NOREA Taskforce ESG Position Paper:

The role of the IT auditor in audits of sustainability information

Version 1.0

July 31, 2023

Preface

This document presents an initial view of NOREA on the role of the IT auditor within audits of sustainability information, developed by NOREA, the Dutch Association of chartered IT-auditors (Register EDP Auditors; 'RE'). This document was developed to discuss the role of IT-auditors within examinations and reviews and to substantiate the (need for) implementation of IT related audit procedures when conducting examinations or reviews of sustainability information by practitioners. This document is drafted as a position paper and is open to discussion, to invite other practitioners and professional bodies to provide their view on the role of the IT auditor.

This document was drafted in response to the upcoming requirements for audits and reviews of sustainability and other nonfinancial information from the CSRD (Corporate Sustainability Reporting Directive). Audits of sustainability information are considered in the context of all relevant laws and regulations, thus not being limited to the CSRD but also including, for example, the SFDR (Sustainable Finance Disclosure Regulation).

There are several considerations and limitations that need to be taken into account when considering the contents and timing of this discussion document:

- CSRD reporting is still in its infancy. The CSRD is an evolution (replacement) of the existing Non-Financial Reporting Directive (NFRD[1]). For the NFRD assurance is not required. Under the CSRD in turn the goal is to provide limited assurance with the disclosed information, turning into reasonable assurance in the future. Given this evolution we note that practitioners are still gaining expertise in how to conduct CSRD audits with limited (or reasonable[2]) assurance. This implies that this document will probably evolve in a similar manner. However, irrespective of the level assurance required the role of the IT-auditor in CSRD reporting is deemed essential;
- IT systems that are being used within the scope of CSRD are being developed and the current market for these systems is somewhat restricted to a few software vendors. The market is developing fast and we expect this market to reach full maturity over the coming years, as more companies will have to report under the CSRD directive[3]. The introduction of new vendors and thus new software (applications) to this market will bring about new developments, opportunities as well as new risks. This will influence the discussion and the opportunities that exist to accept, mitigate, transfer and avoid these risks;

We expect this document to change into a framework (guiding principles) at some point in time. Currently, we are not able to predict this moment. However, the taskforce will continue to monitor the developments and will enhance this document or propose a framework if such an opportunity arises.

[1] Directive (EU) 2014/95/EU

[2] Adoption of reasonable assurance standard by the commission is expected to be October 1, 2028.

[3] The adoption timeline shows an evolving reporting requirement from 2025 to 2029.

Committee participants

On behalf of the NOREA Taskforce Environment, Social, Governance (hereafter: ESG) the following members contributed to the development of this discussion document:

Chairman, main contributor	Jeroen Francot	BDO
Main contributor	Roel Ronken	HLB Witlox Van den Boomen
Main contributor	Meghan Tjallinks	EY
Main contributor	Maryam Amaador	KPMG
Main contributor	Manon van Rietschoten	KPMG
Taskforce member	Jeffrey Martens	Grant Thornton
Taskforce member	Marly van der Meij	MN
Taskforce member	Jeroen van Schajik	BDO
Taskforce member	Daan Smulders	EY
Taskforce member	Jan Stoker	ABN AMRO

Version control

Version	**Date**	**Amendments**
0.1	28-04-2023	Initial outline and draft
0.2	08-06-2023	First official draft
0.3	19-06-2023	Revisions and version submitted to NOREA professional practice committee
1.0	31-07-2023	First version for public consultation

Table of contents

1. General overview

1.1 Introduction

On January 5, 2023, the European Union Corporate Sustainability Reporting Directive[4] (hereafter: CSRD) entered into force. The goal of the CSRD is to make corporate sustainability reporting more common, consistent and standardized within the European Union (EU). Guidelines have been established as to which companies have to adhere to this directive[5], which is to be further implemented into local law. Companies that have to adhere to this directive as implemented in local law are required to file an annual report using the CSRD's forthcoming sustainability taxonomy on how sustainability influences their business, as well as the company's impact on people and the environment. The reporting requirements are being drafted in the EU Sustainability Reporting Standards (hereafter: ESRS) by the European Financial Reporting Advisory Group (EFRAG). The final standards have been adopted by the European Commission as delegated acts in July 2023.

