NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

# NOREA Study report:

## IT-Related Risks and Control Areas in ESG Reporting Framework



Version 1.0

Oktober 16, 2025

## Preface

This document presents a framework of IT-related risks and control areas[1] in the context of reporting on Environmental, Social and Governance (ESG) data and more broadly on Sustainability. This document is considered a first version and a discussion document, which will be developed further together with the input of the broader public. It was developed by NOREA, the Dutch Association of chartered IT-auditors (Register EDP Auditors; 'RE').

The purpose of the framework is to assist both companies and audit organizations (employing IT and financial auditors) in assessing IT-related risks associated with ESG data processing and reporting. It also aids in presenting an overview of control areas that can be considered when implementing (controls over) ESG data collection processes and auditing ESG data.

## Committee participants

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

| | | |
|---|---|---|
| Chairman, main contributor | Jeroen Francot | BDO |
| Main contributor | Marly van der Meij | Datavit |
| Main contributor | Miriam Baart | BDO |
| Main contributor | Lars Mion | KPMG |
| Main Contributor | Tom Lamers | Forvis Mazars |
| Main Contributor | Roel Ronken | Newtone |

## Version control

| Version | Date | Amendments |
|---|---|---|
| 0.1 | 14-02-2025 | Initial outline and draft |
| 0.2 | 04-03-2025 | Second version |
| 0.3 | 28-03-2025 | Third version, initial comments by the NOREA vaktechnische commissie |
| 0.4 | 07-04-2025 | Fourth version, revisions after review and initial feedback |
| 0.5 | 18-07-2025 | Fifth version, further revisions for second review by NOREA vaktechnische commissie |
| 1.0 | 16-10-2025 | Version for publication after review by NOREA vaktechnische commissie |



[1] In this document, "control area" is used to allow users to define individual control measures (5W methodology) relevant to their specific situation.

## Table of contents


1. Introduction 4

*1.1 Purpose* 4

*1.2 Users* 4

*1.3 Aim* 5

*The generic data processing approach* 5

*Intended use* 5

*Limited assurance* 6

*Internal versus external information* 6

*Other laws and regulations* 6

*Disclaimer* 6

2. Context and explanation 7

*2.1 Starting point for creating this document* 7

*2.2 Explanation of the process approach and risk identification* 7

*2.3 Control areas identified and usage of the framework* 8

3. Topics not included in the framework 9

*3.1 Change management* 9

*3.2 Continuity and availability* 9

*3.3 Access controls* 10

*3.4 Fraud risks* 10

*3.5 End user computing* 10

*3.6 Data quality* 11

*3.7 Privacy* 11

*3.8 Cybersecurity* 11

4. Future considerations & points for discussion 12

Appendix – The framework 13

*1. Data source* 14

*2. Interfaces* 16

*3. Data processing* 17

*4. Data storage* 18

*5. Output* 19

# 1. Introduction

## 1.1 Purpose

With the introduction of the Corporate Sustainability Reporting Directive (CSRD[2]) and the European Sustainability Reporting Standards (ESRS) many companies started[3] reporting on different kinds of ESG data. Auditors are involved in providing (limited) assurance on the ESG data being reported. Part of the ESG data originates from IT systems (or applications) and IT is used as a means of processing and reporting this data. This raises question such as:

- Is the data used reliable?
- Is data quality ensured[4]?
- Is confidentiality and integrity of data safeguarded?

In order to answer questions like these and support the assessment of IT-related risks in the context of ESG reporting, the NOREA Taskforce ESG has drafted the framework as presented in this study report. This framework is based on existing frameworks where possible, to ensure overlap where relevant. This framework can assist in assessing IT-related risks linked to sustainability reporting and in identifying appropriate control areas.

The objective of this document is twofold:

1. To present a framework with IT-related risks in the context of ESG reporting, as well as the suggested control areas.
2. To act as a discussion document and a foundation for a concise approach towards assessing IT-related risks in the context of ESG reporting.

