning of the control measure at any given time, while operational effectiveness refers to the actual functioning of the control measure over a longer, often specified, period.

Directive 3000A and includes an opinion as to whether the content of the IT report gives a true and fair view of reality to provide additional assurance for third-party users. In essence, the initial creation of reporting criteria by NOREA may not pose an issue for utilizing them in an assurance engagement. This holds true if the IT auditor collaboratively establishes agreement with the responsible party regarding the appropriateness of the criteria.

An IT report could be included in the organization's annual report. This is then complementary to other aspects, such as descriptions of various developments within or around the organization. Once more, we can draw parallels to CSRD/ESG/sustainability reporting, wherein the organization has the option to incorporate the IT report into the annual report.

Nevertheless, there are some snags to be considered. First, it is necessary to determine the role of the auditor with respect to the statements in the IT report (will a separate opinion be prepared, or should it be considered "other information"?). Another aspect at play here, which may be somewhat more recalcitrant, is the potential contradiction between the description of IT imperfections in the IT report on the one hand and an unqualified opinion on the other. There will be situations where questions may be raised about how certain statements in the IT report relate to an unqualified opinion on the financial statements. The auditor's ability to offer compelling explanations for apparent inconsistencies might not always be readily apparent to a reader.

The NRI does not aim to make the IT report a part of the annual report. We believe it is too early for that at this time and that broader experience with the IT report should first be gained so that such considerations can be evaluated.

PILOT AT CZ: CREATING AN IT REPORT

Over the past year, CZ has gained experience in preparing an IT report. CZ is part of the NRI working group of NOREA, and from that role they have initiated an internal pilot, of which they have also reported back their findings in the aforementioned working group. CZ was the first organization in the Netherlands to pilot the process of drawing an integrated picture of the themes of Digital Innovation and Transformation, Data Governance & Ethics, Outsourcing, Cybersecurity, IT Continuity Management & Privacy and preparing a related audit report.

Tom Verharen, a senior auditor in CZ's Internal Audit Department (IAD), and Jurgen Pertijs, the IT audit manager in IAD, both played distinct roles in the preparation of the IT report and audit report.

Background

A confluence of circumstances led to CZ's need for an integrated picture in the field of IT and the IT report. At the time, the CIO was relatively new to his position, and gaining insights into the organization's IT environment was highly valued from his perspective. CZ also has an IAD with REs and a strong relationship with NOREA's specialist working and knowledge groups, which gave CZ an early introduction to the NRI initiative. In addition, the report provided an opportunity to form a coherent picture of IT management, growth and ambitions.

Preparation and approach

The CZ Board of Directors commissioned a study and an IT report. The owner and person ultimately responsible for the report was the CIO. He helped determine the approach to arrive at the report and made an initial classification of the officials who needed to be involved to produce an IT report. CZ adopted a project-based approach in which information was gathered for the IT report using one workshop per theme. The senior auditor of the IAD supervised the entire project as process supervisor, providing substantive professional knowledge in the field of reporting.

Each workshop took two hours and was prepared in terms of content by the senior auditor from the IAD. Each workshop included pertinent stakeholders aligned with the specific theme. In the case of the "Outsourcing" theme, as discussed earlier in this article, key participants encompassed the procurement manager, supplier managers, and the infrastructure manager. During the workshop, all disclosures of the NRI were discussed. This included looking back and discussing ambition in that area. The workshops were supported by the secretariat to ensure proper recording.

> "Based on the disclosures in the NRI, we formulated questions for each theme to provide a good format for the workshops."
>
> –Tom Verharen (CZ)

After the information was gathered in the workshops, the CIO department created a summary for each theme that was coordinated with relevant officials. These summaries together resulted in the IT report. The IAD provided support in this process to ensure that the report was issued in accordance with the NRI standard.

The entire project to come up with an IT report required a total of about thirteen days of effort from the CIO department, and the IAD also spent about eleven days to come up with an IT report. The project had a lead time of eight weeks and resulted in a comprehensive report that was found to be very valuable from multiple perspectives.