Under the CSRD it is established that there is a clear need for a robust and feasible reporting framework that is accompanied by effective audit practices to ensure the reliability of data and avoid greenwashing and double counting. Further, to be able to report on the ESRS requirements, it is expected of companies to take into account the availability and reliability of data (AFM, 2023). As a result, there is a growing discussion and importance on the role IT (and in accordance, an IT auditor) should play in the context of CSRD and ESRS, but also other audits of other nonfinancial information. The directive states that audits of sustainability information can be performed by other auditors than those performing the statutory audit of the financial statements – as long as these other auditors are accredited in accordance with Regulation (EC) No 765/2008. We believe that Registered EDP-auditors (RE) should play a role in these audits as such as a subject matter expert[6] (as an IT-auditor) to (the team of) any other auditor that is ultimately responsible for the audit engagement. Expertise with regard to ESG reporting and other nonfinancial information is something that all practitioners such as chartered accountants and IT auditors still need to develop, and as such IT auditors should follow these developments closely. Conversely, IT auditors already have subject matter expertise with regard to reliability of data and other relevant factors. Therefore, this document seeks to provide guidance on the role an IT-auditor can play in the audits of sustainability information performed considering the CSRD and ESRS.

With the CSRD and ESRS coming into effect we believe it is very relevant for IT auditors to participate in discussions and developments surrounding ESG reporting as early as possible, as there is a major role that IT auditors may play with regard to (assurance over) ESG data and other nonfinancial information; a role that an IT auditor is perfectly suited for as a subject matter expert on data quality and internal controls over IT systems and processes.

The purpose of this document is twofold in this sense. Firstly, this document seeks to address discussions points as well as give preliminary guidance on the role (an) IT(-

[4] Directive (EU) 2022/2464

[5] The directive will apply to all large EU companies (including EU subsidiaries of non-EU companies) exceeding at least two categories, being: 1) more than 250 employees, 2) a turnover of more than €40mln and, 3) total assets of €20mln. Non-EU companies that have a turnover of above €150 million in the EU will also have to comply.

[6] Subject matter expert may refer to the expertise of an IT-auditor with regards to his knowledge of Information Systems on CSRD, but may also be more specifically related to his knowledge on the reliability and accuracy of data, operating effectives of IT and Information Systems.

auditor) plays in the context of CSRD and ESRS. Secondly, this document addresses the IT audit perspective on sustainability reporting.

1.2 Structure of the position paper

This document is structured in a way that it follows the draft outline of the ESRS. The ESRS is built up into general requirements which are overarching (ESRS 1 and 2), which are then followed by specific topics for Environment (E1 to E5), Social (S1 to S4) and Governance (G1). Companies need to determine, based on guidelines set out in the CSRD and ESRS which topics are relevant to report on, where E1 (climate change) and S1 (own workforce, if the company employs more than 250 FTE) are mandatory. Each topic lists the general requirements of the information and data that must be included in the ESG report. In chapter 2 we present a number of relevant topics that can be considered overarching and focus on the general requirements (ESRS 1 and 2). Furthermore, we address a number of points of attention related to the specific ESRS drafts (E1 – E5, S1 – S4 and G1). This document ends with a conclusion.

1.3 How this position paper was established

This position paper was developed by the ESG taskforce of NOREA in 2023. First, a preliminary analysis of the ESRS reporting requirements was performed and discussed within the Taskforce, which was further deepened by peer reviews. We refer to Appendix 1 for a detailed overview and have outlined the main overarching discussion points in Chapter 2. Appendix 1 includes an overview of each ESRS topic, for which main IT related considerations are included, as well as examples of such considerations. While there is clear overlap of the considerations for each topic, it is clear that even only the mandatory topics (i.e., E1 and S1 [when considering entities with more than 250 FTE]) introduce major IT considerations. As such, any additional topics that are included based on the stakeholder dialog and/or materiality analysis only serve to increase complexity and reliance on IT (related) measures.

2. IT auditor role in context of sustainability information

2.1 Relevant topics

2.1.1 Reliability and availability of data

To comply with CSRD, ESRS and other sustainability related standards such as SFDR, a lot of new data on environmental, social and governance data needs to be collected, transformed and reported on (AFM, 2023). In addition, from an internal perspective this data is also relevant and useful for tracking and managing sustainability objectives. Robust processes for recording ESG data have often not yet been set up in the same manner as for recording financial data for financial statements. The literature and existing research that looks into relationship between sustainability reporting and data quality is scarce. Most of the research focuses on the outcome side, meaning data quality in the report and the use of these reports by investors and market parties (Watson & Wray, 2022). In this context it must be stated that on the output side, data quality is considered as being low and it is difficult to compare across organizations (Lashitew, 2021). In turn research that focuses on data quality in the context of sustainability on the input side seems to be lacking.