## 1.2 Users

The intended users of this document are companies that (will) report on ESG data, as well as (IT) auditors that are engaged in reviewing systems with regard to ESG data. The use by (local) supervisory bodies is also encouraged, since control over IT systems and data is fundamental to show control over ESG (data).

The framework is considered applicable for companies with diverse levels of maturity and complexity. For companies that are new to the field of ESG reporting, the framework can help to start with the intended end state in mind. For mature companies it can be used as a reference to determine whether the IT-related risks recognized in this document are suitably covered in existing processes.



[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2464

[3] Preceding the introduction of CSRD there have been other initiatives, for example the Global Reporting Initiative (GRI). Whilst GRI is voluntary and global, CSRD is focused on the EU and mandatory.

[4] These are just some examples as stated. The DAMA Wheel from DAMA-DMBOK2 recognises a number of different knowledge areas that add to sound data management.

## 1.3 Aim

The intended audience of the framework are companies that are required to report under the CSRD requirements[5] as well as companies that voluntarily report on ESG data.

### *The generic data processing approach*

The presented framework is based on a generic information-processing sequence: input, processing, and output (reporting on information). Based on experiences with ESG reporting, IT-related risks are made ESG specific and control areas per process step are suggested. Note: In data management this is called "consumption". ***Data consumption*** refers to the process through which data is accessed, utilized, and sustained across various platforms, devices, and services.

This follows the logical steps as within any system:

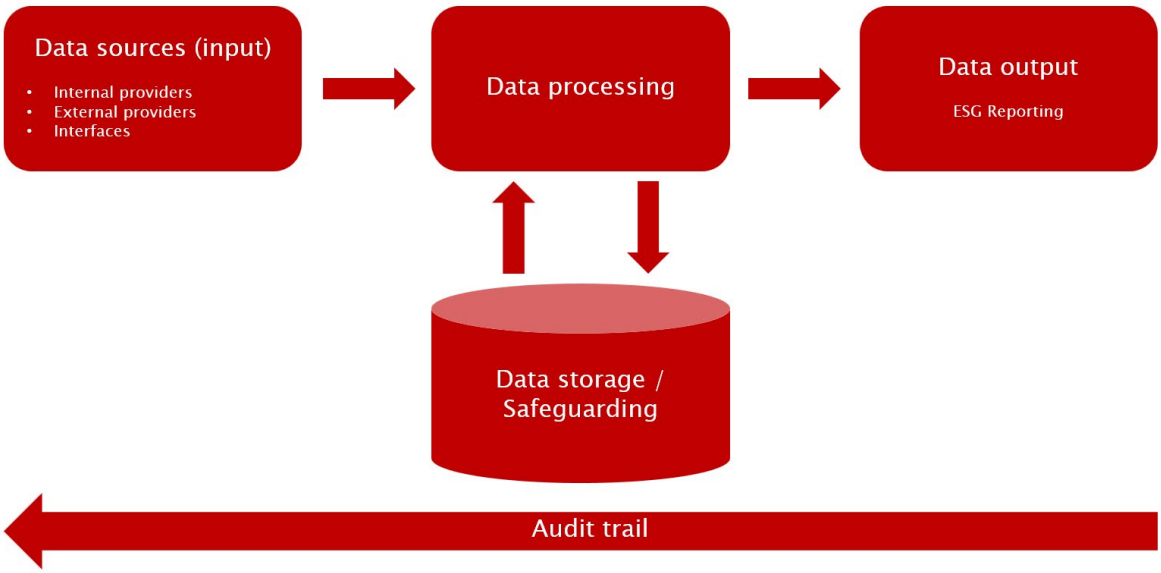


*Figure 1: System overview*

Information is input by systems, input by users (manual) or by means of interfaces extracted from source systems or external data sources. Secondly, ESG data is processed. This can be done by using mechanisms like Extract, Transform and Load, imputation, cleaning, integration, analysis, visualization, enrichment, etc. During this process ESG data is for instance stored in a database. Lastly, ESG data is made available for reporting purposes. Additionally, an overarching audit trail should be present to follow the processing of data throughout the entire process. These steps are likely to be encountered in any situation in which ESG data is prepared.

