NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

ONLINE TRUST
COALITIE

International Digital Reporting Standards

Governance of IT

Version 2.1

May 2025

May 2025

Acknowledgement

This reporting standard is issued by NOREA, the professional association of IT auditors in the Netherlands and was developed to guide organizations and their auditors (Register IT auditor (RE) and their international equivalents) in issuing reports on the Governance of IT.

This version 2.1 serves the handover of this reporting standard to the governing body under NOREA. It becomes effective once this handover is agreed between the parties. For this purpose the standard is renamed from NRI (NOREA Reporting Initiative) to IDRS (International Digital Reporting Standards), and some wording was synchronized to other standards.

Working group participants

Name	Serving as
Alex van der Harst	Partner, KPMG Advisory
Dennis Utermark	Director, KPMG IT Assurance & Advisory
Foppo Spuij	Director, PWC Risk Assurance
Irene Vettewinkel	Audit Director Group Audit, ABN AMRO
Jan Matto	Partner IT Audit & Advisory, Mazars
Jeroen Francot	Manager IT Risk Assurance, BDO
Jeroen van Schajik	Partner IT Risk Assurance, BDO
Joep Janssen	IT auditor and management consultant, Augyconsult
Marc Welters	Partner, EY Technology Risk / Chair NOREA
Marcello Smalbil	Director IT Advisory, Baker Tilly
Michiel Hopstaken	Senior Manager IT Risk Assurance, BDO
Mirjam Baars	Senior IT Auditor, UWV
René Ewals	Managing partner, ACS
Richard van Hienen	Algemeen directeur Auditdienst Rijk
Rob Polderman	IT Auditor, Derpolman BV
Robert Boon	Partner, Deloitte Risk Advisory
Ron Hakvoort	Director, Deloitte Risk Advisory
Ronald van Langen	Senior manager, KPMG
Ruud Kerssens	IT Auditor and cybersecurity expert, TOPP Audit
Salo van Berg	IT Risk Consultant, TIQ Advisory Services
Tobias Houwert	Global Quality and Internal Control Director, Arcadis N.V.
Tom Verharen	Senior Auditor, CZ
Victor Krul	Director NOREA

Postbus 242, 2130 AE Hoofddorp
phone: (+31) 88 4960380
e-mail: info@norea.nl
www.norea.nl

Version control		
Version	Date	Amendments
0.9	June 2022	Consultation Draft
0.10	January 2023	Second Consultation Draft OOB audit firms
0.11	March 2023	Public Consultation Draft
1.0	January 2024	First full version,
2.0	March 2025	Update after pilots, for use during 2025
2.1	May 2025	Renamed to IDRS

Contents

Preface International Digital Reporting Standards on Governance of IT

Introduction

Digitization of our society is happening at an increasing pace. Currently organizations are receiving a variety of requests from different parties to report on how they control their IT and their digital products and services, varying from clients and suppliers to supervisory entities and other stakeholders, each with their own specific requirements. Looking ahead, NOREA anticipate a steep increase in legislation and regulations coming into force on an international (i.e. EU) and national level regarding digital products and services and IT in general. A common denominator in all these legislations and regulations is that they require organizations to report on the (digital) resilience of their digital products and services, and the organization as a whole. Furthermore, the sustainability of organizations as being part of our society is becoming more of interest. Responding to this multitude of reporting requirements places a significant administrative burden on organizations, which is likely to increase even further in the coming years.

Given that there is a common denominator in most, if not all of these reports (i.e. they tend to look at a limited number of digital resilience topics), we believe there is value in adopting a standardized framework for reporting on topics that are most common under these requirements. NOREA, the professional association of chartered IT auditors in the Netherlands has therefore taken the initiative to develop practical guidance for reporting on the governance of IT that can be drafted by organizations. This initiative will be transferred to ECP, the Platform for Information Society in the Netherlands (see ECP.nl), to maintain and develop further in a broader setup. The ultimate objective of this reporting initiative is to serve as international standard for reporting on governance of IT (hence the name International Digital Reporting Standards) by developing disclosure criteria for organizations regarding governance, risk and compliance of their IT-related material topics. Currently there are no legal requirements regarding the content of such reports on the governance of IT. This standard aims to provide a coherent set of disclosures supported by reporting requirements that ensure consistent reporting on the governance of IT for a wide range of stakeholders and apply a reference to identify and report points of improvement within the context of the IT of the organization.

The content of such report on the governance of IT focuses on the measures taken to ensure that an organization has organized its IT in such a controlled manner that it contributes to its strategic goals. This reporting initiative covers the following topics:

- Digital Innovation and Transformation;
- Data & AI;
- Third Party Management;
- Cybersecurity;
- IT Continuity Management;
- Privacy.

This reporting standard pays specific attention to elements that are crucial for an organization and its stakeholders including customers, suppliers, employees and other workers, regulators, investors and society. A report on the governance of IT should also look forward in time at developments in the near future as well as how an organization plans to respond to these. The report on the governance of IT therefore covers the past year as well as the current year.

The disclosures, requirements and guidance in this standard find their origin in generally accepted standards and best practices for each of the topics. Thereby making use of the input from industry, public authorities, experts and other stakeholders in developing sound standards and best practices. See Bibliography for further details.

This International Digital Reporting Standards (IDRS in short) will be complemented with an audit guidance to provide practical guidance for independent IT auditors to allow them to provide an assurance opinion. The opinion of the independent IT auditor enhances the degree of confidence of the intended users of the report on the governance of IT about the reliability of the report and encourages the compiling organization to pay continued attention to the adequate governance of IT to safeguard the IT continuity of the organization.

With this reporting initiative, NOREA contributes to the strengthening of sustainability, compliance, confidentiality, integrity and availability of IT of an organization. It does also contribute to the resilience of digital eco systems and to the protection of our economic system. On the one hand by making organizations more aware of the challenges they are facing and on the other hand by increasing transparency towards their stakeholders. NOREA has consulted various regulators, government agencies and representative organizations in the Netherlands about the continued interpretation of the report on the governance of IT and to obtain broad support. The outcome of this consultation shows an increasing need for transparency regarding the way organizations manage their IT topics and address the expectations of stakeholders including customers, suppliers, employees and other workers, regulators, investors and society. Especially because IDRS uses standards and best practices as a reference it provides top management with a solid perspective on how to address these IT topics in their organization from a governance point of view.

Analogy with GRI Standards

The IDRS has been developed similarly to the structure of the GRI Sustainability Reporting Standards[1] (GRI Standards). The GRI Standards enable an organization to report information about its most significant impacts on the economy, environment, and people, which includes impact on human rights and how it manages these impacts. Although IDRS is not a GRI Standard, NOREA has decided to adopt the structure of the GRI standards and has designed their IDRS for reporting on the governance of IT accordingly. This allows a reporting organization to integrate the report on their governance of IT more easily into its wider report, if based upon these GRI Standards.

[1] https://www.globalreporting.org/

This implies that organizations that apply this IDRS standard, also need to apply the GRI foundation that IDRS is building on.

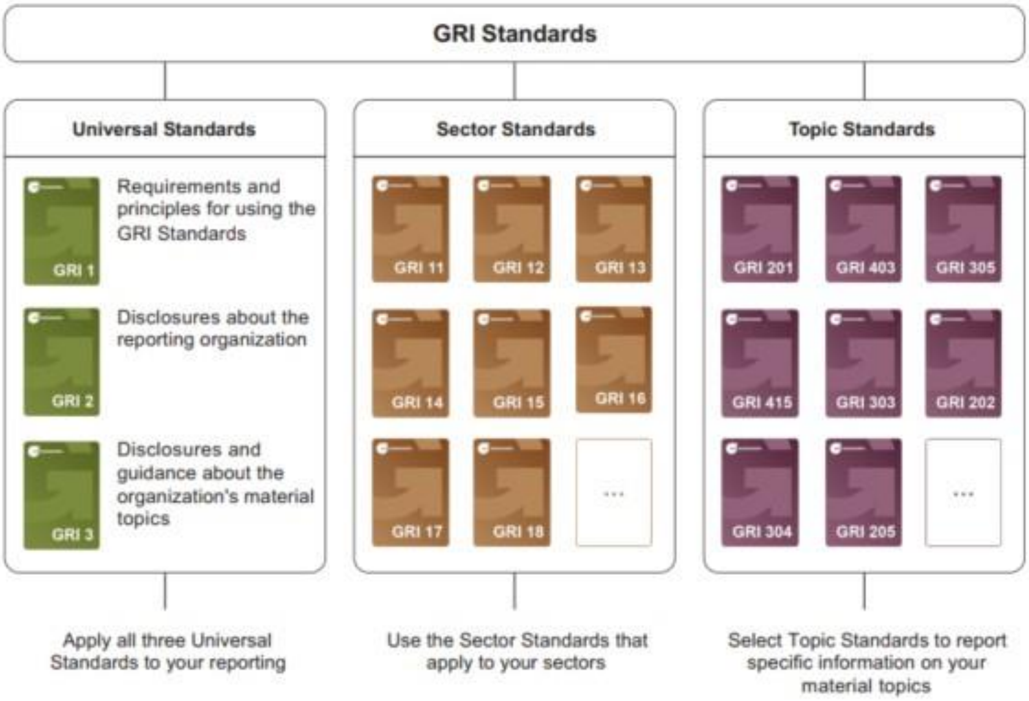
The GRI Standards can support organizations in their wider (sustainability) reporting and are structured as a system of interrelated standards that are organized along three separate series: GRI Universal Standards, GRI Sector Standards, and GRI Topic Standards.

- GRI 1: Foundation 2021 specifies the requirements that an organization must comply with to report in accordance with the GRI Standards. The organization begins using the GRI Standards by consulting GRI 1.
- GRI 2: General Disclosures 2021 contains disclosures that an organization uses to provide information about its reporting practices and other organizational details, including its activities, governance, and policies.
- GRI 3: Material Topics 2021 provides guidance on how to determine material topics. It also contains disclosures that an organization uses to report information on its processes in determining material topics, a list of material topics, and how it manages each topic.

An important element in the analogy is the use of ‘‘Disclosures”. These "Disclosures” cover the attestation by top management towards stakeholders regarding the governance of IT as a material topic and the IT topics identified as being of specific importance for the organization. With these disclosures the top management can proclaim their commitment to having their IT effectively contribute to the strategic objectives of the organization and to being in control.

Topic Standards

In line with the GRI Standards framework, IDRS has been designed by using the form for Topic Standards. The Topic Standards contain disclosures that an organization uses to report on its impacts in relation to particular material topics.


GRI Standards
Universal Standards
Sector Standards
Topic Standards
GRI 1
Requirements and principles for using the GRI Standards
GRI 2
Disclosures about the reporting organization
GRI 3
Disclosures and guidance about the organization's material topics
GRI 11
GRI 12
GRI 13
GRI 14
GRI 15
GRI 16
GRI 17
GRI 18
...
GRI 201
GRI 403
GRI 305
GRI 415
GRI 303
GRI 202
GRI 304
GRI 205
...
Apply all three Universal Standards to your reporting
Use the Sector Standards that apply to your sectors
Select Topic Standards to report specific information on your material topics

Reading guide

This document includes two sections. Section 1 contains a general introduction to the governance of IT topics and the structure of topic standards. It contains disclosures for the governance of the IT topics identified, further defined in requirements about what to report to provide information regarding the IT-related impacts of the organization. Guidance is added to provide support in reporting on these generic topics. Section 1 also includes considerations on the sustainability impacts of the governance of IT topics that could be relevant when addressing the topics in section 2.

Section 2 contains the topic standard. So far NOREA has developed one topic standard consisting of six IT sub-topic standards that are expected by the NOREA working group to be relevant to many organizations, based on their research activities and consultations with a broad group of potential stakeholders. In GRI terms these are referred to as ‘likely material topics’. These sub-topic standards contain disclosures per identified IT (sub-)topic, which provides information about the organization’s (sub-)topic related practice impacts, following the same structure for reporting requirements and guidance.

The six sub-topics are:

1. Digital Innovation and Transformation;
2. Data & AI;
3. Third Party Management;
4. Cybersecurity;
5. IT Continuity Management;
6. Privacy.

The Glossary contains defined terms with a specific meaning when used in the GRI Standards. The terms are underlined in the text of the GRI Standards and linked to the definitions.

The Bibliography lists references used in developing this Standard.

Appendix A contains a set of requirements for Disclosure 3-3 in GRI 3: Material Topics 2021 that organizations shall use to determine their disclosures as per IT-topic.

Using this standard

This standard can be used by any organization, regardless of size, type, sector, geographic location, or reporting experience, to report information on how it manages its IT topics related impacts.

An organization reporting in accordance with this standard, which has been drafted along the lines of the GRI Standards framework, is required to report the disclosures of each IT sub-topic (hereinafter referred to as IT topic) that it has identified as being a material topic[2] . If the governance of IT has been determined as a material topic, the organization shall further list its material IT topics in accordance with the requirements stated in GRI 3-1 and 3-2. By doing so organizations provide relevant information to their stakeholders regarding the importance of IT topics for their operations and continuity of the organization. This information looks events and (expected) developments in the reporting period, which (unless specified otherwise) consists of the past year and the current year (foreseeable future).

If an organization cannot comply with a disclosure that is in scope under the definitions of the IDRS or with a requirement in a disclosure (e.g. because the required information is confidential, creates a risk or is subject to a legal prohibition), the organization is required to specify this disclosure or the requirement it cannot comply with and provide a reason for the omission thereof~~.~~

If an organization cannot report the required information about an item specified in a disclosure because the item (e.g. committee, policy, practice, process) does not exist, it can comply with the requirement by reporting this to be the case. The organization can explain the reasons for not having this item in place, or describe any plans they may have to develop it. The disclosure does

[2] See Requirements 4 and 5 in GRI 1: Foundation 2021.

not require the organization to implement an item such as development of a policy, but to report that the item does not exist.

The IDRS emphasizes that IT is a building block that has become critical for a number of other processes in organizations and needs to be aligned with these processes. For instance, IT continuity versus business continuity. In case the organization reports its continuity management not solely as IT continuity, but in a more wider scope as business continuity, IDRS provides requirements to report on the integration of IT in those topics while the IT-specific elements are addressed in the IT topic part.

Requirements, guidance and defined terms

As this standard has been drafted in line with the GRI Standards framework, the structure per topic is as follows:

- Scope paragraph: depicts the IT topic within the organization;
- Disclosures: mandatory management assertions regarding the specific IT topic;
- Requirements: reporting elements that are mandatory to clarify the disclosure in the report;
- Guidance: information to assist in the reporting process.

The following applies throughout this standard:

- Requirements are presented in **bold font** and are indicated by the word 'shall'. An organization must comply with the requirements to report in accordance with this standard.
- Requirements may be accompanied by guidance.
- Guidance includes background information, explanations, and examples to help the organization better understand the requirements. The organization is not required to comply with guidance although some important reporting elements are expected to be reported, indicated with “should”.
- The standard may also include recommendations. These are cases where a particular course of action is encouraged but not required.
- In the wording of requirements and guidance, “shall”, “should”, “could” and “may” are intentionally used to make clear how the requirement or guidance should be handled in the reporting:
    - “shall” is used in requirements and indicates a mandatory requirement to be addressed in the report;
    - “should” is used in guidance and indicates a strict recommendation, meaning that it is addressed in the report and if not, this is explained in the report;
    - "could” is used in guidance and indicates a possibility or option, meaning that it is not required to be addressed in the report or clarified for reasons of non-reporting;

  - "may” is used in guidance, indicates a possibility and is mostly used for the reporting of specific, possible occurrences, as reporting about these occurrences generally does not provide essential information for stakeholders and might have a negative impact if known by all readers of the report.

- Defined terms are underlined in the text of the standard and are linked to their definitions in the Glossary. Organizations are required to apply these definitions in the Glossary.

Reading audience

When composing an IDRS report, it is required to have a clear understanding of the intended reading audience of the report. This IDRS sets some requirements for the identification of such audience. It refers to the approach within the GRI Standards, where stakeholders are individuals or groups that have interests that are affected or could be affected by an organization’s activities. The report intends to provide information to these stakeholders.

The organization has a level of freedom to tailor the report to the reading audience it intends for the report, e.g. by assuming a basic level of knowledge of IT in general, provided it adheres to the disclosures, requirements and guidance of this standard. It is strongly recommended to describe the assumptions drafting the IDRS based report in the introduction of the report to have a proper understanding for the readers. For the success of their stakeholder communication organizations are encouraged to make the reports accessible and understandable for an audience that represents its stakeholders as widely as possible.

If the report is expected to be used for specific purposes, or used by stakeholders with a specified interest, it is recommended to describe the conditions used in drafting the report for this specific use. When reporting on a topic, in accordance with requirements and guidance provided, it is strongly recommended to apply a management cycle approach to provide the information in a structured order. The plan-do-check-act cycle is an example of such an approach.

Origination

This standard is developed and issued by NOREA, the professional association for chartered IT auditors in the Netherlands. Any feedback on this standard can be submitted to norea@norea.nl for consideration by the taskforce Reporting on Governance of IT.

Due Process

When developing this standard, the NOREA working group applied a multi-stakeholder consultative process involving representatives from organizations and report information users within the Netherlands.