Considering financial statements, robust processes are in place on the input side, e.g., for administering journal entries, consolidating entities, applying segregation of duties, etc. However, for ESG data such processes are often not in place or at the very least not as sophisticated as financial statement data. Furthermore, processes with regard to internal control often do not (yet) apply to ESG data. In addition, ESG data often also comes from

multiple sources, both internal and external from parties in the value chain. Data is collected from different (types of) systems and locations and is registered, compiled and finally reported in different ways. To be able to form an opinion based on this data, it is therefore important that it is reliable and that it reflects reality. If this data is used to achieve objectives such as net zero emissions, however the underlying data is incorrect, the question is whether the measures taken are effective and whether objectives are achieved.

We pose that reliability of data is key in any audit, whether this concerns financial statement audits or audits of sustainability information. As such, the Taskforce ESG believes that reliability of data should be a key concern in audits of sustainability information and that specific attention should be directed towards IT and (automated) data processing. This discussion document aims to provide an overview of those procedures and controls that should be considered in relation to audits of sustainability information.

An auditor of sustainability information will need to consciously think about:

- which data (or system) contains source data and how data is recorded in these systems;
- whether checks should be carried out to determine that the records are correct;
- which checks should be carried out to ensure that the data aggregation runs smoothly and is complete, and that no data is left out.
- the aggregation level of data.

This also means that, on the one hand, relevant data can be easily collected and reported. It is therefore important to embed data reliability in the organization's processes. We consider input controls, control measures related to editing data, storage and data integrity, and output controls relevant in this context.

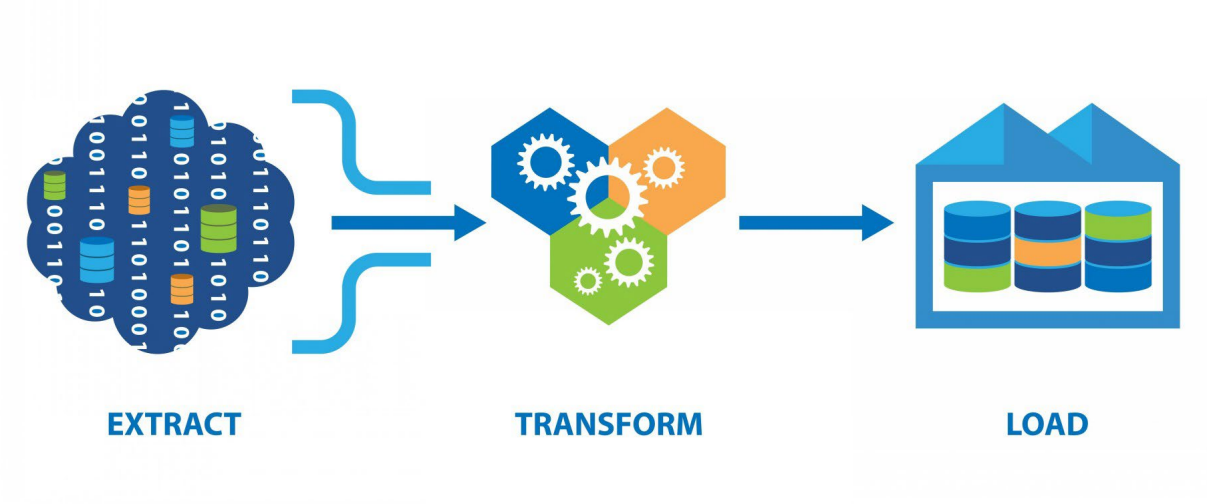
Reliable data leads to applicability, comparability and trust. Data that is relevant to the ESG report, which can be managed and used to make analyses regarding sustainability and related objectives. Data that can be converted into information that contributes to a reliable ESG report for all stakeholders. For the ESG report, it is therefore all the more relevant to ensure the reliability of data, both inside and outside the organization. We believe an (IT) auditor can play a great role in this.

In appendix 1, it is indicated for which ESRS topics reliability and availability of data is considered to be relevant.