### *Intended use*

This framework and the control areas presented can be used in a broad number of situations. For instance, it can be used during an IT implementation in the system design phase and the

[5] With the introduction of the ESG Omnibus simplification package, the EU intends to limit the number of companies that have to report under the CSRD directive. When writing this document, the package has not yet been finalized.

implementation phase. It can also be used for the design and implementation of controls. Furthermore, the framework can also be used in an audit or review of IT systems.

### *Limited assurance*

In reviews of ESG data (such as under CSRD reporting), a limited level assurance is currently the maximum level of assurance required. The reliance on control measures will therefore be limited. However, (international) standards such as ISSA5000 do require understanding of the IT environment and its associated risks and (ultimately) controls[6]. This framework can be helpful in determining and managing the IT-related risks. In the future, a higher level of assurance (reasonable assurance) might be required.

Companies should consider IT-related risks and control areas when considering their internal control environment in relation to ESG information. When setting ESG goals and determining actions (e.g. for emissions reduction), the reliability of the related data is key. Companies are therefore encouraged to:

- consider IT-related risks and control areas when designing and implementing internal controls over ESG information and related processes;
- use the provided framework as a frame of reference.

### *Internal versus external information*

The current iteration of the framework does not differentiate between internal and external information. An important consideration in ESG reporting is that external information from the value chain should be included. This may give rise to additional or specific IT-related risks or risks of unreliable data. While the framework does address risks and control areas concerning data sources, including high-level coverage of external information, this remains a topic for potential future expansion.

### *Other laws and regulations*

The framework does not include specific laws and regulations. Other applicable laws and regulations, for example the General Data Protection Regulation (GDPR), may give rise to different or additional risks and required control measures (e.g. about the allowed level of detail in the reporting on the number of work-related injuries). Users should consider whether other laws and regulations apply, and whether these necessitate additional control measures.

### *Disclaimer*

It should be noted that the framework provided is not an exhaustive list of risks and related control areas. In practice, companies and auditors should determine which risks from the framework are applicable, whether additional risks (not listed in the framework) apply, and which control measures are most suitable to mitigate these risks appropriately. The framework is explicitly not a minimum practice or baseline, it is solely intended as a starting point for companies and auditors to consider risks and control areas for ESG data processing.



[6] International Standard on Sustainability Assurance 5000, General Requirements for Sustainability Assurance Engagements | IAASB, par. 117, 118 and 119R.

## 2. Context and explanation

### 2.1 Starting point for creating this document

ESG related data processing is a process that differs from traditional processes such as financial transactions processing for the financial statements. The reasoning for this is that financial transactions processing and related internal controls are more mature processes. Furthermore, traditional internal controls such as double entry bookkeeping, segregation of duties, etc. are not (yet) as present for ESG related data processing. As a result, a different approach should be applied to ESG data processing.

The initial approach was to take the ESRS data points and to use these data points for identifying risks and control measures. However, this approach failed, mainly because of the vastness of the number of data points, the lack of coherence and the specific implementation within companies, resulting in a framework that was not usable in practice.

The second iteration (this document and framework) was developed taking a generic process approach (see Figure 1). This approach does not differ from standard data processing. However, in the framework, these generic process steps have been made specific for ESG related data and accompanying IT-related risks. The reason for this is that the steps as identified in figure 1 may differ depending on the type of data being recorded. For example, data that is measured by automated systems (e.g. emissions, pipeline throughput) has a different origin compared to manual inputs (e.g. social data).

The NOREA Taskforce ESG has made an effort to determine which IT-related risks and control areas may be relevant related to ESG data processing. By providing an overview of the IT-related risks for each step in the process, companies and auditors can use the framework to determine which steps are relevant for the specific process being considered. This leads to a widely applicable framework that users can apply in their unique instance without limiting the framework to specific risks or controls. For example, users can determine whether IT-related risks are present based on the steps taken in the process in scope. The user can then determine if the IT-related risks should be considered, because of automation in the process.