Audit on the IT report

Already during the design of the project, the IT audit manager of the IAD planned to carry out an audit on the IT report as well to provide the board of directors with more assurance on the content of the report. To make this audit effective and efficient, CZ chose to conduct this audit during the project. An audit file was created and during the workshops, the IAD asked questions and requested additional documentation to determine the reliability of statements. The IAD confirmed observations from the IT report and supplemented them with observations from its own observation of previous audits. The IAD issued an audit report on the IT report and this, together with the report, was presented to the Board of Directors, Supervisory Board and Audit-Risk Committee. Conducting the audit required about six days of commitment from the IAD.

"Performing an audit on the drafting of the IT report was new to us. CZ's IAD issued a report of factual findings."

– Jurgen Pertijs (CZ)

The 2021-2022-2023 IT Report

The IT Report is structured along the six themes mentioned earlier. CZ has peeled off all these themes, looking back 18 months and looking ahead 18 months, in accordance with the reporting standard. All themes are described in the report based on the requirements in the standard. However, in certain cases a choice has been made regarding the depth with which the theme is described. In the case of cyber security, for example, a choice was made not to include certain details in the report.

In addition to the six specific themes, CZ also chose to describe a number of general chapters, because in practice it turned out that there were a number of topics that were repeated in each theme. These include the strategy description, the general organization and a description of the design and operation of CZ's internal risk management and control systems.

User experiences

The then newly appointed CIO responded positively to the report, appreciating the fact that it provided a comprehensive overview of the IT status at CZ in a relatively short timeframe. Furthermore, the report furnished him with a solid baseline measurement and an effective means of communication with stakeholders pertinent to his role. An additional advantage is that the IAD independently reviewed the content of the report.

It has been of added value to the BoD and SB that they could obtain an overall picture of IT in a single report written in clear language. While a significant portion of the information existed in isolation, the IT report has consolidated it, allowing for a unified perspective.

Through structured analysis of IT themes, patterns within them have become discernible. For example, it is clearly noticeable that CZ's role as an IT employer is important to CZ when looking to the future.

The IT report is perceived by users as an enhancement to the test results communicated periodically in terms of the operation of general IT controls (GITCs). Whereas GITCs are more operational in nature, this report is much more tactical and strategic in nature because of the way the disclosures are prepared.

"The IT report really resonated well with the Supervisory Board; they appreciated the integrated picture."

– Jurgen Pertijs (CZ)

Experiences and lessons learned from the project

CZ reflects on the "IT report" project with a favorable perspective. The NRI was not experienced as an oppressive straitjacket and enabled the CIO to present its story in a structured way. The CIO has chosen to continue to issue a report periodically. The specific form this will take has yet to be determined. CZ plans to produce an abbreviated version of the IT report in 2024.

Because of the positive experience, the IAD has chosen to shape its audit programs in the future along the report's six themes.

In a subsequent report, in addition to the entire CIO office, business stakeholders as well as the risk management department will be further involved in the workshops. Business stakeholders own the primary process and are therefore also responsible for the use of IT in it. Risk management manages the risk management process, which also pays broad attention to IT-related risks. Experience has shown that these actors also play an important role in drawing up an integral picture of IT control.

The pilot at CZ has brought NOREA new insights. For example, the general chapters as defined by CZ have now become a permanent part of the NRI standard.

CONCLUSION

The NOREA Reporting Initiative is an initiative created to report and account for IT governance in an integrated and standardized manner. The initiative was developed because of the growing importance of IT in almost all organizations and the need to account for it internally or externally.

The NRI is a reporting standard that also allows for the provision of additional assurance on the fairness of such a report by an independent auditor ("IT statement"). The NRI is not a standards framework for minimum internal control measures, but it does require organizations to describe, for example, whether, and if so, what information security standards they comply with. The NRI aims to provide insight in a standardized way into how an organization has organized IT and how IT contributes to the organization's strategic goals.

We believe that the NRI fleshes out the growing importance of IT in the functioning and futureproofing of organizations. The structure outlined by the NRI offers guidance in identifying the pertinent

themes accurately, ensuring recognition by stakeholders when multiple IT reports are compared side by side. Organizations are enabled to report periodically in accordance with this standard. In doing so, because of the standardization, comparisons can easily be made between multiple reporting periods. We can also imagine that this standard can be used in due diligence investigations; the standardization and recognizability will be a big plus for investors. In a broader sense, the standard can also be used to perform a baseline measurement and based on this, define actions to achieve the desired level of ambition. Internal audit departments can leverage the standard to, for instance, systematically explore the aforementioned topics over a three-year cycle. This approach facilitates engaging in comprehensive discussions with management, utilizing the gathered information to explore how IT can effectively contribute to the organization's overarching goals. Because of the standardization and the fact that there is a well-thought-out reporting standard, the application possibilities are, in our opinion, numerous.