2.1.2 Data governance

Next to reliability of data itself, we believe that appropriate and robust processes with regard to data governance are also relevant for data reliability. This is in line with for instance the DAMA-DMBOK 2[7] model in which data governance is seen as the hub from which 10 data management knowledge areas radiate, one of them being data quality. Data can be extracted, transformed, loaded and recorded by the organization itself, or by external sources. From there, reliability must be guaranteed, and the way data is created is an important aspect of this. If data reliability is not embedded in the organization's processes and procedures, then it matters little to what extent IT systems support the organization as 'garbage in' means 'garbage out' and an IT system itself does not guarantee the reliability of data.

[7] This is considered to be the most well-known and most frequently used guide in the Data Management community.



The lack of a clear governance structure, where responsibilities regarding data are not always properly assigned within the organization, may lead to additional (audit) risks. Finally, organizational measures in relation to processes and systems are also relevant, such as internal control measures regarding the recording, modification or deletion of (ESG) data. Unauthorized access to and modification of data in systems can cause it to become unreliable.

In appendix 1, it is indicated for which topics integrity of data is considered to be relevant.

2.1.3 Data Quality

Data quality can be defined as the planning, implementation and control of activities that apply quality management techniques to data, in order to assure it is fit for consumption and meet the needs of data consumers (DAMA-DMBOK2, 2017). As mentioned before, many companies have sound processes in place with regards to internal control and financial statements (e.g., journal entries processing). However, on the non-financial reporting and ESG reporting side, there is room improvement in terms of data quality. Financial and non-financial/sustainability data should be equally reliable, thus requiring high quality data.

Data quality in itself is a vast field and several dimensions and quality aspects exist, defining data quality. The most common dimensions (DAMA NL, 2020) being:

- Accuracy: The closeness of data values to real values;
- Availability: The degree to which data van be consulted or retrieved by data consumers or a process;
- Clarity: The ease with which data consumers can understand the metadata;
- Completeness: The degree to which all required records in the dataset are present;
- Consistency: The degree to which data values of two sets of attributes (within a record, within a data file, between date files and/or within a record at different points in time) comply with a rule;
- Currency: The degree to which date values are up to date;
- Punctuality: The degree the period between the actual and target point of time of availability of a dataset is appropriate;
- Timeliness: The degree to which the period between the time of creation of the real value and the time that the dataset is available is appropriate;
- Traceability: The degree to which data lineage is available;
- Uniqueness: The degree to which records occur only once in a data file;
- Validity: The degree to which data values comply with rules.

As can be deduced from this list, each of these dimensions carries some kind of weight related to sustainability information. For instance, ESG data needs to be complete in order for any user to carry value or form sound conclusions, whereas at the same time data needs to be current and timely available and should be able to be traced back to its source (system). Given the current maturity of the ESG and sustainability information reporting market (and systems) we see ample opportunity for growth with regard to sustainability information. We feel that companies, auditors and regulators need to focus their efforts on ways to improve data quality and address the dimensions as raised above related to sustainability information. After all, high quality data can assist with forming conclusions and it creates a clear and accurate picture (in terms of ESG data) to the market.

There a number of ways we think data quality of ESG data can be improved, for instance:

1. Data should be assessed and understood. Sources of data need to be identified and at the source point, data quality should be (initially) assessed;
2. There should be a baseline as to what the minimum degree of data quality should be. This baseline should be used within the company and preferably within the eco-system that exists, as to guarantee that all participants are aware of what makes high quality ESG data;
3. Metadata is critical to managing the quality of data. The quality of data is based on how well it meets the requirements of data consumers. Metadata defines what the data represents. Therefore in an ESG setting it should be clear what data is all about and what ESG data represent, in such a way that everybody has the same understanding, for example from the requirements of data and data definitions as stated in reporting standards. Or from the ESG data that is being collected and that all users have the same understanding of what the collected data means and should be interpreted;
4. At the earliest point, controls should be put into place in order to for instance minimize the risk of incomplete or inaccurate data. We refer to the use of application controls, IT dependent manual controls as well as manual controls and tweaking them, if necessary and using them in the field of ESG reporting and safeguarding ESG data quality;
5. Create awareness amongst employees and users of the importance of data quality. High quality ESG data can only be achieved if everybody understands the importance, preferably if this is derived from a long-term ambition or plan;
6. Lastly, we recommend frequently auditing and assessing ESG data quality, internally (as part of monitoring controls at the entity) as well as externally. Processes should be frequently checked and it should be determined whether ambitions/plans are being realized and ESG data quality is indeed improving as expected (to the level of high quality needed).