The next two paragraphs will describe the process approach chosen, the risk identification as well as the control areas.

### 2.2 Explanation of the process approach and risk identification

The Taskforce ESG discussed which data processing steps are present in the context of sustainability reporting. These steps provide the basis for identifying the IT-related risks and control areas. This consists, in the view of the Taskforce ESG, of the following steps as a baseline (also see Figure 1 and the framework in I. Appendix):

1. Data sources (input)
2. Interfaces
3. Data processing
4. Data storage / Safeguarding
5. Data output
6. Audit trail

1) The source of data consists of the way in which data is collected. Because of the types of data that are relevant for the different ESG topics, data may be collected in very specific ways. For example, data related to emissions may be captured by specialized (automated) measurement tools, while data related to people and performance may be captured by manual entry into a system. Each way of data capturing may therefore bring specific risks which need to be addressed appropriately.
2) As a result of the broad scope of data that may be captured, depending on the topics that are in scope, data may need to be transferred to a system (e.g. in case of automated measurement systems) or between systems. The transfer of data therefore brings specific risks with regard to, for example, accuracy, completeness and timeliness.
3) After data is captured, it is possible that data needs to be transformed based on specific requirements from the relevant ESG topics in scope. This may include, for example, the application of emission factors from the Greenhouse Gas Protocol. As such, there are risks associated with the transformation of data.
4) Throughout the data processing process, data must be stored. The (lack of) safeguards that are in place may bring additional risks to the processing of data.
5) Lastly, data that results from the previously mentioned steps leads to the output that is included in reporting.
6) In general, there are overarching risks that need to be addressed when considering ESG data processing, specifically regarding the tracking of changes throughout the entire process. This risks require a sufficient audit trail.

After identifying the data processing steps, the Taskforce ESG determined which IT-related risks are present for each specific step. Because of differences for each step, unique risks may apply per specific situation. By specifying risks for each step, specific (internal) control areas can be identified for each risk individually, but also on a higher level when risks overlap between steps.

By taking a risk-based approach, it is possible to determine which IT (related) risks apply to ESG data processing steps and to specify control areas that may be applied to mitigate these risks. Note that it was a conscious decision not to include overarching risks or risks outside of the boundaries of IT, such as management override (see also section 3.).

### 2.3 Control areas identified and usage of the framework

The control areas that are specified in the framework (see I. appendix) are based on existing frameworks, for example:

- Data management links closely with the DAMA-DMBOK approach[7], which serves as a guide to create a data governance framework but also offering insights into data quality control measures;
- IT-related risks and control measures taps into the Control Objectives for Information and related Technologies (COBIT) as maintained by ISACA.

The control areas selected are those considered most suitable to address the identified IT-related risks. By using existing frameworks, the aim is to reduce the need to identify or

[7] The DAMA-DMBOK (Data Management Body of Knowledge) serves as a comprehensive framework for understanding and implementing effective data management practices.

implement specific control measures that are 'new' to ESG data processing. It is possible to use and leverage existing, known controls from control frameworks that may already be present in systems of internal control, for example for financial transaction processing. Users are invited to determine which controls are suitable to their specific needs and to expand on internal risk management and internal control systems if present, rather than to copy descriptions directly from the framework.

Users should determine which data processing steps are present for each related dataflow to determine the relevant IT-related risks. By considering the risks presented for each ESG topic[8], companies and auditors will be able to determine whether control areas presented are relevant to implement. Users can apply a standard risk assessment process (e.g. by determining the likelihood and severity of a risk). This leads to an efficient approach to IT-related risks, without 'over-implementing' control measures. Of course, companies and auditors are also encouraged to determine whether there may be relevant control areas that are not yet included in the framework which are a better fit for the company. For example, based on existing frameworks or control measures already present in the company's system of internal control.