When it comes to reporting requirements from various regulators, the pressure on organizations is high. Many organizations have to comply with specific laws and regulations, which takes up the available time of not only the second line but also the first line. In that light, ESG regulations will also require a lot of time from organizations in the coming period. In our opinion, the NRI will not further increase the compliance-related workload in the first line. Preparing an IT report in accordance with the NRI obviously takes time, but it reflects the existing situation, not prescribing which requirements an organization must meet. Certainly, the formulation of the IT report might prompt an organization to consider addressing specific facets related to IT control in a different or enhanced manner. However, such considerations arise from an internally driven impetus for change aimed at enhancing the overall organization.

We therefore see the NRI as a sound tool to provide insight to supervisory bodies and as a means for organizations to improve themselves. We believe it is currently too early for mandatory application. More experience should be gained with the standard in the coming period. Anticipating a heightened demand from supervisory bodies and investors for reporting on the IT environment, we recognize that the outlined standard serves as a robust foundation. However, its efficacy is greatly enhanced when complemented by an assurance statement, affirming the accuracy and integrity of the report. This step propels it beyond a mere self-assessment, amplifying its overall value.

References

[NORE23a] NOREA. (2023, March 30). *NOREA-Manifest Op naar een digitaal weerbare samenleving.* Retrieved from https://www.norea.nl/nieuws/norea-manifest-op-naar-een-digitaal-weerbare-samenleving

[NORE23b] NOREA. (2023, March 31). *Norea Reporting Initiative v0.11.* Retrieved from https://www.norea.nl/uploads/bfile/6357a197-6fd2-4904-b43e-7a85e123cb59

[NORE24] NOREA. (2024). *Werkgroep Reporting Initiative.* Retrieved from https://www.norea.nl/organisatie/werkgroepen/werkgroep-norea-reporting-initiative

[Fijn23] Fijneman, R. (2023, January). *IT governance report: food for thought and next steps.* Board Leadership News KPMG.

[GRI] Global Reporting Initiative. (n.d.). *Standards.* Retrieved January 23, 2024, from https://www.globalreporting.org/standards/

[GRI16] Global Reporting Initiative. (2016). *GRI 418: Customer Privacy 2016.* Retrieved from https://www.globalreporting.org/standards/media/1033/gri-418-customer-privacy-2016.pdf

About the authors

Alex van der Harst is a member of NOREA's NRI working group and a partner at KPMG Advisory N.V. with more than 25 years of experience in the fields of IT audit (RE), project management, information security and IT audit in the context of the annual audit. He was a board member of NOREA until July 2023 and has a broad portfolio of private and listed organizations, mainly project organizations and clients in the energy sector.

Ronald van Langen is a member of NOREA's NRI working group and serves as a senior manager at KPMG Department of Professional Practice (DPP). His areas of focus within DPP include audit and assurance methodology, IT in audit, XBRL and ESG assurance. He also chairs NOREA's Professional Practice Committee.

Mariska de Kort is a senior manager at KPMG Advisory N.V. in IT audit. She has a background in clinical informatics and holds a degree in public administration. She has experience auditing companies in the areas of healthcare, life science and wellness.

Tom Verharen is a junior manager Internal Audit Department at CZ and is a member of NOREA's NRI working group. He is also a member of the NOREA Knowledge Group on Cybersecurity and co-author of the NOREA Handreiking Security Operations Center Maturity Framework. Within CZ he is involved in audits on, for example, IT governance, artificial intelligence and cybersecurity.

Jurgen Pertijs is a senior manager Internal Audit Department at CZ and in that role responsible for IT and operational audits within CZ. He is also a member of the working group for the revision of the Maturity Model Information Security of NBA-LIO and NOREA.

NOREA's NRI working group consists of approximately twenty people representing various organizations, including EY, KPMG, Deloitte, PwC, BDO, Mazars, ACS, TOPP Audit, Verdonck Klooster and Associates, ABN Amro, UWV and CZ. A full list is included in the version released for public consultation.