2.1.4 Data confidentiality and data privacy

It goes without saying that in any situation safeguarding confidentiality and privacy (of data) are of the utmost importance. Consider the General Data Protection Regulation (GDPR) and the effect that this regulation has had (and is still having) on companies within the European Union. This has resulted in consumers and companies becoming more aware on how privacy of data is safeguarded and there is an ever-increasing focus on what data is disclosed and what measures are in place in order to safeguard confidentiality and privacy of data processing.

Research has shown that consumers are placing a lot of importance on the way organizations interact with them and the ethical use of data (De Chazal, 2022). Linking this to the table in appendix 1 we distinguish a number of attention points that should be

considered. Safeguarding the confidentiality of environmental data can be deemed of importance in order to uphold the reputation of a company (e.g., S3 – Affected Communities). Furthermore, taking privacy measures is relevant whenever a company is dealing with privacy-sensitive data in the context of Sustainability reporting (e.g., S1 – own workforce or S2 – workers in the value chain), for example for personal data related to gender or disabilities. This implies that companies as well as auditors will have to look at those controls that have been put into place in order to safeguard both confidentiality and privacy. These controls may not be specific to Sustainability Reporting, but it is highly likely that these controls have already been put into place given the importance this data has beyond the context of sustainability reporting.

In appendix 1, it is indicated for which topics reliability and availability of data is considered to be relevant.

2.2 IT auditor role in context of audits of sustainability information

With the new regulations, new systems for the collection and registration of ESG data are also being developed and brought to the market. While some of these systems are developed by known software developers with experience in (financial) reporting or ERP applications, many new developers seek to quickly fill an increasing need for new systems (D'Souza & Singh, 2022). Though well-known developers with experience may understand the requirements in terms of internal controls and General IT Controls that should be placed on such systems (although, even then this is not guaranteed), developers new to these kinds of systems may overlook these requirements, introducing or further increasing risks with regard to reliability of data. As such, the Taskforce ESG believe IT should have a prominent role in preliminary risk assessments with regard to ESG and sustainability reporting (systems).

Furthermore, when auditing forward looking information in terms of CSRD requirements, such as middle term or long term KPI's and goals, IT may also play a role in determining forecasts and expectations through modeling of, for example, decreases in emissions. The reliability of systems providing forecasts based on data provided by the organization is key in determining whether the forecast is realistic and an accurate representation of expectations. Additionally, if these systems provide inaccurate forecasts, for which in audits of the actual data in later years it becomes apparent that these forecasts were not realistic, the procedures performed by the auditor may be questioned.

Considering the key discussion points mentioned above it logically follows that (at least) the following may be relevant for the (IT) auditor in regard to audits of sustainability information:

- Risk assessment: the auditor should assess those risks arising from the use of data and systems that may impact the completeness, accuracy, and/or timeliness of ESG reports;
- General IT Controls and (automated) IT controls: Based on the risk assessment, an (IT) auditor should consider those General IT Controls and (automated) IT controls necessary to mitigate the identified risks;
- Controls over (reliability of) data: Based on the risk assessment, an (IT) auditor should consider those other controls (automated, manual, or both) necessary to mitigate the identified risks. Furthermore, controls over data are relevant when determining if data is of high enough quality to be used for data analyses.

In addition to the discussion above, COSO (2023, *"Achieving effective internal control over sustainability reporting (ICSR): building trust and confidence through the COSO internal*

control—integrated framework") also puts increasing focus on internal controls over IT, mentions the following topics, supporting the discussion included in this discussion document:

- The implementation of general IT controls;
- Oversight over structured and unstructured data;
- The use of commercial IT platforms for producing and delivering sustainability information;
- The use of tagging in digital reporting; and
- Ensuring oversight of outsourced, third-party service providers.

Most notably, when listing the top 10 takeaways (The Committee of Sponsoring Organizations of the Treadway Commission, 2023, page 105), internal controls and IT controls are mentioned as the number 2 takeaway. It is therefore clear that IT cannot be ignored as a major topic within audits of sustainability information, as doing so would leave relevant risks outside of the scope of the engagement, resulting in increased audit risk.

In the first year(s) where reporting under the CSRD is mandatory (starting with reporting over the year 2024), limited assurance will be required and must be verified by a third party. At a later stage it is expected to transition towards reasonable assurance. Although the objective is to have a similar level of assurance for financial and sustainability reporting, a progressive approach is needed (European Commission, 2021). In this transition, the role of the IT auditor should be part of the discussion. Procedures such as (IT) risk assessments are equally relevant within limited assurance audits and should therefore be part of the audit approach.