## 3. Topics not included in the framework

When composing the framework, the Taskforce ESG has specifically focused on the steps related to data processing. Overarching controls, such a General IT Controls (GITC), are not included in the framework. However, these topics are certainly important to consider. The overview below provides a short summary of additional topics that may be considered by users of this framework.

### 3.1 Change management

Change management controls are considered in two ways. Firstly, change management risks and control measures may be present with regard to configurations of IT systems used in the different steps of ESG data processing. As such, for each step in the process and system used, companies and auditors should consider the risks with regard to unauthorized changes to configurations of systems and ensure that adequate change management controls are in place around that. Examples include the risk that configurations of interfaces or batch processing, or that configurations for automated calculations, are adversely affected by changes.

Secondly, risks may be present with regard to changes in terms of updates or changes to systems which may adversely affect system functionality or may lead to disruptions and/or loss of data. Again, companies and auditors should consider the risks present and ensure adequate change management controls such as for example sufficient testing should be considered.

### 3.2 Continuity and availability

With regard to the completeness of data, continuity measures have an overarching role with respect to ESG related risks. There is a general risk that data is incomplete as a result of system disruptions or unrecoverable loss of data. Sufficient continuity measures should be considered to mitigate such risks and to safeguard the continuity of data storage by means

[8] A future addition would be to link the specific topics and risks to individual data streams and data points, for instance under the ESRS framework.

of back-up and recovery controls or even more advanced controls like replication and mirroring.

### 3.3 Access controls

Access controls are relevant because of the overarching risk of unauthorized access to or manipulation of data. This risk can be present in all data processing steps included in the framework. Topics such as segregation of duties may similarly play a role in each step as well as for specific systems and should therefore be considered.

### 3.4 Fraud risks

Fraud risks should always be considered when determining risks that threaten the accuracy or completeness of information. The publication 'ESG-fraude en greenwashing' (2024) by the NBA (Nederlandse Beroepsorganisatie van Accountants) specifies that fraud may occur through manipulation of information. Furthermore, it specifies that there is ample opportunity to do so, because:

- ESG information streams are often without control measures, or control measures are immature;
- There is no overarching 'ESG administration' which makes reconciliations difficult and software implementation is still in development, leading to the use of different systems for specific ESRS topics or even data points;
- 'Double entry bookkeeping' and segregation of duties are (often) not present for ESG data;
- No historical data is present, data points are not related to one another, and there is no uniform measurement for all data points (such as a currency) making numerical analyses less applicable;
- The understanding of data points such as emissions or biodiversity requires specific competencies.

For example, if remuneration or bonus incentives depend on the (performance on) ESG related metrics, there is a risk that these metrics are misrepresented or are under the influence of bias. Next to access controls in general, it is therefore relevant to determine whether specific data processing is present that is susceptible to unauthorized access with the intent to commit fraud and to apply relevant controls to ensure that data is not manipulated.

### 3.5 End user computing

There is a chance that companies will use all kinds of end user computing (EUC) when processing data, for example the use of Microsoft Excel. These kinds of tools offer advantages to users, such as flexibility and ease of use. However, it also poses significant threats and therefore risks towards the processing of ESG data. Specific risks that are to be encountered under end-user computing are:

- Lack of security and therefore the risk of unauthorized access or changes, mainly because of poor security and access controls;
- Complexity, because spreadsheets can become increasingly complex and thereby also creating a huge dependency on the person that has built and maintained the spreadsheet (key person risk);
- Inadequate testing and poor change management controls;

- Model interdependencies if spreadsheets link to each other, thus creating an interdependency risk.

Whilst the use of EUC is not advocated, it is apparent that companies, certainly in the initial phases of ESG reporting, will use these kinds of tools and applications. Specific EUC controls should be considered.

### 3.6 Data quality

Data quality can pose significant challenges in processing and control measures should be considered. Measurements may lack precision, require estimations, or fall short of ideal quality scores. When relying on estimations, it's crucial to understand their impact. Conducting a sensitivity analysis can help assess the effect of imprecise numbers or incorrect estimations. If the analysis indicates a significant impact, obtaining more accurate figures is advisable. It's also important to consider how these estimations affect other data points during the analysis.