Responsibility

While the board of NOREA encourages the use of this standard and related interpretations by all organizations, the preparation and publication of reports based fully or partially on this standard and related interpretations are for the full responsibility of those producing them.

Legal liability

Neither NOREA Board of Directors nor the taskforce Reporting on Governance of IT can assume responsibility for any consequences or damage resulting directly or indirectly from the use of this standard and related interpretations in the preparation of reports, or the use of reports based on this standard and related interpretations.

Copyright and trademark notice

SECTION 1: GOVERNANCE OF IT TOPICS

Introduction

For most organizations, IT[3] plays an (increasingly) important role in achieving their strategic and operational objectives. Due to the growth in possibilities that digital technology offers, as well as the related shift in consumer/customer behavior and expectations that are driven by these digital possibilities, the use of digital technology in products and services has become a success factor to win or survive in the marketplace. Furthermore, digital technology allows for extensive connectivity between parties in the demand- and supply chains and sectors throughout the economy, both public and private, which has led to and still offers potential for new products and services, as well as new business models for existing products and services.

As a natural reciprocal of these increased possibilities, the dependency of digital products, services and business models on technological components and capabilities that enable them requires sufficient care to establish their ongoing safety and resilience. This is true not only for individual organizations, but also across their ecosystems, demand- and supply chains and sectors. And to protect the safety and human rights of the consumers of these digitally enabled products and services.

In answer to the increasing role IT plays in identifying, preventing, mitigating, and accounting for how organizations address actual and potentially negative impact on the economy, the environment, and people, including impact on human rights, a need has emerged for providing information to business partners and other stakeholders regarding the identified impacts and the ways in which the organization has addressed these impacts. By providing this information, organizations can contribute to a more sustainable society. This IDRS allows organizations to report on their material IT topics identified as an integral part of an organization-wide report regarding sustainability as the inter-relationships with these other topics exist with IT being a backbone or opportunity to in realizing sustainability goals. By using the GRI framework as a starting point and referenced standard, the reporting organization is supported to make the reporting for the governance of IT for multiple stakeholders an integral part of their general reporting. As its requirements and complementing guidance are derived from standards and best practices, the reporting provides information on the IT topic identified in comparison with these standards and best practices, providing guidance for further development of the organization on the IT topic.

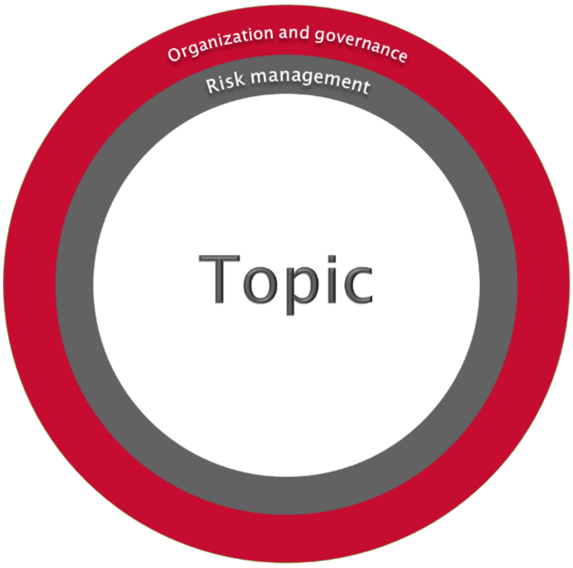
This IDRS contains disclosures for organizations to report information on IT in general and specifically on material topics identified in that domain. It provides guidance on the reporting regarding related impacts and on how a reporting organization manages these impacts. In

[3] In this IDRS standard the concept of IT also includes the use of operational technology (OT) that uses (programmed) electronic technology and de use of devices that are regarded as 'the internet of things' (IoT).

defining disclosures and requirements, the following GRI principles are leading (list and definitions to be found in GRI 1) being:

- accuracy;
- balance;
- clarity;
- comparability;
- completeness;
- sustainability context;
- timeliness;
- verifiability.

Background to Governance of IT as material topic



This standard addresses the topic of governance of information technology (IT) practices. IT plays a dominant role in realizing business goals and creating new opportunities. Moreover, IT has a significant impact on society and the sustainable operation of organizations. It is inevitable that organizations will address IT as a material topic. This reporting standard provides a basis for reporting on the control and development of IT in organizations in their role within the external environment. Every organization is likely to have its own specific IT aspects it will address as material when describing the generic governance of IT as a condition for the effectiveness of its IT operations. Therefore this reporting standard focuses on the generic governance of IT topics, its alignment with the organization's strategy and opportunities and the domain specific topics identified.

Critical for the governance of IT topics identified are "Organization and governance" and "Risk management". These reporting elements set the conditions for the governance and operation of IT that are continuously involved in the 'direction of' and 'control over' the specific material IT topic.

Every IT-related topic needs to be addressed by and managed through controls in the implemented organization and governance structure and is to be empowered by risk management to ensure that the right actions are executed in the most efficient and effective way for the organization in realizing its strategy and its role in the external environment.

For the following identified material IT (sub-domain) topics disclosures, requirements and guidance have been developed.

- Digital Innovation and Transformation;
- Data & AI;
- Third Party Management;
- Cybersecurity;
- IT Continuity Management;
- Privacy.

Sustainability impact of Governance of IT

When an organization prepares to report in accordance with this IDRS, which has been developed along the lines of the GRI framework, it is recommended that they evaluate the sustainability impact of IT. The relationship between sustainability and the governance of IT is twofold:

1. The use of IT in organizations has several sustainability impacts in its use of resources including the following categories;
    a. Environmental impact;
        i. Firstly, consumption of raw materials and energy. As IT relies on electronic devices that contain scarce resources such as metals and that consume energy to operate, organizations need to consider the environmental impact such as the raw materials consumption and carbon footprint of the IT resources used by the organization which includes its suppliers of IT products and services;
        ii. Secondly, the reduction of e-waste. It is important to implement sustainable practices in the governance of IT, considering the lifecycle of IT products and services. This includes the reduction of physical e-waste, through for example circular use of IT devices and re-use of valuable materials and the reduction of virtual e-waste by the reduction of legacy systems and underlying infrastructures that are no longer in the core focus but that cannot be decommissioned because of a knock-on effect this will or might have on core processes;
        iii. Furthermore, governance of IT as a positive impact contributes to a sustainable environment as it limits the use of scarce resources like paper and the need for transport from deliverer to receiver.
    b. Social impact, such as the human rights of workers and users of IT products and services, including labour rights and privacy-related aspects of digital products and services.
    c. Other sustainability impacts from the IT industry, including the economic impact from the IT industry as a whole on economic development of (vulnerable) regions.
2. Sustainability of organizations if IT is not properly managed.

Since availability of IT systems and services is a critical prerequisite for operational activities in almost any organization, flaws in the governance of IT can lead to operational disruptions that, if not addressed adequately, can have serious consequences for the organization, including reputational, operational, financial and even existential risks, as well as for the demand- and supply chains, eco systems and the sectors they are part of.

Governance of IT topics

As IDRS follows the structure of the GRI reporting framework, an organization that has established the governance of IT practices to be a material topic as a result of the process defined in GRI 3-1 is required to list the derived IT topics as well (using Disclosure 3-2 in GRI 3) and report how it manages the IDRS IT topics and its additionally identified and derived IT topics using Disclosure 3-3 in GRI 3: Material Topics 2021[4] and clause 1.1, 1.2 and 1.3 in this section).

For reporting on these IT topics it is important to emphasize that the IDRS is developed using the reporting conditions and structure as defined by the GRI standards. Especially for the governance of IT topics it is important to take into consideration GRI 3-2 and 3.3. In this IDRS the additional disclosures and requirements specific for the governance of IT topics have been defined.

In this IDRS, the governance of IT topics is structured around disclosures for the organization and governance of IT and risk management related to IT.

The organization of the governance of IT aims to fill in the conditions necessary to identify material impact of IT and prioritize the order to remediate potentially negative impact or new opportunities for realizing the overall organizational strategy.

Governance of IT is interrelated with organization and risk management as it is meant to guide and align IT goals with business goals in an effective and efficient way. As a result, it ensures quality of content, evaluates IT performance, ensures legal compliance and identifies business benefits.

The purpose of risk management is the creation and protection of values and the ability to act on the most significant impact on the economy, the environment, and people, including impact on human rights.

This section is therefore designed to **supplement** – and not replace – Disclosure 3-3 in GRI 3 and Appendix A.

[4] For reasons of convenience to the user the disclosures 3-3 in GRI 3: Material Topics 2021 haven been included in Appendix A to this IDRS. In this IDRS reference is made to this Appendix.

Disclosures	
GOV.1	Reporting objectives and defined target audience of the report determine specific information requirements addressed by the report.
GOV.2	Organizing and governing governance of IT to have effective, efficient and acceptable use of information technology (IT).
GOV.3	IT risk management ensures the creation and protection of value while improving performance, encouraging innovation and supporting the achievement of objectives.
GOV.4	Transparency about identified material IT topics and changes to the list of material IT topics compared to the previous reporting period[5].

Organization and Governance

The reporting organization shall report the following information regarding the organization and governance of its IT:

Requirements	
Organization and governance	
GOV.1.1	**The reporting organization shall define and describe its reporting objectives and the target audience for the report, including the derived specific information requirements.**
GOV.1.2	**The reporting organization shall stipulate limitations in terms of level of detail regarding information requirements and reported information.**
GOV.1.3	**The reporting organization shall report how it organizes and governs the IT topics using Appendix A, including:** • **The internal and external context of IT;** • **The characteristics of the organization's activities and how these determine the organization's IT;** • **The organizational structure regarding responsibilities, authorities and communication in respect of demand– and supply chain;** • **IT acquisitions with impact for the implementation of the business strategy;** • **The monitoring of the IT topics and respond from strategic level.**

[5] Unless specified otherwise, the reporting period consists of the past year and the current year (foreseeable future).

GOV.1.4	**The reporting organization shall report on the current and future capabilities of IT as part of the current and on-going needs of the organization’s business strategy specified for (future) material IT topics.**
GOV.1.5	**The reporting organization shall confirm the compliance of its IT with all mandatory legislation and regulations.**

Guidance	
Organization and governance	
GOV.1.1a	The reporting organization should make clear what the objectives are for the report. This sets important guidance for the report, i.e. in terms of distribution circle or granularity of information. If the objective for the report is external (i.e. to be published) the report is likely to contain more condensed information than if the objective is internal.
GOV.1.2a	The reporting organization should make clear what the target audience is for the report. This could include: • Whether the target audience is internal or external to the organization; • The level of (technical) knowledge that is assumed for the reader; • The specific expectations that the readers have from the report and whether those are or are not addressed in the report. • Listing of the type of users of the report, their perspective and which kind of information they require.
GOV.1.3a	The reporting organization should report the internal and external context of the governance of the IT topics and considers: • Organization IT related strategic objectives; • stakeholder expectations; • business needs; • regulatory obligations; • IT acquisitions and other IT initiatives; • business processes.
GOV.1.3b	The reporting organization should report how the organization’s activities are supported by the organization’s IT. This could include: • The nature of the organization’s activities and what requirements these imply for administrative support; • The characteristics of the industry the organization operates in in terms of IT adoption and maturity; • The (strategic) choices of the organization to be successful and the role of IT; • Recent trends and developments in the above-mentioned topics.

	• The enterprise context (industry drivers, relevant regulations, basis for competition), its current way of working and its ambition level in terms of digitization. • The performance of current IT services and develop an understanding of current business and IT capabilities (both internal and external). The current digital maturity of the enterprise and its appetite for change. • Based on the enterprise context and direction, the target IT products and services and required business and IT capabilities. Considering reference standards, best practices and validated emerging technology • Identified gaps between current and target environments and description of the high-level changes in the enterprise architecture. • Taking care of a holistic digital strategy, in cooperation with relevant stakeholders, and a detailed road map that defines the incremental steps required to achieve the goals and objectives. • Ensuring focus on the transformation journey through the appointment of a key-player who helps spearhead the digital transformation and drives alignment between business and IT. • Creating awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprise. •
GOV.1.3c	The reporting organization should report about the policy and activities to ensure that individuals and groups within the organization understand and accept their responsibilities in respect of supply and demand for IT. This includes that those with responsibility for actions also have the authority to perform those actions and make notice.
GOV.1.3d	The reporting organization should describe competency management of those given responsibility to make decisions for IT regarding acceptable use, effectivity, efficiency, integrity and availability.
GOV.1.3e	The reporting organization should describe its activities regarding the respect for human rights and human behavior, including the current and evolving needs of all the ‘people in the process’. And could report on: • customer survey outcomes; • user satisfaction survey outcomes; • training and development; • analysis of service requests.

GOV.1.3f	The reporting organization should report the objectives and the implemented monitoring for each material IT topic that is included in the report and the current status of these material IT topics.
GOV.1.3g	The reporting organization could provide information regarding performed ongoing and/or separate evaluations (by internal audit or external audit) to ascertain whether the components of internal control are present and functioning. The subjects that could be addressed are: • organization and governance of the IT; • IT capabilities; • IT acquisitions; • IT service levels; • legal compliance of IT; • human behaviour and organization culture.
GOV.1.3h	The reporting organization should report on their efforts to ensure deficiencies found in the evaluations are notified timely at the board, management, and control owners.
GOV.1.4a	The reporting organization should describe: • how and what the organization's business strategy takes into account regarding the current and future capabilities of IT; The reporting organization could describe: • the identified current and future (planned) capabilities; • the plans to satisfy the current and on-going needs of the organization's business strategy; • the status of the plans and their execution.
GOV.1.4b	The reporting organization should report which key elements make the IT fit for purpose in supporting the organization, providing the services, levels of service and service quality required to meet current and future IT requirements.
GOV.1.5a	The reporting organization should describe which relevant (types of) legislation and regulation are applicable for its IT environment. This could include the various jurisdictions that the organization is operating in.
GOV.1.5b	The reporting organization should report the effectiveness of compliance controls regarding IT for: • design and implementation of compliance controls; • monitoring of compliance controls; • periodical evaluation of the compliance controls.

	And could report on: • executed compliance audits (external/internal); • results from ad follow-up on those audits.

Risk Management

The reporting organization shall report the following information regarding the risk management of its IT:

Requirements	
Risk management	
GOV.2.1	**The organization shall report IT related risks are managed using Appendix A, including:** • **the scope and boundaries of the risk management process;** • **integration into all organizational activities;** • **Commitment of top management and governance bodies;** • **the risk management framework regarding the planning, decision making, executing, necessary modification and communication.**
GOV.2.2	**The reporting organization shall report on the continuous monitoring and adaptation of the risk management framework to address external and internal changes.**
GOV.2.3	**The reporting organization shall report on the evaluation of the effectiveness of the risk management framework based upon periodically measuring and determining its suitability to support achieving the objectives of the organization.**

Changes to material topics

The reporting organization shall report the following information regarding the changes to the list of material topics it has included in the report.

Requirements	
Material topics	
GOV.3.1	**The organization shall report the changes it has made to the list of material topics that it has included in the report, explaining the reasons for these changes.**

Guidance	
Risk management	
GOV.2.1a	The reporting organization should describe the scope and boundaries of its IT risk management and could consider: • the maturity level of the risk management process; • the basic criteria underlying IT risk management; • the risks that can arise because of the boundaries applied; • identification of critical assets; • the organization's strategic business objectives and IT policy; • expectations of stakeholders; • the geographical locations; • socio-cultural environment; • interfaces; • regulatory obligations; • business pressures (from opportunities and threats).
GOV.2.1b	The reporting organization could describe the main roles, responsibilities and accountabilities regarding: • development of the risk management process; • identification and analysis of the stakeholders; • roles and responsibilities of internal and external parties (such as business partners) and interface with organization & governance; • interface with the enterprise risk management; • escalation paths; • documentation of risk management policies and procedures.
GOV.2.1c	For describing the risk management framework the reporting organization should consider: • risk management approach; • risk identification; • risk evaluation criteria; • impact criteria; • risk acceptance criteria.
GOV.2.1d	The reporting organization could report about risk identification by considering: • identification of critical assets; • identification of threats and other possible impacts; • identification of existing controls; • identification of vulnerabilities; • identification of consequences (of unidentified risks).

GOV.2.1e	The reporting organization could report about risk analysis by considering: • the risk analysis methodology; • assessment of the threats, possible impacts and other consequences; • assessment of the incident likelihood; • level of risk determination.
GOV.2.1f	The reporting organization could report about risk evaluation by considering: • risk evaluation criteria; • risks with value levels (e,g, low, moderate, high, critical) assigned; • the importance of the business process supported by the asset / set of assets.
GOV.2.1g	The reporting organization could report about the executing of, and results from, risk treatment that consist of options: • risk mitigation or remediation; • risk modification; • risk retention; • risk avoidance; • risk sharing.
GOV.2.1h	The reporting organization should report about the risk acceptance that was made formally and documented.
GOV.2.1i	The reporting organization should include a commitment statement by top management and governance bodies on risk management considering: • the purpose to manage risks in relation to the organization's strategic objectives and other policies; • the need to integrate IT risk management in the enterprise management and culture of the organization; • making necessary resources available; • measurement and reporting within the organization's performance indicators; • review and improvement.
GOV.2.1j	The reporting organization should report on the risk communication with the decision makers (including governance bodies) and other stakeholders.
GOV.2.2a	The reporting organization should report on the execution of, and results from, risk assessments, consisting of risk identification, risk analysis and risk evaluation, which can be an iterative process.