2.3 Data collection, processing and reporting

When considering ESG reporting, systems for reporting ESG data and metrics should also be considered within the context of IT. While the abovementioned factors broadly apply, organizations may use specific systems for aggregating and reporting data, which may be used internally as well as externally. Such systems may range from general reporting or dashboarding systems, to more complex environments including datawarehouses or datalakes. When considering data in the context of ESG reporting it may therefore be relevant for the auditor to include these systems in the scope of the engagement.

There are multiple factors to take into account, such as the means by which data is aggregated in systems (e.g. through interfaces) and which data validations are applied in order to guarantee accuracy, completeness and timeliness. Furthermore, when data is collected externally, connections to external sources must be considered. In addition to the sources and aggregation of data, transformation of data within systems may also be relevant, for example when calculations or other transformation models are applied.

Lastly, under the CSRD, electronic reporting by means of XBRL will be mandatory, which may lead to further (IT related) challenges in terms of reporting systems and internal controls related to these systems.

2.4 IT auditor role in related assurance engagements

In addition to the role of the IT auditor in the context of audits based on CSRD or other sustainability related audits, IT auditors already perform audits of nonfinancial information. This includes, among others, audits based on ISAE3000, ISAE3402 and SOC 2. As such, IT auditors (Register EDP Auditors in the Netherlands) are in fact trained and educated specifically to provide assurance on topics unrelated to financial information, where (internal) controls as discussed in the previous sections of this document are key. As such, it stands to reason that practitioners with relevant expertise regarding nonfinancial

information can (and should) play a role in (the teams of) audits of sustainability information on the basis of CSRD.

Furthermore, as part of the CSRD, companies will need to report data from throughout the value chain. This means that data must be collected from, for example, external suppliers, shipping providers, etc. It is therefore expected that assurance with regard to external data will become necessary in order to form a conclusion with regard to this external data. As such, assurance (engagements) related to third parties providing data or services related to an organizations sustainability efforts will play a part in gaining assurance over external sources in the value chain. It is currently unclear whether assurance over such external data or services may be performed under current standards such as ISAE3000 or ISAE3402, or whether new standards aimed specifically at assurance over sustainability procedures or data may be developed.

2.5 Member state option in CSRD directive

Recently the Dutch minister of finance wrote the following in the ''progress report for the future of the accounting sector'' (please note that we both included the original Dutch text and the English translation) (Kaag, 2023);

"Sustainability reporting; The tasks of audit firms are expanded with the introduction of the Corporate Sustainability Reporting Directive (CSRD). With the introduction of this directive, companies must report on the sustainability impact and risks. Accountants examine these reports. The directive contains a member state option to also invite parties other than audit firms (RA / CPA auditors) to audit the sustainability reports. The "Kwartiermakers Accountancy" see advantages in this. For example, it can ensure that companies can find an auditor more easily and it relieves the workload at audit firms. I also see that the Member State option can help broaden the number of people who can audit sustainability reporting and that this can bring benefits. In order to gain a better insight into this, I will include a question about this during the consultation of the draft legislation for the implementation of the CSRD. I also take the considerations of the quartermasters into account in the decision-making."

"Duurzaamheidsverslaggeving; De taken van accountantsorganisaties worden uitgebreid met de komst van de Corporate Sustainability Reporting Directive (CSRD). Met de komst van deze richtlijn moeten ondernemingen rapporteren over de duurzaamheidsimpact en -risico's. Accountants controleren deze rapportage. De richtlijn bevat een lidstaatoptie om ook andere partijen dan accountantsorganisaties de duurzaamheidsverslaggeving te laten controleren. De kwartiermakers zien daar voordelen in. Zo kan het ervoor zorgen dat ondernemingen makkelijker een controleur kunnen vinden en het verlicht de werkdruk op accountantsorganisaties. Ik zie ook dat de lidstaatoptie kan bijdragen aan het verbreden van het aantal mensen dat duurzaamheidsverslaggeving kan controleren en dat dit voordelen kan opleveren. Om hier beter inzicht in te krijgen zal ik hierover bij de consultatie van het voorstel van wet ter implementatie van de CSRD een vraag opnemen. Ook de overwegingen van de kwartiermakers neem ik mee in de besluitvorming."