In monitoring data quality, achieving “perfection” is not always feasible. Efforts to enhance data quality should prioritize the most critical data elements. The standard data quality processes outlined in the DAMA-DMBOK can offer valuable guidance for establishing effective monitoring and follow-up activities to improve data quality.

### 3.7 Privacy

When processing ESG related data, especially in the context of the social topics, personal data may be processed, for which companies must adhere to relevant laws and regulations such as the GDPR. The framework does not explicitly include risks and related control measures regarding personal data or privacy. The NOREA Privacy Control Framework can be used to consider Privacy risks and control measures.

### 3.8 Cybersecurity

Cybersecurity may play an important role in the context of ESG reporting. The risks of unwanted destruction, loss, alteration or provision of personal data are top three business risks nowadays and these risks also apply to an ESG reporting setting.

An overview of cybersecurity measures is not included. Refer to existing frameworks for cybersecurity, for instance the NIST Cybersecurity framework, for specific details on these kinds of risks and the control measures that can be taken.

## 4. Future considerations & points for discussion

The framework is a first step towards defining IT-related risks in the context of ESG reporting. Suggestions for future development are:

- The link between the individual ESRS data points and the framework could be further developed. More guidance could be given on how specific IT-related risks apply to specific ESRS data points;
- A split could be made between processing internal and external Sustainability/ESG data and the different requirements and risks. For instance, data that is processed externally can be managed and assessed differently from data that is processed internally (within the company). The risks and control areas can be different in each setting;
- A distinction could be made between key- and non-key control areas when processes are more mature;
- A more detailed mapping could be made to existing frameworks (e.g. COBIT, CIS, etc.).

This framework is intended to be a starting point for discussion. The Taskforce invites auditors and companies to share their views and opinions, specifically raising the following points for further discussion:

1. In general, is the framework helpful in assessing IT-related risks and identifying relevant control areas? If any, what improvements could be made?
2. Are there any topics or areas that are relevant in the context of sustainability information that have not yet been identified in the study report? If any, which are these and why should these be included?
3. Are there additional IT-related risks that should be included in the framework? If any, which are these and why should these be included?
4. Are there additional control areas that should be included in the framework? If any, which are these and why should these be included?
5. What future developments to the framework, other than those already noted, should be considered by the Taskforce ESG and why?

The Taskforce expects the ESG data process to mature further in the upcoming years. Therefore, the current framework is a starting point for addressing IT-related risks and relevant control measures that can be implemented to address those risks in the context of ESG reporting.

## Appendix – The framework

The following pages show the framework itself. Within each data processing step, risks and control areas are listed. Items indicated with an 'X' show the interrelation between a risk and control area or vice versa.

1. Data source

| **Control area is detective or preventive by nature** | **Preventive** | **Detective/preventive** | **Preventive** | **Preventive** | **Preventive** | **Preventive** | **Preventive** |
|---|---|---|---|---|---|---|---|
| **Control area** | **Defined policies and process descriptions are in place.** | **Controls to ensure that measuring equipment is working accurately are implemented. E.g. periodic review of database registers or periodic calibration of measurement equipment.** | **Procedures to prevent potential for fraud on measuring equipment leading to inaccurate or incomplete data are in place.** | **Controls to ensure measuring equipment is protected against unauthorized modifications (physical as well as software modifications) are implemented.** | **Input controls are in place. E.g. field validations, list selection, mandatory fields, tolerances, limits, sequence check (ascending numbering), syntax checks, queries that enforce correct periods.** | **A four-eyes principles and/or segregation of duties is in place.** | **Logical access controls are implemented.** |
| The risk is that measurement equipment is not working accurately because of faulty configuration, technical issues or fraud during measurement. | X | X | X | X | | | |
| The risk is that data input is not accurate, because of unauthorized alteration of source data or unintentional errors. | | | | | X | X | X |
| The risk is that data input is not complete, because of incorrect scoping or incomplete data capture. | | | X | | X | X | |
| The risk is that data is not reliable, because of tampering or conducting business with untrustworthy suppliers. | | | X | | | | |
| The risk is that data is not accurate, because of incorrect timing or cut off. | | | | | X | | |
| The risk is that data can be adjusted by an unauthorized person. | | | X | | | | X |
| The risk is that an observation or measurement is not consistent, because of changing rules, lack of uniformity or different data definitions. | | | | | | | |