GOV.2.2b	The reporting organization should report on the changes to (the context of) the organization as a result of the outcome of the risk assessment process and could provide an overview of the updated risk picture.
GOV.2.2c	The reporting organization should report on the changes to the risk management process due to results of that process.
GOV.2.2d	The reporting organization could provide information regarding performed ongoing and/or separate evaluations (by internal audit or external audit) of the risk management process. The subjects that could be addressed are: • effectiveness of the risk management process; • identified critical assets; • identification of risks; • evaluation of risks; • monitoring and review of the risk management process; • communication about risks and risk treatment; • effectiveness of the follow-up.
GOV.2.3a	The reporting organization should report on the evaluation of the effectiveness of the risk management framework. This could include outcomes of periodical reviews and evaluations of the framework and its components, and the subsequent improvement actions that have been defined.

SECTION 2: LIKELY MATERIAL IT TOPICS

Likely material topics

This section comprises the likely material topics for IT. In the GRI standards material topics are the topics that organizations report about. GRI 3: Material Topics 2021 chapter 1 sets out the process to determine the material topics. When developing this IDRS, conducted research activities and consultations with a broad group of potential stakeholders to discuss their views and expectations for the usability of the report on governance of IT topics. This resulted in the list of IT topics to be included in such report that are relevant for most organizations; In GRI terms 'likely material topics'. The IDRS contains the disclosures, requirements and guidance for these topics. Organizations determine their list of material topics, meaning organizations do not need to include all likely material topics in their report. It also means organizations can include their own material topics, following the guidance in GRI 3: Material Topics 2021 to determine disclosures, requirements and further content to be disclosed on such topics. The six likely material topics of the IDRS are:

1. Digital Innovation and Transformation;
2. Data & AI;
3. Third Party Management;
4. Cybersecurity;
5. IT Continuity Management;
6. Privacy.

Each topic describes the most significant IT impacts related to the topic and lists disclosures that have been identified as relevant for reporting on the topic by reporting organizations. The organization is required to review each topic in this section and determine whether it is a material topic for the organization, and then to determine what information to report for its material topics.

Topic IDRS-1 Digital Innovation and Transformation

Scope

Digital innovation & transformation (DI&T) is about the way the organization develops itself in its use of digital means to improve itself and realize its (strategic) objectives. Any organization that uses digital means has a requirement to determine, plan and execute changes to its organization and digital capabilities in order to develop to a desired future state, supporting the realization of its strategic business objectives.

Digital innovation & transformation should set the preconditions for an organization:

- to accomplish their strategic goals;
- to anticipate to new (digital driven) revenue models and create lasting value for all stakeholders (this goes beyond financial value alone);

- preserve or improve the ability and capability to anticipate on technological, sectoral and regulatory developments and alike;
- to protect digital related investments and intellectual property;
- to guarantee business continuity and going concern, attract and retain high-performing people and maintain efficient processes;
- to establish a culture of adaptability;
- to preserve or improve competitiveness and to remain relevant in the market.

Digital innovation and transformation interacts with the governance of IT topics in the following manner:

- Innovation initiatives can lead to consequences in the governance of IT topics. Specifically in case of disruptive innovation these consequences can be substantial;
- Stakeholder objectives and concerns are likely input for the architecture principles used.
- Portfolio/program and project management also applies to transformation of the IT governance structures within the organization.

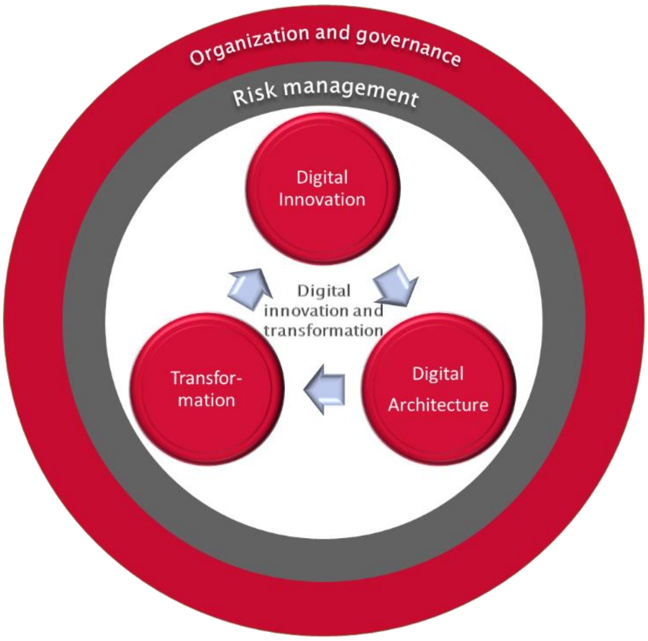
The governance of the IT topic digital innovation and transformation is addressed in section 1 “Governance of IT topics” specifying “IT Organization and governance” and “Risk management”. The requirements regarding specific roles, responsibilities and accountability for digital innovation and transformation are to be defined in this IT topic digital innovation and transformation as a result of the disclosure “GOV-1.1: IT organization and governance”.

In the context of this standard the generic aspects for IT organization and governance are described at the level of the “Governance of IT topics”. The reporting organization can decide to describe the topic specific aspects of “IT Organization and governance” in the paragraph about “Governance of IT topics” or can describe this at the IT topic digital innovation and transformation.

The risk management aspects of digital innovation and transformation, as part of the enterprise risk management, are addressed in the “IT Risk management”. Although the conditions for the risk management for digital innovation and transformation are set by “IT Risk management” and fulfilled, it is important that the monitoring of the digital innovation and transformation provides risk relevant information to the “IT Risk management” processes as well. This is part of the reporting on IT topic digital innovation and transformation.

A separate scope paragraph in the report by the reporting organization should describe how the scope of digital innovation and transformation is included in this report on the governance of IT. The scope paragraph should include clarification that the report on the governance of IT covers the past year and the current year.

Separate from the organization and governance and risk management, digital innovation and transformation has three main aspects that are important to address, including the interrelationship between these aspects to describe a resilient digital innovation and transformation management system:



Digital Innovation: is about the way the organization introduces changes (to its organization, processes, products and services, etc.) in order to realize additional value for realizing its business strategy. These changes are reflected in the enterprise architecture that the organization maintains.

Enterprise Architecture: the application of enterprise architecture methods and processes for the purpose of creating a successful digital enterprise. It is the sum of the organization's enterprise architecture domains; Business-, Data-, Application- and (supporting) Technology-architecture. It describes the digital capabilities the organization needs and plans to deliver value, as well as the organizational, systems, data and technology landscapes to enable these capabilities.

Transformation: is about the way the organization manages change to its enterprise architecture (including the application, data and technology landscapes) to accomplish its strategic objectives. For this it can maintain portfolios of change initiatives such as programs and projects. Where projects are temporary change initiatives at the lower lever aimed at achieving one or more defined objectives; programs are groupings of projects and other change activities aimed at realizing specific benefits for the organization; and portfolios are groupings of programs, projects and other change activities to realize strategic objectives. If an organization uses alternative setups to manage change, such as agile delivery, these are included as well. For the avoidance of doubt: the way individual changes (often, but not necessarily executed within projects) are handled (change management process) is part of this topic as well.

Digital Innovation and Transformation – disclosures on the governance of the topic

An organization reporting in accordance with the GRI Standards is required to report how it manages each of its material topics. An organization that has determined digital innovation and transformation practices to be a material topic in the domain of the use and the governance of IT is required to report how it manages the topic using Appendix A.

This section is therefore designed to **supplement** – and not replace the disclosures determined using Appendix A and the Governance of IT topics.

Requirements	
Governance of IT topic digital innovation and transformation	
GOV-DI&T-1.1	**The reporting organization shall report how it manages digital innovation and transformation using the requirements in Appendix A and the context and scope of digital innovation and transformation in addition to Governance of IT topics 1.1. This scope includes innovation, enterprise architecture and transformation.**
GOV-DI&T-1.2	**The reporting organization shall report how it manages the risk inherent to digital innovation and transformation in addition to Governance of IT topics 1.2.**

Guidance	
Governance of digital innovation and transformation	
GOV-DI&T-1.1a	The scope description should include the scope and context of the innovation management system, enterprise architecture management and change management system, considering: • how business objectives are set; • how innovation ideas or value opportunities are generated; • the role of architecture to align different perspectives around digital innovation and transformation initiatives; • how said initiatives are converted into changes, projects, programs and portfolios, or equivalent change initiatives; • the intended readers of the report; • scope limitations and exclusions of digital innovation and transformation.
GOV-DI&T-1.1b	The reporting organization could describe the integration of digital innovation and transformation in the wider organization, considering: • top management approval; • communication with relevant business partners; • supply chain initiatives; • documented digital innovation and transformation policies;
GOV-DI&T-1.1c	The organization could describe the roles and responsibilities regarding digital innovation and transformation in the organization, considering: its digital innovation organization;

	• the role of architecture, e.g. as a separate function. And how stakeholder needs (objectives and concerns) are translated into the architecture framework of the organization, e.g. as architecture principles. • its project, program and portfolio management organization; • the awareness around innovation and transformation in general, including regarding ethical aspects of innovation; • the various lines of defense within the organization; • the collaboration with business partners and other external parties.
GOV-DI&T-1.1d	The reporting organization could describe the results from analyzing the monitoring information regarding digital innovation and transformation, explicating identified points of improvement and which of them have been implemented in the reporting period. The organization may refer to the detailed monitoring and evaluation as per DI&T-1-1.1a and DI&T-1-3.1b.
GOV-DI&T-1.2a	The reporting organization should describe how it manages the risks that are specific for the way IT contributes to: • digital innovation, being the development and introduction of new ideas; • its transformation of the organization, governance and activities towards the targets the organization has set. The organization could describe: • its activities to prevent or reduce undesired outcomes of its innovation and transformation activities, taking into account the uncertainties associated with the innovation opportunities and the types of risk that can occur. This includes change risk. • how it responds in case review of innovation initiatives uncovers deviations from innovation policies, planning and/or budgets that carry material risk of nonconformity.

Digital Innovation and Transformation – topic disclosures

An organization is expected to compile information regarding the governance of digital innovation and transformation and provide figures regarding the occurrence of innovation events and the impact for the reporting organization and its demand and supply chain.

Disclosures Digital innovation and transformation	
DI&T-1	**Digital innovation is applied to realize business objectives. Opportunities are identified and pursued to bring innovations to life and their value/success is measured, monitored and evaluated by management.**
DI&T-2	**Enterprise architecture methods and processes are used in digital innovation and transformation.**
DI&T-3	**Transformation is applied to manage change to realize strategic objectives at four levels; individual changes, projects, programs (comprising multiple projects) and the overarching portfolio(s).**

When compiling the information specified in the disclosures, the reporting organization shall include the following requirements.

Requirements	
Topic Digital innovation and transformation	
DI&T-1.1	**The reporting organization shall report on its digital innovation process.**
DI&T-2.1	**The reporting organization shall report on the role and application of enterprise architecture in its digital innovation & transformation.**
DI&T-3.1	**The reporting organization shall report on its framework for realization of changes.**

Guidance	
Topic Digital innovation and transformation	
DI&T-1.1a	The organization should set out the highlights of its digital innovation & transformation vision and policy, which could include: • its strategic business vision in relation to the identified relevant technological, sectoral and regulatory IT related developments that could provide opportunities for innovation; • its commitment to innovation activities; • the innovation management principles it applies; • its commitment to consider ethical and sustainability aspects in its innovation activities. • how it acquires strategic intelligence it uses as input for its digital innovation and transformation.

	• how it sets innovation objectives and how these are planned (and budgeted) for; • how innovation opportunities are identified, how concepts are created and validated, and how solutions are developed and deployed; • how the innovation initiatives are evaluated in the context of the innovation objectives; • how the innovation process is evaluated. outcomes of the evaluation of the innovation initiatives lead to changes to the innovation management system of the organization.
DI&T-1.1b	The organization may describe how it makes sure the plans for innovation are: • consistent with the innovation policy, aligned with the innovation vision and are consistently applied across the organization; • communicated to stakeholders in order to create awareness and support; • measured, monitored and reviewed on a regular basis.
DI&T-1.1c	The organization could describe: • the organizational units and processes it has in place to set its innovation objectives; • how it considers creativity and exploration versus efficiency and timeliness of its innovation initiatives; • how it handles innovation initiatives that can become disruptive or radical; • how it establishes and maintains the leadership style and culture of innovations; • how it considers the needs and expectations of business partners and other external parties (stakeholders). • How it considers its end-customers and their human rights. • how it manages its intellectual property as part of its digital innovation and transformation.
DI&T-1.1d	The organization may describe initiatives in collaboration with business partners and other external parties in its ecosystem(s) to improve innovation capabilities.
DI&T-1.1e	The organization could describe the highlights of its innovation process. This may include the following: • how their innovation initiatives ideas are converted into concepts and how these concepts are explored, evaluated and refined towards solution design. • how solutions are developed, tested and deployed. • how the value generated by innovation initiatives and their resulting concepts and solutions is measured and how their evaluation is organized. This can include formal reviews by management and/or internal (or external) audit.

	• how it reviews the innovation management system and how management is involved in this process.
DI&T-1.1f	The organization may include the following aspects of the innovation management system: • suitability, how well does it fit in the organization's environment, culture, etc.; • adequacy, does it cover all aspects of innovation sufficiently; • effectiveness, does it achieve its goals; • efficiency, does it use affordable (and minimal) resources
DI&T-1.1g	The organization may include the following: • changes in the organization and its environment since the previous reporting period; • the way in which innovation objectives have been achieved; • the performance of the innovation management system, i.e. through the value created by its most significant outcomes; • the capabilities created for the organization; • deviations and nonconformities that have occurred; • the appropriateness of the evaluation and review cycle and changes that need to be made to it, if any.
DI&T-2.1a	The organization should describe: • the (types of) architecture descriptions it uses to describe its architecture from business, data, application and technology angles; • how it keeps alignment between the target architecture layers, including dependencies with business partners, suppliers or other third parties; • its mechanisms to align its innovation and change initiatives with the realization of its target architecture (architecture roadmap).
DI&T-2.1b	The organization could describe (to a certain extent, not revealing competitive information): • what its target architecture looks like; • what architecture standards it has adopted and how these standards are applied in its digital innovation and transformation; • how architecture principles are set, approved and maintained. This may include alignment with organization strategy and objectives and stakeholder expectations; • how it aligns newly developed solutions and other changes with the existing architecture.
DI&T-2.1c	The organization may describe how it updates, maintains and communicates the current architecture on the level of its:

	• strategic target architecture; • organizational target architecture; • process target architecture; • application and technology target architecture; • data target architectures.
DI&T-2.1d	The organization could describe how its change initiatives (e.g. portfolios, programs and projects) in the reporting period have contributed to realization of its target architecture.
DI&T-2.1e	The organization may describe how it periodically reviews the progress of its target architecture realization.
DI&T-3.1a	The organization should describe its policies and procedures regarding the execution of change initiatives (such as individual changes, projects, programs and portfolios).
DI&T-3.1b	The organization could describe how it conducts change, project, program & portfolio management to a certain level of detail, including: • analysis and management of the request for change and the proposed solutions, to determine and define the optimal mix of change initiatives (portfolio components); • how it monitors progress, impediments and outcomes including continuous validation of alignment with the strategic direction, operational and financial goals: • The realization process of change as part of the software development lifecycle. This includes concepts such as Devops or equivalent; • the monitoring and reporting on portfolios and their components; • financial budget and benefit tracking of portfolios and their components;
DI&T-3.1c	The organization could describe: • how it monitors the performance of change initiatives (such as individual changes, projects, programs and portfolios); • how it produces and uses management information about its change initiatives. digital innovation & transformation. This may include the progress of portfolios and their components and value creation in relation to the strategical objectives; • how it monitors alignment between the change execution (at change, project, program, portfolio level combined), the target architecture and the realization of the strategic objectives to avoid IT debt and waste of change capacity.
DI&T-3.1d	The organization should describe the following:

	• monitoring of progress of IT change initiatives versus plan; • monitoring of critical dependencies between portfolio components and/or with business partners and external parties; • tracking and measuring benefits realized by projects/programs and portfolios; • monitoring of change/project/program/portfolio budgets; • monitoring of change risk; how changes impact the risk profile and actions taken to address these impacts; • ongoing alignment with strategic, operational and financial goals.
DI&T-3.1e	The reporting organization should describe its digital innovation & transformation workforce management (as the availability of motivated and skilled resources is pivotal for the success of digital innovation & transformation). This may include qualitative and quantitative aspects of its workforce requirements and how these are sourced and maintained.
DI&T-3.1f	When describing its digital innovation & transformation workforce management the organization may describe: • whether the workforce composition (employees, contractors and other workers), knowledge & skills (learning culture, specialisms), (digital) mindset and recruitment (talent attraction, retaining scarce expertise, career opportunities, development path) are in line with the strategic ambition of the organization; • whether IT changes are executed by a competent IT workforce. • whether sourcing preferences for developing IT solutions are clear and monitoring of alignment is in place.
DI&T-3.1g	The organization may describe whether its management reporting includes aspects like: • overall IT service performance development; • digital portfolio progress & impediments; • finance (IT debt, IT spend/investments in innovation, budget overruns, IT costs (like employees, vendor services, licenses, run and security costs, generic back-office services like HR and housing); • IT change fail rate.
DI&T-3.1h	The reporting organization should provide information regarding, if any, performed ongoing and/or separate evaluations (by internal audit or external audit) of the change initiatives (project, program & portfolio management) and the effectiveness in practice.