The taskforce wants to explore whether IT auditors (RE) could take a prominent position for ESG reports within a IT-driven environment using the member state option as mentioned in the CSRD. The first action here is exploring how the IT auditor could gain the required understanding of sustainability reporting and fulfill the ESG – specific training requirements.

3. Conclusion

In conclusion, this document has provided a number of topics of discussion and relevance regarding audits of sustainability information and the role of the IT auditor within these audits. Based on expectations of the requirements of such audits, as well as discussions

from external sources such as AFM and COSO and the EC, it clearly follows that IT and data related risks are relevant in providing assurance with regard to sustainability information. Appropriately responding to such expectations involves assessing IT risks and related IT- and data controls, which necessitates the role of the IT auditor within engagement teams. With numerous IT related risks, it is called into question whether appropriate assurance can be provided if such risks are not addressed. Therefore, the Taskforce ESG sees the role of the IT auditor within audits of sustainability information as paramount, which is why the Taskforce strongly advocate the IT auditor as a practitioner capable of addressing these risks, and being equally capable of providing assurance regarding sustainability information.

Furthermore, we would like to explore the possibility for an IT auditor to provide assurance on sustainability reports (particularly in IT-dominant environments), provided that this IT auditor meets ESG - specific training requirements (to be defined).

We would like to invite the reader to share your thoughts / feedback on the involvement of IT auditors in the audit of sustainability information. The Taskforce would like to ask the reader the following questions:

- **What does the reader think of the role of IT auditor as substantiated in the position paper?**
- **Is the role of the IT auditor in audits related to sustainability information sufficiently (clearly) substantiated?**
- **Are there topics that the reader believes are relevant in the context of sustainability information that have not yet been identified in the position paper?**
- **In what way can the IT auditor gain knowledge about sustainability / meet the education requirements as named in the "*concept wetsvoorstel implementatie richtlijn duurzaamheidsrapportering*"?**
- **Could an IT-auditor, in your view, be the assurance provider (lead engagement partner) for sustainability information? Please include a rationale for your answer.**

The deadline for responses is September 30, 2023. Responses may be sent to norea@norea.nl

Appendix 1

No.	Topic	Key points to consider	Examples
1.	Environmental		

1.1	E1 Climate change control	• Reliability of data
		• Availability of data (including external data sources)
		• Integrity of data
		• Accuracy
		• Completeness
			• Emission calculations or estimations, ranging in complexity from scope 1 to scope 3.
			• Collection of data from internal as well as external sources, such as fleet management, office management etc.
			• (Calculation of) carbon credits.
			
			• Application controls related but not limited to:
			  ○ Emission registration and calculation
			  ○ Biomass calculations or estimations;
			  ○ Interfaces for data exchange
			  ○ Emission reductions

1.2	E2 Pollution	• Reliability of data
		• Availability of data
		• Integrity of data
		• Accuracy
		• Completeness
			• Potential financial effects due to material pollution-related opportunities and how the undertaking may financially benefit from material pollution-related opportunities. Examples being (of which accuracy and completeness has to be assessed):
			  ○ Share of net revenue
			  ○ Operating and capital expenditures
			  ○ Provisions for environmental protection

			• Calculations potentially performed on emission types, i.e. air pollution, water, inorganic pollutants, microplastics.
1.3	E3 Water & Marine	• Reliability of data • Availability of data • Integrity of data • Accuracy • Completeness	• Operations disclosure & measurement of water consumption. • Availability of internal and external data with regard to water consumption and disposal. • Financial effects due to material risks arising from water and marine resource related and/or dependencies such as impact on cashflow, performance, etc.
1.4	E4 Biodiversity	• Reliability of data • Availability of data • Integrity of data	• Include a description of its material inflows: products (including packaging) and materials, and property, plant and equipment used in the undertaking's own operations and along the value chain. • Data availability, from internal as well as external sources, is of importance. • Calculation methods used.
1.5	E5 Resource use & Circular Economy	• Reliability of data • Availability of data • Integrity of data	
2. Social			
2.1	S1 Own workforce	• Reliability of data • Availability of data • Integrity of data • Confidentiality • Privacy	• Registration and reporting of sensitive/personal data • Reliability of data in general regarding personal data: data definitions, the registration of data (including segregation of duties or other application controls to guarantee reliability) and data quality controls.