Data source (continued)

| **Control area is detective or preventive by nature** | **Preventive** | **Detective** | **Preventive** | **Detective** | **Detective** |
|---|---|---|---|---|---|
| **Control area** | **Data governance policies and procedures are in place. This includes the presence of clear data definitions (such as a data dictionary) and data owner for critical data points/data elements.** | **Monitoring controls for data quality are in place. E.g. reconciliations, four-eyes principle (retrospective check), benchmarking/ variance analysis (buildings, equipment, offices), trend analysis (previous periods), consistency check and automated data quality monitoring rules.** | **Clear agreements (data definitions, cut-off in time, transparency of calculations / traceability) with third parties are in place.** | **Monitoring controls over assurance reporting on data delivered by third parties are in place.** | **Monitoring controls over assurance reporting on the processes/controls carried out by third parties are in place.** |
| The risk is that measurement equipment is not working accurately because of faulty configuration, technical issues or fraud during measurement. | | | | | |
| The risk is that data input is not accurate, because of unauthorized alteration of source data or unintentional errors. | X | X | | | |
| The risk is that data input is not complete, because of incorrect scoping or incomplete data capture. | X | X | | | |
| The risk is that data is not reliable, because of tampering or conducting business with untrustworthy suppliers. | | X | X | X | X |
| The risk is that data is not accurate, because of incorrect timing or cut off. | | X | | | |
| The risk is that data can be adjusted by an unauthorized person. | | X | | | |
| The risk is that an observation or measurement is not consistent, because of changing rules, lack of uniformity or different data definitions. | X | X | X | | X |

## 2. Interfaces

| **Control area is detective or preventive by nature** | **Detective** | **Detective** | **Preventive/Detective** | **Preventive** | **Preventive** |
|---|---|---|---|---|---|
| **Control area** | **Controls to monitor the effectiveness of the interface are implemented.** | **Transfer error lists as a result of monitoring and defined follow-up actions to ensure completeness of data are implemented.** | **Controls using batch totals/hash totals to check completeness and/or accuracy of transfer are implemented.** | **Logical access controls (related to interface adjustments) are implemented.** | **Controls to ensure that transferred files cannot be modified on "intermediate locations" (access to directory and/or file is protected) are implemented.** |
| The risk is that data transfer is not complete. | X | X | X | | X |
| The risk is that incomplete data transfer is not addressed appropriately. | X | X | | | |
| The risk is that data transfer is not accurate. | X | X | X | X | X |
| The risk is that data transfer is not timely, because of incorrect (automatic) processes or handling of timely follow up of transfer errors. | X | X | | | |
| The risk is that data is adjusted during transfer, because of unauthorized access. | | | | X | X |
| The risk is that unauthorized changes are made to the interface. | X | | | X | |