Topic IDRS-2 Data & Artificial Intelligence

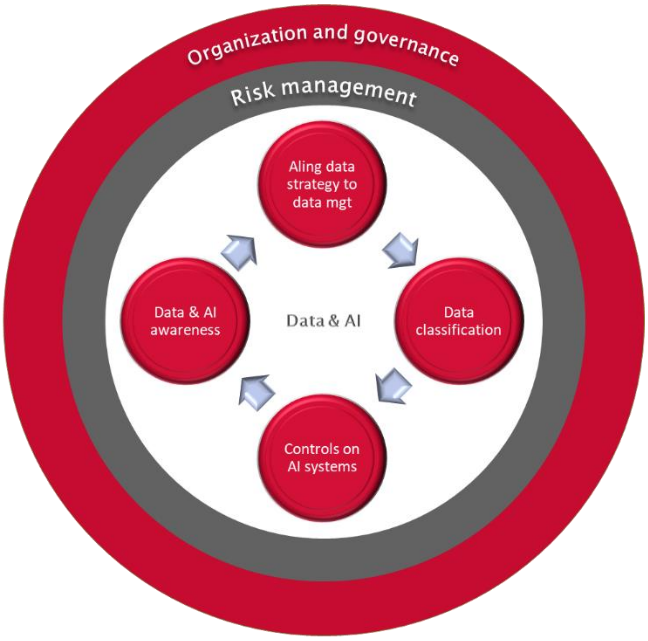
Scope

Technical and legal developments as well as the various forms of implementation of the use of data & AI are occurring at a rapid pace. This will also have consequences for the way in which the use of data & AI is reported on. The requirements outlined in this topic will therefore be regularly adjusted and supplemented in the near future.

The objective of this Data & Artificial Intelligence topic (further data & AI) is to extract the value of data processing & AI for its stakeholders through the exercise of authority, control, and shared decision-making (planning, monitoring, and enforcement) over data management and the use of AI including setting data risk appetite and constraints, protecting civil liberties, minimizing risks to individuals and society, and maximizing the public good.

Organizations with good data & AI practises are expected to be:

- trustworthy organizations for data owners and data users to transact with;
- able to provide reliable data for sharing;
- protectors of intellectual property and other value derived from data;
- organizations with policy and practice in place to deter hackers and fraudulent activity;
- prepared to minimize the impact of data breaches;
- aware of when and how data can be reused;
- able to demonstrate good data handling practises *[Source ISO 38505-1:2017].*



AI is a powerful tool for organizations. There is no directly comparable technology to AI in terms of the use of data, the breadth of its application and ease of accessibility. An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the data-input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment. AI is a general-purpose technology that has the potential to improve the welfare and well-being of people, to contribute to positive sustainable global economic activity, to increase innovation and productivity, and to help respond to key global challenges. Alongside benefits, AI also raises challenges for our societies and economies, notably regarding economic shifts and inequalities, competition, transitions in the labor market, and implications for democracy and human rights. AI thus poses a unique challenge both in formulating and enforcing regulations and norms. The large amount of data processed by AI requires to maintain trust on the use of AI. With the development and use of AI, there is also a need for an AI policy that guides the handling of AI. Organizations with mature data governance can use this to embed AI in the organization. Topics such as bias and explainability should be explained at the policy level so that these types of important decisions are not determined at the operational level and lead to non-compliance and potential reputational damage.

A management system for AI assists an organization in systematically managing the risks associated with AI deployment and enhancing the performance of AI systems. The AI management system ensures that the organization effectively deploys AI and similar algorithms in a responsible manner, improves quality, and identifies and controls risks in practice.

The AI management system should be integrated with the organization's processes and overall management structure. Specific issues related to AI should be considered in the design of processes, information systems and controls *[Source ISO 4200:2023]*.

Governance of the topic

The governance of this topic is addressed in the "Governance of topics for IT" of this standard as part of the "IT organization and governance" structure. The requirements regarding specific roles, responsibilities and accountability for governance of data & AI are to be defined in this IT topic data & AI as a result of the disclosure "GOV-1.1: IT organization and governance".

In the context of this standard the generic aspects for IT organization and governance are described at the level of the "Governance of IT topics". The reporting organization can decide to describe the topic specific aspects of "IT Organization and governance" in the paragraph about "Governance of IT topics" or can describe this at the IT topic data & AI.

The IT risk management as part of the enterprise risk management covers the specific risks involved with this topic. For data & AI the disclosures and requirements have been determined under the assumption that generic IT risk management attributes are addressed in the "IT Risk management". Although the conditions for the risk management for data & AI are set by "IT Risk management" and fulfilled, it is also important that the monitoring of the data & AI provides risk relevant information to the "IT Risk management" processes as well. This is part of the Topic description of data & AI.

A separate scope paragraph, should describe how the scope of data & AI is included in this report on the governance of IT. It is recommended to report on the data &AI of the reporting organization rather than limit it to the IT responsibilities. The scope paragraph should include clarification that the report on the governance of IT covers the past year and the current year.

For data & AI the following aspects are important to address for each aspect and the interrelationship between the aspects to build, operate and maintain a resilient data & AI system:

Improving (including innovation):

- Business processes;
- Services;
- Products;
- Accountability;
- Compliance.

Enabling:

- Customers;
- Employees;
- Supply chain partners;
- Suppliers.

Following principles of good data & AI practise, governing bodies assist management in ensuring that the use of data & AI throughout the organization contributes positively to the performance of the organization through:

- innovation in services, markets and business;
- appropriate implementation and operation of data assets;
- clarity of responsibility and accountability for both the protection and potential to add value;
- minimization of adverse or unintended consequences in the use of data & AI.

These organizations with good data & AI practises are expected to be:

- trustworthy organizations for data owners and data users to transact with;
- able to provide reliable data for sharing;
- protectors of intellectual property and other value derived from data & AI;
- organizations with policy and practice in place to deter hackers and fraudulent activity;
- prepared to minimize the impact of data breaches;
- aware of when and how data & AI can be reused;
- able to demonstrate good data & AI handling practices.

Data & AI – disclosures on the governance of the topic

An organization reporting in accordance with this standard is required to report how it manages each of its material topics. An organization that has determined data & AI practices to be a material topic in the domain of the use and the governance of IT is required to report how it manages the topic.

This section is therefore designed to **supplement** – and not replace – requirements for the governance of topics.

Requirements	
Governance of IT topic data & AI	
GOV-DATA-1.1	**The reporting organization shall report how it manages the integration of data & AI in the organization.**
GOV-DATA-1.2	**The reporting organization shall report how it addresses risks related to data & AI and depending business processes.**

Guidance	
Data & AI	
GOV-DATA-1.1a	The organization should describe the role of data to keep track of the business (such as people, accounting inventory and so on) and as a raw material for AI, information products, knowledge, innovation and insight.
GOV-DATA-1.1b	The organization should describe how: • it has assessed the risk and impact of the use of data & AI based on a stakeholder analysis; • it has defined objectives regarding data & AI in relation to the identified stakeholders; • the data & AI policies and procedures are documented and approved; • the data & AI policies and procedures set the rules to protect the use of organization's critical data and data products, in line with its business goals, strategy and risk appetite and whether they are applicable to all employees and stakeholders who are affected or could be affected by the data assets of the organization; • the implementation of the data & AI policies and procedures is supported by appropriate investments in human and technical resources; • it has established a structure for conflict resolution regarding the use of data & AI and data & AI related products, which ties back into possibly improving existing policies and procedures.
GOV-DATA-1.1c	The organization should describe whether: • roles and responsibilities are documented; • the organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control to prevent fraud, sabotage, theft, misuse of data and other compromises; • the organization obtains or generates and uses relevant, quality information to support the functioning of internal control;

	- the single Senior Responsible Owner (SRO) has approved the use of critical data before deployment and implementation; - the organization has established a mechanism allowing others to flag issues related to privacy or data protection; - assurance on data processing and AI providers is managed.
GOV-DATA-1.1d	When reporting on the result of the analysis of monitoring data & AI and identifying and implementing points of improvement the organization should describe the use of appropriate measurement systems, the performance of data & AI use of the organization, further the way strategies relating to data are being implemented an the use of data & AI conforms internal policies and external requirements such as regulations and stewardship requirements, including: - data retention and disposal requirements - reuse, sharing or selling of data and its associated rights, licensing or copyright; - accounting for cultural norms, ethical standards, bias, discrimination or profiling in decision making.
GOV-DATA-1.2a	When reporting on risks related to data & AI and depending business processes the organization should describe whether: - the risk associated with data and AI is examined to ensure an appropriate level of data risk aligns with the overall risk appetite; - not using available data for the benefit of manage operational risks, such as financial risks, safety data and new types of customer organizations is examined; - lack of trustworthy or business relevant data impacts the ability to carry out critical organizational functions; - decision making on data and the use of AI meets ethical standards and counteract bias, discrimination or profiling.

Data & AI – topic disclosures

An organization is expected to compile information regarding the governance of data & AI and provide figures regarding the occurrence of data breach events and the impact for the reporting organization and its supply chain.

Disclosures IT topic data & AI	
DATA-1	**Data & AI management is aligned to data & AI strategy**

DATA-2	**Employees are aware of the safe use and protection of the organization's data assets.**
DATA-3	**AI systems and other decision supporting systems are controlled.**
DATA-4	**Data is classified based on criticality/sensitivity.**

When compiling the information specified in the disclosures, the reporting organization shall include the following requirements.

Requirements	
Topic data & AI	
DATA-1.1	**The organization shall report on the way it aligns its data & AI strategy and data & AI policy.**
DATA-2.1	**The organization shall report on activities to promote awareness and IT literacy on data & AI.**
DATA-3.1	**The organization shall report on the control activities concerning the use of AI and other decision supporting systems.**
DATA-4.1	**The organization shall report on data classification policies and procedures and what measures are applied based on the classified criticality/sensitivity of the information.**

When reporting on its approach of data & AI the reporting organization should apply the following guidance.

Guidance	
Topic data & AI	
DATA-1.1a	When reporting on the way it connects data & AI management to data & AI strategy the organization should describe the way the governing body and management teams work together to implement the strategy to support data & AI management and take value, risk and constraints concerning the collection, storage, reporting, decision making, distribution and disposal of data into account.
DATA-1.1b	When reporting on management of data & AI the organization could describe the way it manages the quality of transaction data, product data and business master data through:

	• data &AI operations processes that focus on data quality and the usage of data, including data & AI architecture management, data & AI design and data & AI processing; • data & AI quality monitoring defining a systematic approach to assess the levels of data & AI quality, including data & AI quality planning, data & AI quality criteria setup and data & AI quality measurement; • data & AI quality improvement processes, including data & AI stewardship and data flow management, data & AI error cause analysis and data & AI error correction.
DATA-1.1c	The reporting organization should provide information regarding, if any, performed ongoing and/or separate evaluations (by internal audit or external audit) of the effectiveness of controls related to data & AI, and the follow-up to findings addressing nonconformities, their causes and the verification of the actions taken on these findings.
DATA-2.1a	When reporting on data & AI awareness and information campaigns the organization should describe: • the regular data & AI awareness and information campaigns it has in place to inform all employees in the organization; • the measures to ensure, to their best extent, a sufficient level of AI literacy of the staff members and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used • the safe use and protection of the organization's data assets, IT/AI systems AI (and other) risks employees should be aware of, including AI act and GDPR non-compliance, fundamental human rights, possible internal or external violations and their role in mitigating data & AI breaches; • mandatory training for newcomers on data governance and training on AI; • specific training for senior management on data & AI; • if the Intranet site has a dedicated section on data & AI topics, guidelines and best practices, including a (whistle blower) hotline to report any issues.
DATA-3.1a	The organization shall describe how it has performed an assessment on: • the impact of its AI systems, in line with the criticality of the area to be protected and the data processed, to assess its broader societal impact (e.g., impact beyond the individual (end)user, such as potentially indirectly affected stakeholders) and the steps the organization has taken

	to counteract identified risks, differentiated in 3 risk categories based on the potential danger the applications pose: 1. unacceptable risk applications, 2. high-risk applications and 3. limited or low-risk applications. ○ The first category bans applications and systems that create an unacceptable risk. For example, unacceptable uses include real-time biometric identification in public spaces, where AI scans faces and then automatically identifies people. ○ The second category covers high-risk applications, such as a resume-scanning tool that ranks job applicants based on AI. This type of application is subject to strict regulations and additional protective measures to ensure that people are not discriminated against based on their gender, ethnicity or other protected characteristics. Higher-risk AI systems are those that may have more serious implications, such as automated decision-making systems that can affect people's lives. In these cases, it is important that users are made aware of the implications of using such systems and are given the option to opt out if they feel uncomfortable. ○ The third category is limited-risk AI systems, which are those that have specific transparency obligations of which users must be made aware. This allows users to make informed decisions about whether they wish to continue with the interaction. Examples of low-risk AI systems include AI-enabled video games or spam filters, which can be used freely without adverse effects. • the legal compliance of the AI system and its underlying technology.
DATA-3.1b	When reporting on the use of AI systems the organization should describe how: • the organization has involved stakeholders that are impacted by the AI system during development and implementation; • the organization has arranged the task allocation between the system and humans for meaningful interactions and appropriate human oversight and control; • the organization has implemented an appropriate level of human control to control the risks of the AI system and its outcomes; • the organization implemented measures to respect the rule of law, human rights, democratic values and diversity, and includes appropriate safeguards to ensure a fair and just society;

	• the organization measures, mitigates and monitors regularly how the model performs against prohibited discrimination grounds (including how this monitoring is performed); • the organization regularly monitors the outcome of the AI system against bias. • the organization ensures transparency and responsible disclosure around AI systems to safeguard that people understand when they are engaging with them and can challenge outcomes; • the organization safeguards that AI systems are robust, secure and safe throughout their entire lifecycle so that, in conditions of normal use, foreseeable use or misuse, or other adverse conditions, they function appropriately and do not pose unreasonable safety risk; • the organization can be held accountable for the proper functioning of AI systems and for the respect of the above principles, based on their roles, the context, and consistent with the state of art.
DATA-3.1c	When reporting on the use of AI systems the organization should describe, following ISO 42001:2023, the • determination of organizational objectives, involvement of interested parties and organizational policy; • management of risks and opportunities; • processes for the management of concerns related to the trustworthiness of AI systems such as security, safety, fairness, transparency, data quality and quality of AI systems throughout their life cycle; processes for the management of suppliers, partners and third parties that provide or develop AI systems for the organization.
DATA-4.1a	When reporting on data classification the organization should describe whether: • the organization maintains documented, approved and enforced data classification policies and procedures, describing how to classify information based on confidentiality, authenticity, integrity, availability and legal/ regulatory requirements (e.g. data protection); • clear owners of the information (categories) are determined, to properly conduct the data classification; • data classification policies and procedures describe what control measures are applied based on the classified criticality/sensitivity of the information.

Topic IDRS-3 Third Party Management

Scope

Third-party management involves the way in which organizations oversee and control interactions with external entities that provide goods, services, or perform functions on behalf of the organization. Reasons for organizations to use third-parties can include managing their cost, transfer risks, obtain access to scarce knowledge or realize strategic business objectives.

Third party management is an important means to optimize value chains across organizations, where comparative advantages in terms of economies of scale and use of scarce resources or knowledge can be shared between organizations. In today's world where digitization enables seamless connectivity between organizations, their ecosystem partners, clients and suppliers, third party management has become a common way to manage supply chains, build market platforms and other types of business models. As the business processes and/or functions that are outsourced to third parties often rely on IT regarding continuity and security, this standard focuses on the management of such outsourced services and processes from an IT perspective. Meaning that in this IDRS outsourcing is regarded to entail the IT aspects of the outsourced services and processes.

When looking at (the IT aspects of) Third party management in the context of optimizing an organizations value chain it is important to note that, where tasks and processes can be outsourced, the responsibilities that an organization has towards its stakeholders cannot. This requires the organization to establish appropriate oversight over its third parties. And to assess and monitor risks related to the activities of the third-party, perform due diligence as well as monitoring of the overall performance in terms of strategic value and financial and operational outcomes.

It is particularly important to note that in this due diligence and monitoring of third parties, the other material IT topics of this IDRS (such as cybersecurity, IT continuity, data governance and AI, privacy, etc.) are regarded. The reporting prescribed by this IDRS expects these topics and the way they are managed (by the organization's third parties) to be described in the sections where these material IT topics are described. To prevent duplication of requirements in this IDRS, the third-party management section describes the way third parties are managed, not the content of the material IT topics that are performed by the third parties.

In certain sectors third-party management is bound to specific supervisory regulations. Where regulatory requirements apply, these requirements should be regarded as a minimum level in the reporting of organizations and be regarded as an integral part of the reporting requirements.