			• The possibility of auditing the reliability of (sensitive) personal data • S1-7 asks for contextual data and changes in data over time • The use of external sources, calculation methods or other methods when making estimations if data is not present. • Confidentiality and privacy aspects of personal data, including logical access controls.
2.2	S2 Workers in the value chain	• Reliability of data • Availability of data (including external data sources) • Integrity of data • Confidentiality • Privacy	• Registration and reporting of sensitive/personal data • Reliability of data in general regarding 'personal' statistics: how is this captured, are application controls possible? Accuracy, completeness, some form of 'integrity'? • Contextual data and changes in data over time requires tracking systems and models. • The use of external sources, calculation methods or other methods when making estimations if data is not present. • Confidentiality and privacy aspects of personal data.
2.3	S3 Affected communities	• Reliability of data • Availability of data • Integrity of data • Completeness • Confidentiality	• Channels for raising issues might have IT (related) components, including integrity and confidentiality considerations. • Issues that are raised must be monitored and addressed. Completeness and timeliness aspects, as well as documentation may play a role here. • Tracking of effectiveness of actions requires systems, which includes

			completeness, integrity and confidentiality considerations.
2.4	S4 Consumers and end users	• Reliability of data • Availability of data • Integrity of data • Completeness	• information-related impacts for consumers and/or end-users (for example, privacy, freedom of expression and access to (quality) information • Channels for raising issues might have IT (related) components, including integrity and confidentiality considerations. • Issues that are raised must be monitored and addressed. Completeness and timeliness aspects, as well as documentation may play a role here. • Tracking of effectiveness of actions requires systems, which includes completeness, integrity and confidentiality considerations.
3. Governance			
3.1	G1 Business Conduct	• Reliability of data • Availability of data • Integrity of data	• Includes many qualitative measures, policy and procedures. Tracking of issues, incident, training, awareness etc. may have a link to IT • Payment practices specifically requires the average time the undertaking takes to pay an invoice from the date when the contractual or statutory term of payment starts to be calculated, in number of days.

References

AFM (2023, March 30). *Big steps needed to ensure compliant reporting of sustainability information in annual reports from 2024.* https://www.afm.nl/en/sector/actueel/2023/maart/grote-stappen-nodig-duurzaamheidsinformatie-jaarverslag

D'Souza, A., & Singh, R. (2022). Global ESG Reporting Software Market Size, Share & Industry Trends Analysis Report By Component (Solution and Services), By Vertical, By Organization size (Large Enterprises and SMEs), By Deployment Mode, By Regional Outlook and Forecast, 2022 - 2028. In *KBV Research. https://www.kbvresearch.com/esg-reporting-software-market/#:~:text=The%20Global%20ESG%20Reporting%20Software,%2C%20sustainable%2C%20and%20investment%20recommendations.*

DAMA International. (2017) *DAMA-DMBOK: Data Management Body of Knowledge*, 2nd edition.

DAMA NL. (2020). Dimensions of Data Quality. *In https://www.dama-nl.org/wp-content/uploads/2020/09/DDQ-Dimensions-of-Data-Quality-Research-Paper-version-1.2-d.d.-3-Sept-2020.pdf.*

De Chazal, E. (2022, August 16). Understanding Data Security & Privacy in ESG. *Skillcast*. https://www.skillcast.com/blog/data-security-privacy-esg#:~:text=Data%20privacy%20%26%20security%20is%20an%20ESG%20win&text=Moreover%2C%20it%27s%20increasingly%20clear%20that,the%20businesses%20they%20interact%20with .

Kaag, S. (2023, 07 25). Open Overheid. Retrieved from https://open.overheid.nl/documenten/04cae5d1-80f9-4b5b-891a-c41d7e21afdc/file

Lashitew, A. A. (2021). Corporate uptake of the Sustainable Development Goals: Mere greenwashing or an advent of institutional change? *Journal of international business policy, 4*(1), 184–200.

The Committee of Sponsoring Organizations of the Treadway Commission. (2023). ACHIEVING EFFECTIVE INTERNAL CONTROL OVER SUSTAINABILITY REPORTING (ICSR): Building Trust and Confidence through the COSO Internal Control—Integrated Framework. In *https://www.coso.org/Shared%20Documents/COSO-ICSR-Report.pdf.*

Watson, L. A., & Wra, D. (2022). THE DIGITAL TRANSFORMATION OF SUSTAINABILITY DATA: Digital sustainability data enables better decision making and improves companies' reporting and strategic planning. *Strategic Finance*, 36–41.