## 3. Data processing

| **Control area is detective or preventive by nature** | **Preventive** | **Preventive** | **Preventive** | **Detective** | **Preventive** | **Detective** |
|---|---|---|---|---|---|---|
| **Control area** | **A four-eyes principle for setup and configuration of data processing systems and controls is in place.** | **Policies, procedures and work instructions for manual calculations/processing are in place.** | **A four-eyes principle for manual calculations/processing is in place.** | **Monitoring controls for data quality are in place. E.g. reconciliations, four-eyes principle (retrospective check), benchmarking/ variance analysis (buildings, equipment, offices), trend analysis (previous periods), consistency and automated data quality monitoring rules.** | **Logical access measures related to automated processing and system configurations are implemented.** | **Formal documentation of all calculations, e.g. used formulas, functions or other processing techniques, is present.** |
| The risk is that data processing and/or calculations are inaccurate. | X | X | X | X | | |
| The risk is that formulas are not applied appropriately. | X | X | X | X | | |
| The risk is that data processing is not complete. | X | X | X | X | | |
| The risk is that data cleansing is not performed appropriately. | | | | X | | |
| The risk is that there is no documentation of applied calculations, formulas or functions. | | | | | | X |
| The risk is that changes that are applied to processing techniques (e.g. calculations, formulas or functions) are not controlled appropriately, because of the lack of a change management procedure. | X | | | | | |
| The risk is that changes that are applied to processing (e.g. calculations, formulas or functions) are not controlled appropriately, because of unauthorized changes. | X | | X | X | X | |

4. Data storage

| **Control area is detective or preventive by nature** | **Preventive** | **Preventive** | **Detective** | **Preventive** | **Preventive** |
|---|---|---|---|---|---|
| **Control area** | **Logical access controls to prevent unauthorized access are in place.** | **Logical access controls to prevent unauthorized changes are in place.** | **Controls to monitor access or changes to data are in place.** | **Data is stored in locations as required by general laws and regulations and/or company policy.** | **Data at rest is encrypted as required by general laws and regulations and/or company policy.** |
| The risk is that stored data is accessed unauthorized. | X | | X | | X |
| The risk is that stored data is changed unauthorized. | | X | X | | X |
| The risk is that data is stored in unauthorized locations. | | | | X | |

## 5. Output

| **Control area is detective or preventive by nature** | **Preventive** | **Preventive** | **Preventive** | **Preventive** |
|---|---|---|---|---|
| **Control area** | **Data governance policies and procedures are in place. This includes the presence of clear data definitions (such as a data dictionary) and data owner for critical data points/data elements.** | **A four-eyes principle is in place.** | **Standard reports are used where possible.** | **Controls on queries/filters when compiling the report are implemented (e.g. standard lists, logging on queries, audit trail).** |
| The risk is that data is incorrectly processed into a report. | X | X | X | X |
| The risk is that data is incompletely processed into a report. | | X | X | X |
| The risk is that inconsistent data definitions are used for the same data (no alignment of data definitions). | X | | | |
| The risk is that data cannot be traced back to its source. | X | | | |
| The risk is that reports can be adjusted. | | | X | |
| The risk is that data is not accurate, because of incorrect timing or delimitation. | X | X | X | X |
| The risk is that XBRL tagging is not accurate. | X | X | X | |

Output (continued)

| **Control area is detective or preventive by nature** | **Detective/preventive** | **Detective** | **Preventive** | **Detective** |
|---|---|---|---|---|
| **Control area** | **Slice/dice software with logging is used to ensure an audit trail.** | **Controls to reconcile output with the source are implemented.** | **Logical access controls related to reports are implemented.** | **Controls to review the master file containing the mapping of the CSRD report with the XBRL Tagging (and changes to the master file, if applicable) are implemented.** |
| The risk is that data is incorrectly processed into a report. | X | X | | |
| The risk is that data is incompletely processed into a report. | X | X | | |
| The risk is that inconsistent data definitions are used for the same data (no alignment of data definitions). | | | | |
| The risk is that data cannot be traced back to its source. | X | | | |
| The risk is that reports can be adjusted. | | | X | |
| The risk is that data is not accurate, because of incorrect timing or delimitation. | X | | | |
| The risk is that XBRL tagging is not accurate. | | | | X |

## 6. Audit Trail

| **Control area is detective or preventive by nature** | **Preventive/Detective** | **Detective** |
|---|---|---|
| **Control area** | **Transparent dataflow to track data through various processes and systems.** | **Logging/audit trail (including date/time) is available to monitor unauthorized usage or anomalies.**<br><br>**Requirement: logging cannot be altered or deleted.** |
| The risk is that data cannot be traced back to its source. | X | X |