Governance of third-party management is seldom the sole domain of the IT function. Due to the possibilities it offers to achieve strategic advantages and/or financial benefits most organizations that have reached a certain level of maturity often treat third-party management as a strategic means, involving appropriate levels of management to oversee and steer it. This includes organization wide competencies (such as business, finance, compliance, legal, risk, IT, IT risk) across various lines of defense. For the purpose of reporting on the governance of IT topics the involvement of all these disciplines is in scope, provided they are applicable to way the organization manages third parties.

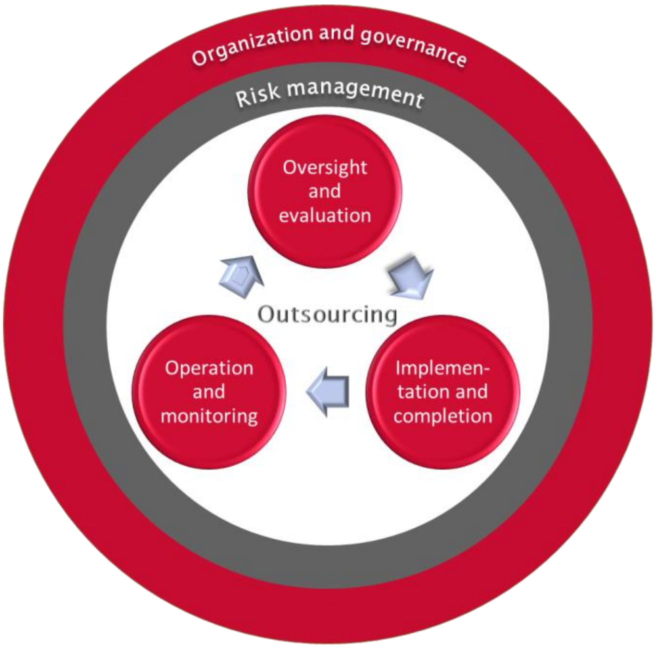
The governance of the IT topic third-party management is addressed in section 1 “Governance of IT topics” specifying “IT Organization and governance” and “Risk management”. The requirements regarding specific roles, responsibilities and accountability for third-party management are to be defined in this IT topic third-party management as a result of the disclosure “GOV-1.1: IT organization and governance”.

In the context of this standard the generic aspects for IT organization and governance are described at the level of the “Governance of IT topics”. The reporting organization can decide to describe the topic specific aspects of “IT Organization and governance” in the paragraph about “Governance of IT topics” or can describe this at the IT topic third-party management.

The risk management aspects of third-party management, as part of the enterprise risk management, are addressed in the “IT Risk management”. Although the conditions for the risk management for third-party management are set by “IT Risk management” and fulfilled, it is important that the monitoring of the third-party management provides risk relevant information to the “IT Risk management” processes as well. This is part of the reporting on IT topic third-party management.

The report section on third-party management should contain a separate scope paragraph where the scope of third-party management is included. It is recommended to report this scope from the (wider) business view on third-party management of the reporting organization rather than limit it to the IT perspective of third-party management. The scope paragraph should include clarification that the report on the governance of IT covers the past year and the current year.

For the structure of IT reporting about third-party management three aspects are distinguished that, including their interrelationships, are used to describe a resilient third-party management system:



- Oversight and evaluation: describes how third-party management is overseen and controlled, how opportunities to use third parties are identified, how the overall value and other objectives of third parties are monitored and evaluated, and how the third party services portfolio is connected to the rest of the organization;
- Implementation and completion: describes the evaluation and selection of (candidate) providers, the contracting of the products and services and the subsequent implementation of the third party arrangement, as well as the decommissioning of the arrangement upon completion or termination;
- Operation & monitoring: describes the delivery of services, including the connections (interfaces and handovers) with the rest of the organization, and service management.

Third-party management – disclosures on the governance of the topic

An organization that has determined third-party management of processes or services to be a material topic in the use and governance of IT is required to report how it manages the topic using Appendix A (see requirement GOV-TPM-1.1 in this section).

This section is therefore designed to **supplement** – and not replace – requirements in Appendix A and section 1: Governance of IT topics.

Requirements	
Third-party management	
GOV-TPM-1.1	**The reporting organization shall report how it governs third-party management using requirements in Appendix A and the context and scope of the third-party management in addition to 'Governance of IT topics' 1.1.**
GOV-TPM-1.2	**The reporting organization shall describe how it manages risks related to its use of third party processes and services in addition to 'Governance of IT topics' 1.2.**

Guidance	
Governance of IT topic third party management	
GOV-TPM-1.1a	The reporting organization should describe the internal and external context and considers: • stakeholders and their relevant requirements; • legal and regulatory requirements; • mission, goals and internal and external obligations; • the parts of the organization that are impacted by third party management; • the intended readers of the report; • products, processes and/or services that are included.
GOV-TPM-1.1b	The reporting organization should describe the integration of third party management as a tool of management in the overall value chain of the organization considering: • impact on customer experience including their human rights; • impact on (IT) employees and other workers, including their human rights; • impact on the organization's ecosystem; • approval by governance bodies; • scope limitations and exclusions. The organization could report on: • communication with relevant business partners; • documented third party management policy; • reviewed in conjunction with the organization strategic goals and objectives.
GOV-TPM-1.1c	The reporting organization should report on the roles and responsibilities regarding third party management, including management and governance bodies, which are documented and implemented in order to support the (IT) Strategic objectives. The organization could report on: • IT and information security key roles, such as Chief Information Officer (CIO's), Chief Operating Officer (COO) and Chief Information Security Officer (CISO), and whether these are well supported and have adequate access to the management body in order to escalate IT topics when needed. • whether the organization maintains a register of third parties and the processes and products or services they provide.

	• whether the third party management policy defines roles and responsibilities, as well as competencies required to monitor and manage the risks from the third party services.
GOV-TPM-1.1d	The reporting organization could describe the results from analyzing the monitoring information regarding third party processes and services, such as service level reporting, performance/value management, incident information, contract management topics, etc., regarding points of improvement and which of them have been implemented in the reporting period.
GOV-TPM-1.2a	The reporting organization should report how it identifies, assesses, monitors and manages all risks related to third party management, where it could consider the IT related risks from angle of the following risk domains: • cyber security risks; • operational risks; • continuity risks; • data related risks such as confidentiality, authenticity, integrity, availability and portability of data; • compliance risks, e.g. with applicable regulatory requirements, including data privacy; • governance risks; • legal risks, including the contractual arrangements; • how it assesses the risk that third party management impacts the experience by the customer; • third-party risks; • financial risks.

Third party management – topic disclosures

If an organization, when reporting in conformity with this standard, uses third parties to provide processes or services where these are supported by IT it is expected to compile information regarding the governance of third party management, at least from a perspective of the IT support of these processes or services, and provide information about the impact the third party management has for the reporting organization and its demand and supply chain.

Disclosures Third party management	
TPM-1	**Third party management is governed and managed and the value and other overall objectives of third party management are monitored and evaluated.**

TPM-2	**Candidate third parties for providing processes and services are selected, evaluated (to determine preferred candidate) and services are contracted, implemented and (eventually) terminated based on identified requirements;**
TPM-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;**

Requirements	
Topic Third party management	
TPM-1.1	**The organization shall report how it conducts ongoing oversight over its third party portfolio, including the ongoing evaluation of the overall third party performance against objectives.**
TPM-2.1	**The reporting organization shall report on its processes, policies and procedures for the initiation, implementation and termination of third party processes and services.**
TPM-3.1	**The reporting organization shall report on its policies and procedures on the ongoing monitoring of the performance of third party processes and services. This includes responding to occurrences (e.g. incidents) and other service management aspects.**

Guidance	
IT topic Third party management	
TPM-1.1a	The organization should describe how it handles, in the context of its strategic ambitions, the following topics: • its third party strategy, which includes alignment with the overall organization strategy; • the third party management governance, which includes decision making by senior executives and involvement of governance bodies.
TPM-1.1b	The organization could describe how it handles, in the context of its strategic ambitions, the following topics in relation to third party management: • value management; • organizational change management; • people management;

	• service level management and contract management; • incident management; • knowledge management; • technology management; • threat management.
TPM-1.1c	The organization could describe how it handles the following topics: • the identification of opportunities for using third parties to realize strategic goals by e.g. outsourcing processes and/or services to external service providers • its third party management approach, which includes the types of third party activities considered, the business case approach, the impact and risk analyses and decision making process; • its third party management planning, which includes the sourcing implementation plan; • communication to stakeholders about (changes in) the portfolio of third party services.
TPM-1.1d	The organization should describe its portfolio of planned and realized third party services, stipulating the services that have been initiated, transferred or terminated during the reporting period.
TPM-2.1a	The organization should describe how it handles the initiation of third party arrangements. This could include: • setting requirements for third party opportunities; • identifying candidate providers; • selection criteria, including sustainability topics (ESG); • selecting providers, including due diligence; • risk assessment of third party opportunities; • establishing third party agreements.
TPM-2.1b	When reporting on its approach of initiating third party processes or services, if applicable in the reporting period, the organization should describe how it handles the service transfer. This should include: • if applicable, the possible transfer of employees and other workers, including their human rights. This could include: • the planning and design of the transfer activities;

	• the possible transfer of staff and assets and the related legal and change management procedures; • the communication aspects related to the start of the services by the third party.
TPM-2.1c	The organization should describe, when applicable, how it adheres to the regulatory requirements for third party management. This could include describing how it provides for the following items in the agreements with third parties: • direct audit rights at the provider; • direct access by supervising / regulating bodies to the provider (if applicable); • availability, authenticity, integrity and confidentiality of data and information; • appropriate exit plans in case of planned/unplanned termination.
TPM-2.1d	The organization should describe, when applicable, how it handles the following topics: • decommissioning of the service in general; • the (re-)transfer of workers including their human rights; • the continuity of the business process supported by the third party.
TPM-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; • fulfilment of contractual, compliance and regulatory obligations.
TPM-3.1a	When reporting on its approach of managing operational third party processes and services (if any) the organization should describe how it handles service management. This could include the following topics: • performance monitoring of the processes and services; • financial management; • agreement management; • incident management; • managing changes.
TPM-3.1b	The organization should describe, if applicable in the reporting period, how it obtains assurance over the third party processes and services, e.g. through Service Organization Control reports or other types of reporting.

TPM-3.1c	The organization could describe how it applies, based on the outcomes of ongoing monitoring of the performance, and potential changes on the demand side of the processes and services, a change cycle, e.g. according to plan-do-check-act.

Topic IDRS 4 – Cybersecurity

Scope

Cybersecurity is primarily concerned with *[Source ISO 27100:2018]* safeguarding of people, society, organizations and nations from cyber risks. Cyber risks occur where digital interaction takes place among organizations and people with public or private entities take place, including formal and informal interactions. Therefore, cybersecurity differs from information security by perspective and concerns while they are closely related. Information security addresses maintaining the confidentiality, authenticity, integrity and availability of information while cybersecurity focuses on managing cyber risks that can have impact on environment, humans and economy and is not only restricted to information. Especially cybersecurity also needs to address cyber risks that might occur for other technology then Informational Technology, like OT (Operational Technology), IoT (Internet of Things) and IIoT (Industrial Internet of Things).

Any interaction made possible through cyberspace potentially has a near-instantaneous impact anywhere in the world and could impact organizations. The interaction with other entities and business partners through cyberspace and the dependencies on this interaction for the reporting organization, result in the necessity to have a fair view on cyber risks in business relationships. Therefore, the effectiveness of cybersecurity depends on the level of cybersecurity throughout the value chain of closely operating business partners. It is the responsibility of the reporting organization to control its connections and activities in cyberspace, perform due diligence and contribute to the cybersecurity of the value chain of business partners on which it relies for achieving its business objectives.

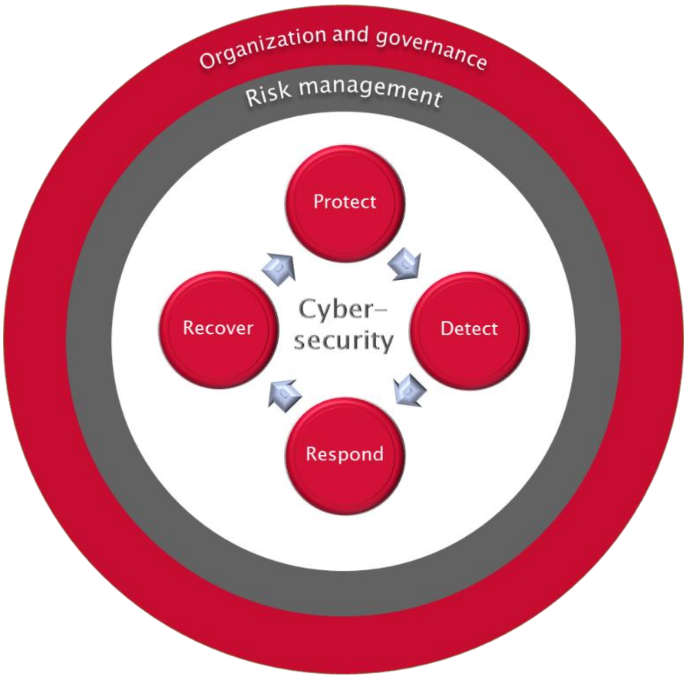
The objective of adequate cybersecurity is *[Source ISO 27100:2018]* to maintain an acceptable level of stability, continuity and safety of business partners and people operating in cyberspace. For current business and future development it is important that the organization proofs to be a valuable and trusted partner in business relationships and determines in its due diligence the potential impact that cyber risks, if not adequately addressed by the organization and its business partners, may have a negative effect on economy, environment, and people, including impacts on their human rights.

Given the constraint that the reporting organization needs to realize this objective against affordable cost, several stakeholders are interested in the decision making and level of cybersecurity of the organization. While it is not possible to always achieve this objective, cybersecurity aims to reduce cyber risks to an acceptable level. Although cybersecurity is a goal for the reporting organization as a whole, IT provide numerous services to mitigate (impacts from) cyber risks. In this reporting initiative the scope is governance of IT regarding cybersecurity, although this should be aligned with the corporate strategy that covers cybersecurity from an enterprise perspective. This alignment is addressed in disclosures GOV-CYBER-1.1 and GOV-CYBER-1.2. If such a corporate strategy does not exist, this reporting initiative still provides a reporting standard to inform stakeholders.

The IT governance determines the identified goals for the department regarding cybersecurity based upon the strategic goals of the reporting organization.

The governance of the IT topic cybersecurity is addressed in section 1 “Governance of IT topics” specifying “IT Organization and governance” and “Risk management”. The requirements regarding specific roles, responsibilities and accountability for cybersecurity are to be defined in this IT topic cybersecurity as a result of the disclosure “GOV-CYBER-1.1: IT organization and governance”. In the context of this standard the generic aspects for IT organization and governance are described at the level of the “Governance of IT topics”. The reporting organization can decide to describe the topic specific aspects of “IT Organization and governance” in the paragraph about “Governance of IT topics” or can describe this at the IT topic cybersecurity.

The risk management aspects of cybersecurity, as part of the enterprise risk management, are addressed in the “IT Risk management”. Although the conditions for the risk management for cybersecurity are set by “IT Risk management” and fulfilled, it is important that the monitoring of the cybersecurity provides risk relevant information to the “IT Risk management” processes as well. This is part of the reporting on IT Topic Cybersecurity.



A separate scope paragraph, in the report from the reporting organization, should describe how the scope of cybersecurity is included in this report on the governance of IT. It is recommended to report on the cybersecurity of the reporting organization rather than limit it to the IT responsibilities. Furthermore it is, given the implicit attribute of cyber risks to have potential impact for everyone connected to cyber space, necessary to identify the scope from a demand and supply chain perspective as well. Especially for the IT topic cybersecurity, the reporting organization needs to be aware that sharing information about the cybersecurity status can imply an increase of vulnerability. As business partners should be adequately informed, the reporting organization should determine the level of required detail to inform other stakeholders in general. If requirements are not addressed in the report, it is required to specify this in the GRI content index (if GRI is used), and provide a reason for omission with an explanation according to GRI-3 “Using this Standard”. The scope paragraph should include clarification that the report on the governance of IT covers the past year and the current year.

As part of the enterprise risk management the reporting organization should report how the cyber risks are identified and related to critical systems. The following elements of cybersecurity are the foundation to address relevant controls and their interrelationship to build, operate and maintain a resilient cyber security management system to address the cyber risks identified :

- Protect for cyber risks;
- Detection of potential threats;
- Respond to a cyber incident;
- Recover from a cyber incident.

Cybersecurity – disclosures on the governance of the topic

An organization reporting in accordance with the GRI Standards is required to report how it manages each of its material topics. An organization that has determined Cybersecurity practices to be a material topic in the domain of the use and the governance of IT is required to report how it manages the topic using Appendix A (see requirement GOV-CYBER 1.1 in this section).

This section is therefore designed to **supplement** – and not replace – the disclosures determined using Appendix A and the Governance of IT topics.

Requirements	
Governance IT topic Cybersecurity	
GOV-CYBER-1.1	**The reporting organization shall report how it governs cybersecurity using Appendix A and the context and scope of the cybersecurity governance in addition to 'Governance of IT topics' 1.1.**
GOV-CYBER-1.2	**The reporting organization shall report how it manages (potential) cyber risks in addition to Governance of IT topics 1.2.**

Guidance	
Governance IT topic Cybersecurity	
GOV-CYBER-1.1a	The scope description should include the context of the cybersecurity management system considering: • business activities, product and/or services that are potentially impacted by cyber risks; • its relation with other entities that operate in the same cyberspace for which the organization is dependent regarding its own continuity and protection of assets and resources; • applicable law and specific regulatory requirements; • the intended readers of the report; A disclaimer could be stated that cyberspace is constantly evolving and a complex environment with public components and other people and entities attached. This is contextual for the report

	presented at a certain date while developments might have unforeseen impact at reporting date.
GOV-CYBER-1.1b	The reporting organization could describe the integration of the cybersecurity with the information security in the organization considering: • top management approval; • scope including limitations and exclusions; • communication with relevant business partners; • documented cybersecurity management policy; • reviewed in conjunction with the enterprise information security and (IT) continuity management policy and planning.
GOV-CYBER-1.1c	The reporting organization could describe the cybersecurity policy and plan considering: • accountability for the cybersecurity management; • current cyber risk posture; • resource availability in terms of timely, quality and quantity; • awareness and training; • testing the effectiveness of the cybersecurity management; • potential costs and benefits; • technological limitations and/or opportunities; • involved business partners and (security) service providers; • identified regulatory obligations.
GOV-CYBER-1.1d	The reporting organization could report the results from analyzing the monitoring information regarding protection safeguards, detecting potential cyber risk events, responses to occurred incidents and executed recoveries regarding points of improvement and which of them have been implemented in the reporting period.
GOV-CYBER-1.2a	The reporting organization should describe the integration of the cyber risk management in the enterprise risk management process in addition to Governance of IT topics 1.2 considering: • determined critical IT; • (cyber related) threats and vulnerabilities; • results from impact analysis; • monitoring the development of identified cyber risks; • options for protection, resilience, recovery and restoration; • risk responses; • role and responsibilities in the demand and supply chain; • maintaining sufficient IT cybersecurity skills and knowledge

	• legal and regulatory requirements regarding cybersecurity and cyber risk management including civil liberties obligations
GOV-CYBER-1.2b	The reporting organization could describe the goals and the changes in cyber risks, and/or cybersecurity management, compared to the former reporting period considering: • identification of new critical IT; • new identified threats; • potential impacts of identified threats for critical IT; • detection of potential threats; • responses to incidents; • recovery from incidents; • the organization's risk appetite; • technical requirements (segmentation, back-up, encryption, outsourced IT); • identity and access policies
GOV-CYBER-1.2c	The reporting organization could also report about: • the interaction with the public authorities regarding occurred cybersecurity events and the follow-up by the reporting organization;

Cybersecurity – topic disclosures

An organization is expected to compile information regarding the governance of cyber risks and figures regarding the occurrence of cyber risk events and the impact for the reporting organization and its demand and supply chain.

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

Requirements	
IT Topic Cybersecurity	
CYBER-1.1	**The reporting organization shall report the status of, and the activities for, protection safeguards that limit cyber risks.**
CYBER-2.1	**The reporting organization shall report the activities for timely detection of cyber risk events.**
CYBER-3.1	**The reporting organization shall report the activities with regards to the response on cyber risk incidents.**
CYBER-4.1	**The reporting organization shall report the activities to recover from cyber risk incidents and the impact on:** • **business partners;** • **economy;** • **environment and /or ;** • **people, including impacts on their human rights.**

Guidance	
Topic Cybersecurity	
CYBER-1.1a	The reporting organization should describe how its access control establishes that: • employees, business partners and other involved external persons and workers are aware, informed and managed for securing access to critical IT; • identities and credentials are managed for authorized devices and users including secure authentication of users; • physical access and remote access (including for maintenance purposes) are managed and protected; • the organization manages access permissions by using the principles of least privilege and segregation of duties; • the network integrity is protected against unauthorized access, including network segregation as appropriate.
CYBER-1.1b	The reporting organization should describe how it manages that: • all users are informed and trained and • roles and responsibilities of senior executives, privileged users, employees and other workers and third party stakeholders (e.g. suppliers, customers, business partners) are understood towards both physical security and information security;.

CYBER-1.1c	The reporting organization should describe how it establishes that: • data at rest is protected; • data-in-transit is protected; • assets are formally managed through removal, transfers and disposal; • capacity is planned to ensure availability. The organization may describe its activities regarding: • data leakage protection; • integrity checking mechanisms to verify software, firmware, and information integrity; • protection of communications and control networks; • securing logfiles.
CYBER-1.1d	The reporting organization could report on the system development life cycle to manage systems and could report on the change control process. The organization may include in the description the use of separate environments for at least development, test and production and specific controls regarding the change control using these separate environments.
CYBER-1.1e	The reporting organization should report on the patch management process. The organization could report about: • identification of patch sensitive software and assets; • routine patching; • emergency patching; • emergency mitigation; • unpatchable assets (if any); • patch management security impact and controls; • impact for maintenance plans.
CYBER-1.1f	The reporting organization should report on the backup strategy and activities to ensure that backups are conducted, secured, maintained and tested periodically.
CYBER-1.1g	The reporting organization could report on the monitoring of the effectiveness of the protective controls and on the process improvements as result of this monitoring, including the communication about the status of the protective controls with appropriate partners and management.
CYBER-2.1a	The reporting organization should report on the detection controls. The organization may report on: • implemented audit / log records;

	• installed logging of sensors, and their review; • changes in critical business applications, data and databases; • changes in digital infrastructure; • tested detection processes and the results; • the required and available skills and competencies for analyzing logs; • involvement of third party services; • the use of Security information and event management solutions; • enabling technologies and/or equipment.
CYBER-2.1b	The reporting organization could report on the analytical use of logging to identify and understand attack targets and methods. The organization may report about: • the involvement of an internal or external provided Security Operations Centre; • the type and volume of identified hacks during the reporting period; • setting thresholds based upon the outcome of the risk management process; • addressed threats in conjunction with connected partners.
CYBER-2.1c	The organization should report about the monitoring, and could report on: • monitoring for unauthorized access to connections, devices and software; • external service provider activity; • malicious code.
CYBER-2.1d	The reporting organization may report on detected events with identified potential impact and follow-up considering the impact on: • business partners; • economy; • environment; • people, including impacts on their human rights.
CYBER-2.1e	The reporting organization could report on their activities for vulnerability management. The organization may report on performed vulnerability scans including follow up, status of mitigation and the involvement of appropriate partners.
CYBER-2.1f	The reporting organization could provide information regarding, if any, performed ongoing and/or separate evaluations (by internal audit or external audit) of the effectiveness of detection controls and the follow-up to findings

	addressing nonconformities, their causes and the verification of the actions taken on these findings.
CYBER-3.1a	The reporting organization should report the response planning, and testing the effectiveness of these plans in practice, including the collaboration with appropriate partners and relevant business partners.
CYBER-3.1b	The reporting organization should report on the response process for incidents that have arisen. The organization could report on: • the investigation of notifications from the detection system(s); • the categorization of incidents with identification of their (potential) impact; • the involvement of employees and other workers and appropriate business partners with their responsibilities, role and order of operations when an incident occurs; • the security during the disruption caused by an incident; • the collection of evidence; • the containment of incidents; • the impact on: ○ business partners; ○ economy; ○ environment; ○ people, including impacts on their human rights.
CYBER-3.1c	The reporting organization could report on the information communicated regarding the execution and results of responses. The organization can make this specific for: • informing top management including governance bodies; • informing involved employees and other workers; • information provided to business partners and other stakeholders; • information provided to oversight bodies and/or supervisory entities.
CYBER-3.1d	The reporting organization may report about occurrences of executed response plans, their effect, impact and identified (potential) improvements.
CYBER-3.1e	The reporting organization could provide information regarding, if any, performed ongoing and/or separate evaluations (by internal audit or external audit) of the response processes and the effectiveness in practice.

CYBER-4.1a	The reporting organization should report on the process to restore its IT after incidents.
CYBER-4.1b	The reporting organization may report about: • period of unavailability; • data loss; • financial impact for recovering ; • the wider economic impact; • impact on humans.
CYBER-4.1c	The reporting organization may report on occurrences of executing response plans, their effect and impact.
CYBER-4.1d	The reporting organization could provide information regarding the communication of executing restore plans and can make that explicit for: • improvements of the process to be addressed by the top management; • dependencies from business partners; • the joint efforts in the relevant supply chain to limit the impact of incidents;
CYBER-4.1e	The reporting organization could provide information regarding, if any, performed ongoing and/or separate evaluations (by internal audit or external audit) of the recovery processes and the effectiveness in practice.

Topic IDRS 5 – IT Continuity Management

Scope

Business Continuity Management can be defined as the management system that provides the capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption. *[ISO 22300:2018]*.

Failures of IT services do have an increasing impact on the continuity of business operations. As critical business functions, that require business continuity, are generally reliant on IT the governance of IT regarding continuity and security becomes a key part of the enterprise continuity management. Separate from the impact on the organization, unavailability of IT may have a negative effect on the wider economy, environment, and people, including impacts on their human rights.

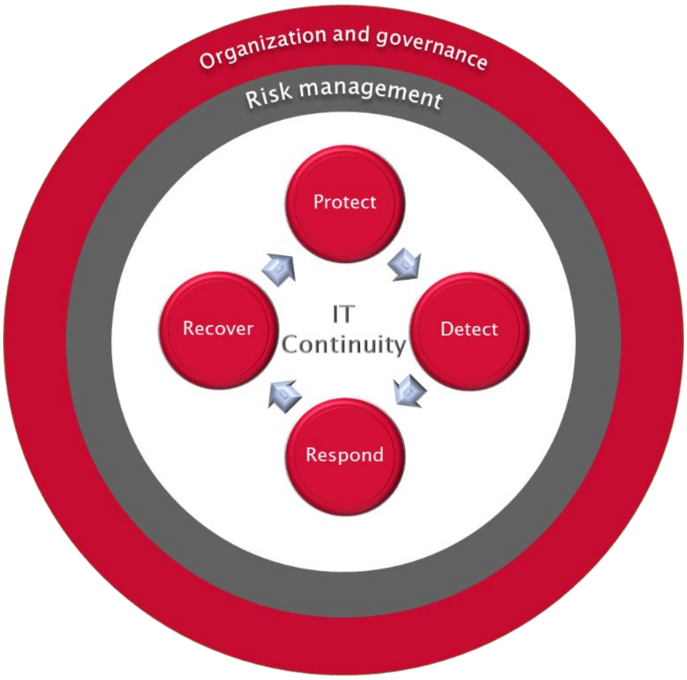
Given the constraint that the reporting organization needs to realize these objectives against affordable cost and continuity management of IT contributes to the business continuity of the organization, several stakeholders are interested in the decision making and level of control over IT continuity by the organization.

The objective of business continuity management is to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise. Although business continuity management is a goal for the reporting organization as a whole, IT provide numerous of services to mitigate the risks for unavailability of the IT that has impact on critical business functions. IT continuity management should be part of the business continuity management of the reporting organization. A business continuity management system can effectively protect against harm to humans, assets and environment and can limit costs that arise from disruptions. Furthermore it can contribute to competitive advantages by continuing operations during disruptions, resilience of the organization and trust of stakeholders in the operations of the organization.

The IT management determines the identified goals from strategic management of the reporting organization regarding IT continuity. As a consequence the reporting requirements in this standard need to be made specific for the organization within the scope of the reporting.

The governance of the topic IT continuity management is addressed in the section 1 “Governance of IT topics” specifying “IT Organization and governance” and “Risk management”. The requirements regarding roles, responsibilities and accountability for IT continuity management are to be defined in this IT topic IT Continuity management as a result of the disclosure “ITCM-1: T Organization and governance”. In the context of this standard the generic aspects for IT organization and governance are described at the level of the “Governance of IT topics”. The reporting organization can decide to describe the topic specific aspects of “IT Organization and governance" in the paragraph about "Governance of IT topics" or can describe this in the IT topic IT Continuity management paragraph.

The IT risk management, as part of the enterprise risk management, covers the specific risks involved with this topic. For IT continuity management the disclosures and requirements have been determined under the assumption that generic IT risk management attributes are addressed in the "2 – IT Risk management". Although the conditions for the risk management for continuity of IT are set by "IT Risk management" and fulfilled, it is important that the monitoring of the IT continuity measures provides risk relevant information to the "IT Risk management" processes as well. This is part of the Topic IT Continuity management.



A separate scope paragraph, in the report from the reporting organization, should describe how the scope of IT continuity is included in this report on the governance of IT. It is recommended to report on the business continuity of the reporting organization rather than limit it to the IT responsibilities.

Furthermore it is, given the implicit attribute of non-availability of IT to have potential impact for business processes and humans, necessary to identify the scope from a demand and supply chain perspective as well.

If requirements are not addressed in the report it is required to specify this in the GRI content index (if GRI is used), and provide a reason for omission with an explanation according to GRI-3 "Using this Standard". The scope paragraph should include clarification that the report on the governance of IT covers the past year and the current year.

For IT continuity management the following aspects are important to address relevant controls and their interrelationship to build, operate and maintain a resilient IT continuity management system:

- Protect for disruptions;
- Detection of potential threats;
- Respond to an incident;
- Recover from unavailability.

IT continuity management – disclosures on the governance of the topic

An organization reporting in accordance with this IDRS is required to report how it manages each of its material IT topics. An organization that has determined IT continuity practices to be a material IT topic in the use and governance of IT is required to report how it manages the topic using Appendix A (see requirement GOV-ITCM 1.1 in this section).

This section is therefore designed to **supplement** – and not replace – the disclosures determined using Appendix A and section 1: Governance of IT topics.

Requirements	
IT Continuity management	
GOV-ITCM 1.1	**The reporting organization shall report how it manages IT continuity using Appendix A and the context and scope of the IT continuity management in addition to 'Governance of IT topics' 1.1.**
GOV-ITCM 1.2	**The reporting organization shall report how it manages risks related to intention and unintentional disruptions of the IT and depending business processes in addition to Governance of IT topics 1.2.**

Guidance	
IT Continuity management	
GOV-ITCM-1.1a	The reporting organization should include the internal and external context of IT continuity management and could consider: • stake holding parties and their relevant requirements; • legal and regulatory requirements; • mission, goals and internal and external obligations; • the parts of the organization that are included in the IT continuity management; • the dependency on the IT continuity of other entities; • products and/or services that are included; • the intended readers of the report; • disclaimer: 100% IT availability cannot be achieved at acceptable cost.
GOV-ITCM-1.1b	The reporting organization should describe the integration of the IT continuity management with enterprise business continuity management (if available) considering: • top management approval; • scope including limitations and exclusions;

	• communication with relevant business partners; • supply chain initiatives to provide continuity in the exchange of data and reliance on each other’s IT; • documented IT continuity policy; • reviewed in conjunction with the enterprise continuity management policy and planning.
GOV-ITCM-1.1c	The reporting organization could describe the IT continuity policy and continuity plan considering: • accountability for the IT continuity management; • current IT continuity posture; • target state of continuity; • resource availability in terms of timely, quality and quantity; • awareness and training; • testing the effectiveness; • potential costs and benefits (affordability); • technological limitations and/or opportunities; • involved business partners in the continuity plan; • identified regulatory obligations.
GOV-ITCM-1.1d	The reporting organization could report the results from analyzing the monitoring information regarding protection safeguards, detecting potential disruption events, responses to occurred incidents and executed recoveries, regarding points of improvement and which of them have been implemented in the reporting period.
GOV-ITCM-1.2a	The reporting organization should report how it addresses risks related to intention and unintentional disruptions of the IT and depending business processes considering: • determined critical IT for which unavailability could have material impact on economy, human and/or environment; • identified threats that can have material impact on environment, human, societal and the IT demand and supply chain; • potential impacts of identified threats for critical IT; • options for protection, resilience, recovery and restoration; • monitoring the risk for disruption; • maintaining sufficient IT continuity skills and knowledge;
GOV-ITCM-1.2b	The reporting organization could describe the goals and the changes in IT continuity risks, and/or IT continuity management, compared to the former reporting period considering: • identification of new critical IT;

	• new identified threats; • the organization's risk appetite; • identified RTO's and RPO's for critical IT services; • technical requirements (back-up, locations, sites, power, telecom, encryption, outsourced etc.).
GOV-ITCM-1.2c	The reporting organization could also report about: • the interaction with the public authorities regarding occurred cybersecurity events and the follow-up by the reporting organization;

IT continuity management – topic disclosures

An organization is expected to compile information regarding the management of availability risks and figures regarding the occurrence of disruptions and the impact for the reporting organization and its supply chain.

Disclosures IT continuity management	
ITCM-1	**Developed and implemented appropriate safeguards to ensure disruptions are prevented.**
ITCM-2	**Disruptions are detected at the earliest stage to minimize the impact to IT services, reduce the recovery effort and maintain the quality of service.**
ITCM-3	**Appropriate response to disruptions to minimize downtime and allow effective and efficient recovery.**
ITCM-4	**Maintained and tested recovery strategy and process to ensure timely availability of services and to maintain the integrity of data.**

Requirements	
Topic IT continuity management	
ITCM-1-1	**The reporting organization shall report the implementation, status and activities regarding appropriate safeguards to ensure that disruptions are prevented or undesired effects are reduced.**
ITCM-2-1	**The reporting organization shall report the efforts regarding detection of (potential) disruptions.**

ITCM-3-1	**The reporting organization shall report the efforts for responding to (potential) disruptions.**
ITCM-4-1	**The reporting organization shall report the recovery from disruptions with impact on:** - **business partners;** - **economy;** - **environment and/or;** - **people, including impacts on their human rights.**

Guidance	
Topic IT Continuity management	
ITCM-1.1a	The reporting organization should describe its activities regarding the implementation of controls that provide protection safeguards for IT continuity: - back-up arrangements including use of external location(s) and storage off-site and testing the effectiveness; - access control including remote access and access by business partners and other external persons; - availability of sufficient expertise and competencies; - awareness and training specific for user groups defined by role and impact for availability including business partners; - specific resilience control measures in the change management process; - coordination with business partners. And could report on how it handles IT continuity in relation to: - data protection at-rest against unauthorized access and/or leakage during disruptions; - maintenance of the digital infrastructure; - technological solutions; - competency management.
ITCM-1.1b	The reporting organization could describe the results of the monitoring of the controls that provide protection safeguards and improvements that have been implemented to make these controls more effective.
ITCM-1.1c	The reporting organization may describe occurrences of controls providing protection safeguards being effective in preventing incidents and/or disruptions caused by deviation in the executing of the preventive controls.

ITCM-1.1d	The reporting organization could report on the communication regarding the setup and objective of controls within the organization and with the business partners. Including the sharing of detection information in the supply chain.
ITCM-1.1e	The reporting organization should provide information regarding, if any, performed ongoing and/or separate evaluations (by internal audit or external audit) of the effectiveness of controls that have the objective to provide protection safeguards.
ITCM-2. 1a	The reporting organization should report on the detection controls. The organization could report on: • the required and available skills and competencies; • the involvement of the supply chain; • the identification and logging of anomalies and events that could cause (potential) disruptions. The organization may report on: • the (detected) changes in critical business applications, data and databases; • changes in supporting detection technology, equipment and networks; • enabling technologies and/or equipment; • redundancy applied in the IT to ensure continuity of IT services; • the documentation of potential disruptive events; • the communication and sharing of detective information in the supply chain.
ITCM-2.1b	The reporting organization could describe the results of the monitoring of detection controls. The reporting organization may report on: • the monitoring of the quality of detection data; • the changes in critical supporting IT systems identified by detection controls; • the follow-up on information from internal and external data sources describing events with potential effect on availability; • the analysis of the result of detection and subsequent improvements made to increase effectiveness of the detection; • the assessment of the identified events with potential effect on availability.
ITCM-2.1c	The reporting organization may report occurrences of detected incidents that could have caused disruptions with impact for critical assets and business processes considering the impact on: • business partners;

	• economy; • environment; • people, including impacts on their human rights.
ITCM-2.1d	The reporting organization could report how it communicates on the setup and objective of detection controls within the organization and with business partners.
ITCM-2.1e	The reporting organization could provide information regarding, if any, performed ongoing and/or separate evaluations (by internal audit or external audit) of the effectiveness of detection controls and the follow-up to findings addressing nonconformities, their causes and the verification of the actions taken on these findings.
ITCM-3.1a	The reporting organization should describe activities regarding the controls to respond to an IT service disruption or detection of one or a series of related events that became incidents. The reporting organization could report on: • the incident response plan; • identified strategies for response; • testing the incident response plan. And may report on: • the identification of severity and IT roles involved, including priority setting and timescales for availability; • the impact on: ○ business partners; ○ economy; ○ environment and; ○ people, including impacts on their human rights; • the implications from legal and compliance perspective; • access by third parties to render support during the response; • coordination with business partners.
ITCM-3.1b	The reporting organization could describe the results of the monitoring of the incident response process and controls considering: • documentation of incidents; • classification of the incidents; • applied strategies; • speed of reaction compared to the risk involved; • effectiveness of the incident response;

	• communication between involved employees and other workers, accountable management and (where applicable) business partners and other external organizations; • preparation for recovery.
ITCM-3.1c	The reporting organization may describe executed response plans and to what extent the responses effectively limited the impact of incidents and/or disruptions considering: • the identification of the incident; • severity identification including potential impact and identified response; • the response(s) made immediately, in real-time or in near real-time and whether investigation was involved; • follow-up on the response regarding the identified effect of the incident for the availability of IT and need for recovery; • review of the response and identification of lessons learned, cause analysis and (where needed) adjustment to the existing controls; • informing all parties (employees, workers, business partners, suppliers) involved and (potentially) affected.
ITCM-3.1d	The reporting organization could report on the communication regarding the setup and objective of the response process within the organization as well as with business partners. This can include sharing of incident and response information in the supply chain.
ITCM-3.1e	The reporting organization could provide information, if any, regarding performed ongoing and/or separate evaluations (by internal audit or external audit) of the effectiveness of incident response plans and processes.
ITCM-4.1a	The reporting organization should report on the process for recovery from IT service disruption(s). The reporting organization could report on: • its recovery plan; • identified renewal strategies; • involvement of resilience partners; • timelines for recovery; • and communication with involved management and business partners. And may report on: • availability of integer data in time and other information security requirements; • identifying the impact on business processes;

	• analysis and planning of activities to recover, their dependencies and the availability of necessary resources; • the restore process.
ITCM-4.1b	The reporting organization may report recovery activities due to IT incidents with disruptive impact considering: • the impact of the incident and outcome of the response, within the organization, on its clients and within the demand and supply chain; • involved organizations executing the recovery plans; • impact on people, economy and environment; • impact on the organization and its business partners; • determined effectiveness of the recovery plan; • communication within the supply chain.
ITCM-4.1c	The reporting organization could report about the communication regarding the setup and objective of the recovery process within the organization and with the involved organizations, business partners, regulatory authorities and other stakeholders. The reporting organization may consider reporting about: • impact on people, economy and environment; • support from the reporting organization to affected victims. survivors and displaced residents; • how the business functions of responding organizations involved in the recovery activities were supported; • benefits for vulnerable groups / communities.
ITCM-4.1d	The reporting organization could provide information regarding, if any, performed ongoing and/or separate evaluations (by internal audit or external audit) of the effectiveness of recovery process and independent determination of the impact of incidents that caused disruption of the IT and had impact on critical business processes.

Topic IDRS 6 – Privacy

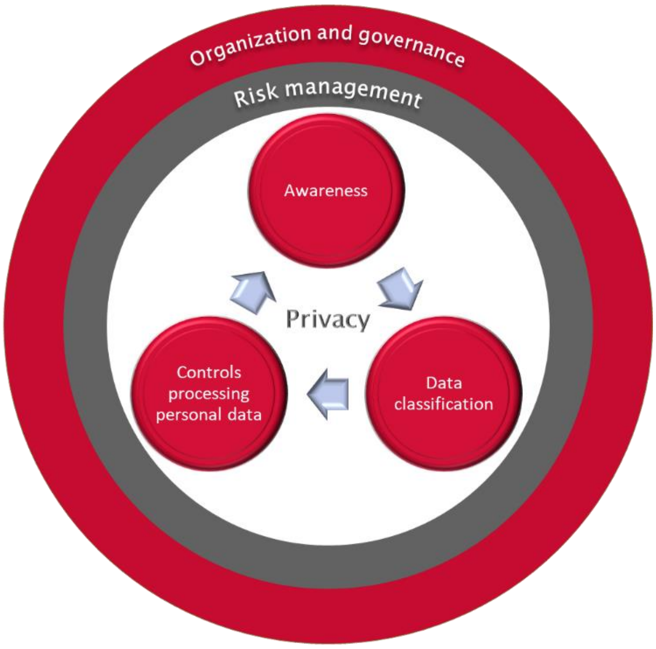
Scope

Extensive and innovative uses of personal data bring greater economic and social benefits, but also increase privacy risks. The objective of Privacy is to protect the use of personal data processed by the organization, in line with its business goals, strategy and risk appetite and applicable to all employees and stakeholders who are impacted or could be impacted by the personal data processed by the organization.

Rapid technological developments and globalization have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data between countries and international organizations, while ensuring a high level of the protection of personal data and respecting the human rights of all natural persons involved.

For privacy the following aspects and their interrelationships are important to address to build, operate and maintain a resilient privacy management system:

- Create and maintain awareness in the organization;
- Classify data to identify personal data;
- Apply appropriate controls for processing of personal data.


Organization and governance
Risk management
Awareness
Privacy
Controls processing personal data
Data classification

The governance of this topic is addressed in the section 1 “Governance of IT topics” of this standard, specifying “IT Organization and governance” and “Risk management”. The roles, responsibilities and accountability for privacy are to be defined in “IT Organization and governance”. The IT risk management as part of the enterprise risk management covers the specific risks involved with this topic. The privacy disclosures and requirements have been determined under the assumption that generic IT risk management attributes are addressed in the “IT Risk management”. Although the conditions for the risk management for privacy are set by “IT Risk management” and fulfilled, it is also important that the monitoring of the privacy provides risk relevant information to the "IT Risk management" processes as well. This is part of the topic description of privacy.

A separate scope paragraph, should describe how the scope of privacy is included in this report on the governance of IT. It is recommended to report on the privacy aspects of the reporting organization as a whole rather than limit it to the IT responsibilities. The scope paragraph should include clarification that the report on the governance of IT covers the past year and the current year.

Privacy – disclosures on the governance of the topic

An organization reporting in accordance with this IDRS is required to report how it manages each of its material IT topics. An organization that has determined privacy to be a material IT topic in the domain of the use and the governance of IT is required to report how it manages the topic using Appendix A and disclosure GOV-PVCY-1.1 in this standard).

This section is therefore designed to **supplement** – and not replace – the requirements in Appendix A and section 1: Governance of IT topics.

Requirements	
Privacy	
GOV-PVCY-1.1	**The reporting organization shall report how it manages the integration of privacy governance in the organization.**
GOV-PVCY -1.2	**The reporting organization shall report how it addresses risks related to privacy and depending business processes.**

Guidance	
Privacy	
GOV-PVCY -1.1a	The organization should describe how the scope of privacy applies to the (types of) personal data the organization collects, processes and maintains, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties of data subjects.
GOV-PVCY -1.1b	The organization should describe how: • business strategic goals are realized by use of personal data; • the organization uses a privacy by design framework; • the organization has performed a data protection impact assessment (e.g. risk and impact of the use of personal data on the

	rights and freedoms of data subjects, based on a stakeholder analysis); • the organization has defined objectives regarding privacy in relation to the identified stakeholders; • the implementation of the personal data policies and procedures is supported by appropriate investments in human and technical resources; • the organization has established a structure for conflict resolution regarding the use of personal data, which ties back into possibly improving existing policies and procedures; • the organization has established documented policies and procedures to prevent, mitigate and respond to unauthorized or accidental access to someone's personal information; • the organization has established documented policies and procedures to disclose personal data breaches that occurred during the reporting period, e.g. based on their severity.
GOV-PVCY -1.1c	The organization should describe how: • the roles and responsibilities are organized throughout the personal data lifecycle; understanding, preparation, modelling, evaluation, deployment, maintain, run and remove; • the single Senior Responsible Owner (SRO) has approved the use of personal data before collection and processing; • the organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control to prevent privacy compromises; • duties are segregated to prevent fraud, sabotage, theft, misuse of personal data and other compromises; • third party assurance of data processors is managed.
GOV-PVCY -1.1d	The organization should describe how: • the organization obtains or generates and uses relevant, quality information to support the functioning of internal control over privacy protection; • the organization has established a mechanism allowing others to flag issues related to privacy protection; • protection against data leaks is implemented, properly managed and continuously monitored; • data leaks are reported to the appropriate Data Protection Authority in the respective country;

	- it discloses the number of material cyber-related data leaks that occurred during the reporting period and are required to be disclosed.
GOV-PVCY -1.2a	The organization should describe how: - it assesses risk on loss of or unauthorised access to personal data as a result of a failure of the organisation, destruction, use modification or disclosure of personal data; - it assesses risk on theft, unauthorised copying or the like; - it assesses risk on intrusion from outside sources; - the organization incorporates Privacy Impact Assessments and Data Protection Impact Assessments into the organisation's risk management and how it uses this to promote accountability.

Privacy – topic disclosures

An organization is expected to compile information regarding the governance of Privacy and provide figures regarding the occurrence of personal data breach events and the impact for the reporting organization and its stakeholders.

Disclosures Privacy	
PVCY-1	**Employees are aware of the safe use and protection of personal data.**
PVCY-2	**Processing of personal data is controlled in work and labor processes.**
PVCY-3	**Personal data is classified based on confidentiality, authenticity, integrity, availability and legal/regulatory requirements (including GDPR).**

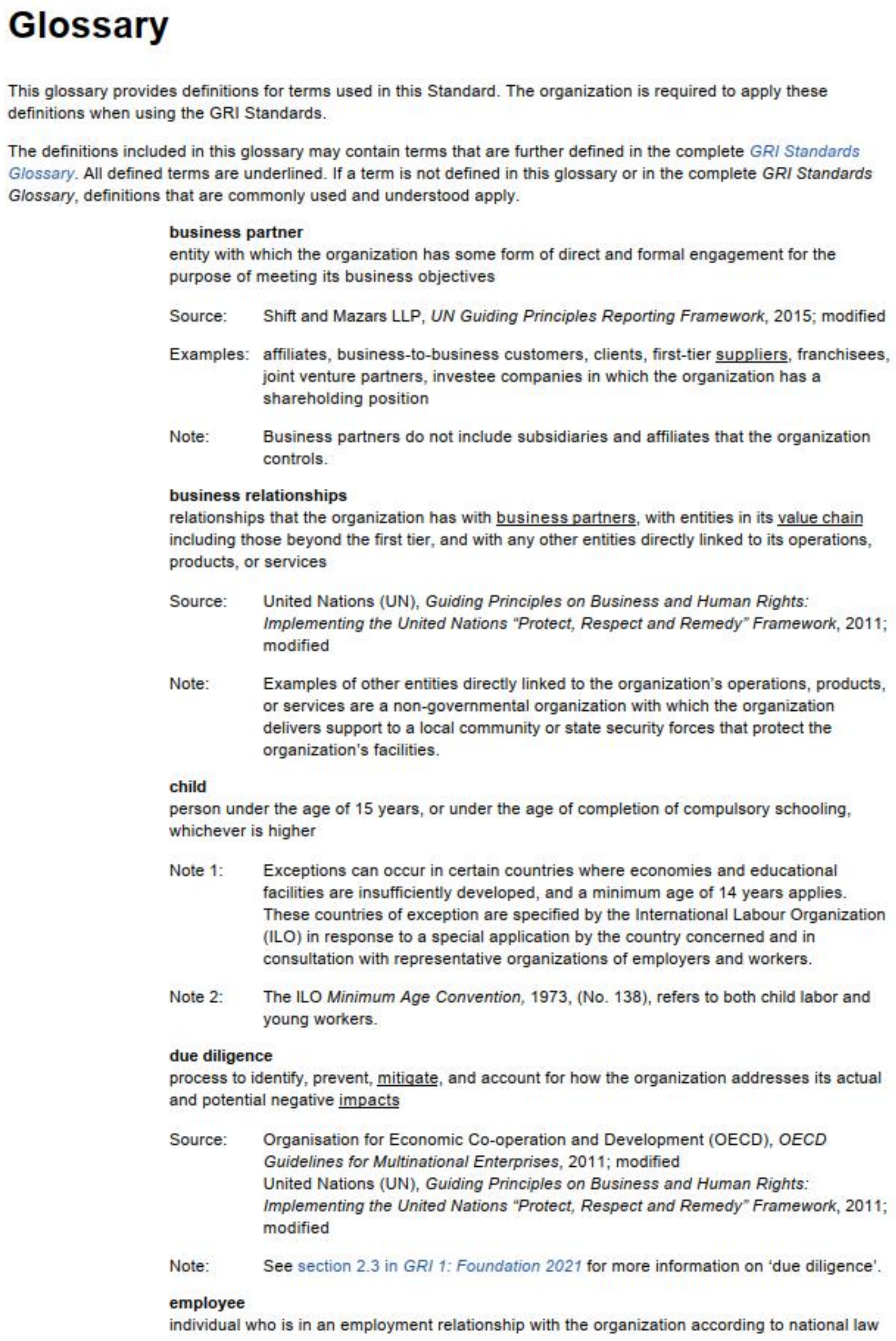
Requirements	
Topic Privacy	
PVCY-1.1	**The organization shall report on activities to promote awareness on privacy.**
PVCY-2.1	**The organization shall report on privacy controls in work and labor processes.**
PVCY-3.1	**The organization shall report on classification of personal data.**

Guidance	
Topic Privacy	
PVCY-1.1a	The organization should describe: • the privacy awareness and information activities it has in place to inform all employees and other workers in the organization; • how newcomers receive mandatory training on privacy; • any specific trainings senior executives and members of governing bodies receive on privacy; • if the intranet site has a dedicated section on privacy topics, guidelines and best practices, including a (whistle blower) hotline to report any issues.
PVCY-1.1b	The organization could describe the way awareness efforts include explaining the safe use and protection of the organization's personal data, IT systems and the privacy risks they should be aware of, including OECD privacy principles, GDPR non-compliance, fundamental human rights, possible internal or external violations and their role in mitigating and remediating privacy breaches;
PVCY-2.1a	The organization should describe: • what limits it applies to the collection of personal data and if any such data is obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject; • how it establishes that personal data is relevant to the purposes for which it is to be used, and, to the extent necessary for those purposes, is accurate, complete and kept up-to-date; • how personal data is protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data; • the role of the data controller, who is accountable for complying with measures which give effect to the principles stated above; • how the collection of personal information is limited to what is directly relevant and necessary to accomplish a specified purpose.
PVCY-2.1b	The organization should describe: • whether the purposes for which personal data are collected and processed is specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose;

	• personal data is not disclosed, made available or otherwise used for purposes other than those specified in accordance with the above measure, except when one of the following conditions applies: ○ consent of the data subject has been obtained; or ○ by the authority of law; • there is a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
PVCY-2.1c	The organization could describe whether individuals have the right: • to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; • to have communicated to them, data relating to them within a reasonable time; • at a charge, if any, that is not excessive; • in a reasonable manner; and • in a form that is readily intelligible to them; • to be given reasons if a request is denied, and to be able to challenge such denial; and • to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.
PVCY-3.1a	The organization should describe how: • the organization maintains documented, approved and enforced data classification policies and procedures, describing how to classify personal information based on confidentiality and legal/ regulatory requirements; • ownership of the personal information (categories) is determined, to properly conduct the data classification.
PVCY-3.1b	When reporting on data classification policies and procedures the organization should describe what control measures are applied based on the classified criticality/sensitivity of the information.
PVCY-3.1c	The reporting organization could provide information regarding, if any, performed ongoing and/or separate evaluations (by internal audit or external audit) of the effectiveness of privacy related controls and the follow-up to findings addressing nonconformities, their causes and the verification of the actions taken on these findings.

Glossary of GRI terms

This chapter includes the Glossary of terms as per GRI 1 – Foundation 2021.



Glossary

This glossary provides definitions for terms used in this Standard. The organization is required to apply these definitions when using the GRI Standards.

The definitions included in this glossary may contain terms that are further defined in the complete *GRI Standards Glossary*. All defined terms are underlined. If a term is not defined in this glossary or in the complete *GRI Standards Glossary*, definitions that are commonly used and understood apply.

business partner
entity with which the organization has some form of direct and formal engagement for the purpose of meeting its business objectives

Source: Shift and Mazars LLP, *UN Guiding Principles Reporting Framework*, 2015; modified

Examples: affiliates, business-to-business customers, clients, first-tier suppliers, franchisees, joint venture partners, investee companies in which the organization has a shareholding position

Note: Business partners do not include subsidiaries and affiliates that the organization controls.

business relationships
relationships that the organization has with business partners, with entities in its value chain including those beyond the first tier, and with any other entities directly linked to its operations, products, or services

Source: United Nations (UN), *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, 2011; modified

Note: Examples of other entities directly linked to the organization's operations, products, or services are a non-governmental organization with which the organization delivers support to a local community or state security forces that protect the organization's facilities.

child
person under the age of 15 years, or under the age of completion of compulsory schooling, whichever is higher

Note 1: Exceptions can occur in certain countries where economies and educational facilities are insufficiently developed, and a minimum age of 14 years applies. These countries of exception are specified by the International Labour Organization (ILO) in response to a special application by the country concerned and in consultation with representative organizations of employers and workers.

Note 2: The ILO *Minimum Age Convention*, 1973, (No. 138), refers to both child labor and young workers.

due diligence
process to identify, prevent, mitigate, and account for how the organization addresses its actual and potential negative impacts

Source: Organisation for Economic Co-operation and Development (OECD), *OECD Guidelines for Multinational Enterprises*, 2011; modified
United Nations (UN), *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, 2011; modified

Note: See section 2.3 in *GRI 1: Foundation 2021* for more information on 'due diligence'.

employee
individual who is in an employment relationship with the organization according to national law

or practice

governance body
formalized group of individuals responsible for the strategic guidance of the organization, the effective monitoring of management, and the accountability of management to the broader organization and its stakeholders

highest governance body
governance body with the highest authority in the organization

Note: In some jurisdictions, governance systems consist of two tiers, where supervision and management are separated or where local law provides for a supervisory board drawn from non-executives to oversee an executive management board. In such cases, both tiers are included under the definition of highest governance body.

human rights
rights inherent to all human beings, which include, at a minimum, the rights set out in the *United Nations (UN) International Bill of Human Rights* and the principles concerning fundamental rights set out in the *International Labour Organization (ILO) Declaration on Fundamental Principles and Rights at Work*

Source: United Nations (UN), *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, 2011; modified

Note: See Guidance to 2-23-b-i in *GRI 2: General Disclosures 2021* for more information on 'human rights'.

impact
effect the organization has or could have on the economy, environment, and people, including on their human rights, which in turn can indicate its contribution (negative or positive) to sustainable development

Note 1: Impacts can be actual or potential, negative or positive, short-term or long-term, intended or unintended, and reversible or irreversible.

Note 2: See section 2.1 in *GRI 1: Foundation 2021* for more information on 'impact'.

indigenous peoples
indigenous peoples are generally identified as:

- tribal peoples in independent countries whose social, cultural and economic conditions distinguish them from other sections of the national community, and whose status is regulated wholly or partially by their own customs or traditions or by special laws or regulations;
- peoples in independent countries who are regarded as indigenous on account of their descent from the populations which inhabited the country, or a geographical region to which the country belongs, at the time of conquest or colonization or the establishment of present state boundaries and who, irrespective of their legal status, retain some or all of their own social, economic, cultural and political institutions.

Source: International Labour Organization (ILO), *Indigenous and Tribal Peoples Convention*, 1989 (No. 169)

local community
individuals or groups of individuals living or working in areas that are affected or that could be affected by the organization's activities

Note: The local community can range from those living adjacent to the organization's operations to those living at a distance.

material topics
topics that represent the organization's most significant impacts on the economy, environment, and people, including impacts on their human rights

Note: See section 2.2 in *GRI 1: Foundation 2021* and section 1 in *GRI 3: Material Topics 2021* for more information on 'material topics'.

mitigation
action(s) taken to reduce the extent of a negative impact

Source: United Nations (UN), *The Corporate Responsibility to Respect Human Rights: An Interpretive Guide*, 2012; modified

Note: The mitigation of an actual negative impact refers to actions taken to reduce the severity of the negative impact that has occurred, with any residual impact needing remediation. The mitigation of a potential negative impact refers to actions taken to reduce the likelihood of the negative impact occurring.

remedy / remediation
means to counteract or make good a negative impact or provision of remedy

Source: United Nations (UN), *The Corporate Responsibility to Respect Human Rights: An Interpretive Guide*, 2012; modified

Examples: apologies, financial or non-financial compensation, prevention of harm through injunctions or guarantees of non-repetition, punitive sanctions (whether criminal or administrative, such as fines), restitution, restoration, rehabilitation

reporting period
specific time period covered by the reported information

Examples: fiscal year, calendar year

severity (of an impact)
The severity of an actual or potential negative impact is determined by its scale (i.e., how grave the impact is), scope (i.e., how widespread the impact is), and irremediable character (how hard it is to counteract or make good the resulting harm).

Source: Organisation for Economic Co-operation and Development (OECD), *OECD Due Diligence Guidance for Responsible Business Conduct*, 2018; modified
United Nations (UN), *The Corporate Responsibility to Respect Human Rights: An Interpretive Guide*, 2012; modified

Note: See section 1 in *GRI 3: Material Topics 2021* for more information on 'severity'.

stakeholder
individual or group that has an interest that is affected or could be affected by the organization's activities

Source: Organisation for Economic Co-operation and Development (OECD), *OECD Due Diligence Guidance for Responsible Business Conduct*, 2018; modified

Examples: business partners, civil society organizations, consumers, customers, employees and other workers, governments, local communities, non-governmental organizations, shareholders and other investors, suppliers, trade unions, vulnerable groups

Note: See section 2.4 in *GRI 1: Foundation 2021* for more information on 'stakeholder'.

supplier
entity upstream from the organization (i.e., in the organization's supply chain), which provides a product or service that is used in the development of the organization's own products or services

Examples brokers, consultants, contractors, distributors, franchisees, home workers, independent contractors, licensees, manufacturers, primary producers, sub-contractors, wholesalers

Note: A supplier can have a direct business relationship with the organization (often referred to as a first-tier supplier) or an indirect business relationship.

supply chain
range of activities carried out by entities upstream from the organization, which provide products or services that are used in the development of the organization's own products or services

sustainable development / sustainability
development that meets the needs of the present without compromising the ability of future generations to meet their own needs

Source: World Commission on Environment and Development, *Our Common Future*, 1987

Note: The terms 'sustainability' and 'sustainable development' are used interchangeably in the GRI Standards.

value chain
range of activities carried out by the organization, and by entities upstream and downstream from the organization, to bring the organization's products or services from their conception to their end use

Note 1: Entities upstream from the organization (e.g., suppliers) provide products or services that are used in the development of the organization's own products or services. Entities downstream from the organization (e.g., distributors, customers) receive products or services from the organization.

Note 2: The value chain includes the supply chain.

vulnerable group
group of individuals with a specific condition or characteristic (e.g., economic, physical, political, social) that could experience negative impacts as a result of the organization's activities more severely than the general population

Examples: children and youth; elderly persons; ex-combatants; HIV/AIDS-affected households; human rights defenders; indigenous peoples; internally displaced persons; migrant workers and their families; national or ethnic, religious and linguistic minorities; persons who might be discriminated against based on their sexual orientation, gender identity, gender expression, or sex characteristics (e.g., lesbian, gay, bisexual, transgender, intersex); persons with disabilities; refugees or returning refugees; women

Note: Vulnerabilities and impacts can differ by gender.

worker
person that performs work for the organization

Examples: employees, agency workers, apprentices, contractors, home workers, interns, self-employed persons, sub-contractors, volunteers, and persons working for organizations other than the reporting organization, such as for suppliers

Note: In the GRI Standards, in some cases, it is specified whether a particular subset of workers is required to be used.

Bibliography

This section lists authoritative intergovernmental instruments and additional references used in developing this Standard, as well as resources that can be consulted the organization.

IDRS – Governance of IT topics

Authoritative instruments Governance of IT topics:

1. International Organization for Standardization (ISO):
   1.1. *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements;* 2017 [Recently superseded by ISO 27001:2022]
   1.2. *ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management, 2018*
   1.3. *ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection — Governance of information security*, 2020
   1.4. *ISO 31000:2018 Risk management — Guidelines*, 2018
   1.5. *ISO/IEC 38500:2015 Information technology — Governance of IT for the organization*, 2015
   1.6. *ISO/IEC TS 38501:2015 Information technology — Governance of IT — Implementation guide*, 2015
   1.7. *ISO/IEC TR 38502:2017 Information technology — Governance of IT — Framework and model*, 2017
   1.8. *ISO/IEC 38506:2020 Information technology — Governance of IT — Application of ISO/IEC 38500 to the governance of IT enabled investments,* 2020
2. Committee of Sponsoring Organizations of the Treadway Commission (COSO)
   2.1. COSO Enterprise Risk Management (ERM) Framework, 2017
3. National Institute of Standards and Technology (NIST)
   3.1. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, 2018
   3.2. *NISTIR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM*), 2020
   3.3. *NIST Special Publication 800-37 rev. 2: Risk Management Framework for Information Systems and Organizations*, 2018
4. Global Sustainability Standards Board (GSSB),
   4.1. GRI 1: Foundation 2021
   4.2. GRI 2: General Disclosures 2021ISO 42001_2023 *ISO/IEC 20000*
   4.3. GRI 3: Material Topics 2021
5. CobiT 2019
6. *IT servicemanagement*

Resources Governance of IT topics:

1. Committee of Sponsoring Organizations of the Treadway Commission (COSO)
   1.1. *Managing Cyber Risk in a Digital Age,* 2019
   1.2. *Enhancing Board Oversight,* 2012
   1.3. *Developing key risk indicators to strengthen enterprise risk management,* 2010
2. International Organization for Standardization (ISO):
   2.1. *ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management, all parts 2016 -2020*

IDRS-1 Digital Innovation and Transformation

Innovation

- ISO 56002, Innovation management — Innovation management system — Guidance

Architecture

- The Open Group Architecture Framework (TOGAF), version 9
- ISO 42010:2011, Systems and software engineering – Architecture Description

Transformation

- ISO 21500:2021, Project, programme and portfolio management — Context and concepts
- ISO 21502:2020, Project, programme and portfolio management — Guidance on project management
- ISO 21503:2017, Project, programme and portfolio management — Guidance on programme management
- ISO 21504:2022, Project, programme and portfolio management — Guidance on portfolio management

IDRS-2 Data & Artificial Intelligence

Data & AI

- ISO 38505 1 and 2, Governance of data
- NOREA Guiding Principles Trustworthy AI investigations Guiding principles for investigations of enterprise artificially intelligent AI systems (concept)
- ISO IEC TR 24368_2022 AI. Overview of ethical and societal concerns
- ISO IEC 38507_2022 Governance implications of AI
- ISO IEC_23894_2023 AI Guidance on risk

- AI Management system
- OECD AI Principles overview
- Data Management International (DAMA)
- Data Management Body of Knowledge (DMBOK)
- Federal Data Strategy (USA) Data Ethics Framework
- General Data Protection Regulation (EU) 2016/679
- Digital rights and principles (EU) January 2022
- AI Act 2024

Data management

- ISO-8000 Data Quality, Exchange of complex data
- ISO-25010 Product Quality, Data Quality Usability (Replaces ISO-9126)
- ISO-25012 Data Quality (Computer Aided)
- ISO27001/ISO27002/ISO31000 - Data Security

IDRS-3 Third party management

- ISO 37500:2014 - Guidance on outsourcing
- EBA Guidelines on outsourcing arrangements, EBA/GL/2019/02
- Bill Hefley, Ethel A. Loesche, eSourcing Capability Model for Client Organizations (eSCM-CL), 2009
- Good practices for managing outsourcing risks (dnb.nl)

IDRS-4 Cybersecurity

Authoritative instruments Cybersecurity:

1. International Organization for Standardization (ISO):
    1.1. *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements, 2019*
    1.2. *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements;* 2017 [Recently superseded by ISO 27001:2022]
    1.3. *ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls*, 2013 [Recently superseded by ISO 27001:2022]

1.4. *ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management, 2018*

1.5. *ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection — Governance of information security*, 2020

1.6. *ISO 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity,* 2011

1.7. *ISO/IEC TS 27100:2020 Information technology — Cybersecurity — Overview and concepts,* 2020

1.8. *ISO/IEC TS 27110:2021 Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines*, 2021

1.9. *ISO/IEC 29146:2016 Information technology — Security techniques — A framework for access management,* 2016

1.10. *ISO/IEC 29115:2013 Information technology — Security techniques — Entity authentication assurance framework,* 2013

2. National Institute of Standards and Technology (NIST)

2.1. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, 2018

2.2. *NISTIR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM*), 2020

2.3. *NIST Special Publication 800-37 rev. 2: Risk Management Framework for Information Systems and Organizations*, 2018

3. Center for Internet Security (CIS.),

3.1. *CIS Critical Security Controls (CIS Controls) V8*, 2021

3.2. *Establishing Essential Cyber Hygiene*, 2022

4. Nationaal Cyber Security Centrum (NCSC)

4.1. *Aandachtspunten crisismanagement en crisiscommunicatie bij digitale incidenten*, 2022

Additional references Cybersecurity:

1. International Organization for Standardization (ISO):

1.1. *ISO/IEC 27019:2017 Information technology — Security techniques — Information security controls for the energy utility industry, 2017*

1.2. *ISO/IEC TR 27103:2018 Information technology — Security techniques — Cybersecurity and ISO and IEC Standards, 2018*

1.3. *ISO/IEC 27033-1:2015 Information technology — Security techniques — Network security, 2015*

1.4. *ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management, all parts 2016 -2020*

1.5. *ISO/IEC 27036-1:2021 Cybersecurity — Supplier relationships, 2021*

1.6. *ISO/IEC 27040:2015 Information technology — Security techniques — Storage security, 2015*

2. National Institute of Standards and Technology (NIST)

2.1. *NIST Special Publication (SP) 800-40 Revision 4, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*, 2022
2.2. *NIST SP 1800-31, Improving Enterprise Patching for General IT Systems: Utilizing Existing Tools and Performing Processes in Better Ways*, 2022
2.3. *NIST Special Publication SP 800-161r1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations,* 2022

Resources Cybersecurity:

1. European Union Agency for Cybersecurity (ENISA)
   1.1. *ECSF EUROPEAN CYBERSECURITY SKILLS FRAMEWORK, 2022*
   1.2. *Risk management standards,* 2022
   1.3. *Raising awareness of cybersecurity,* 2021
   1.4. *ENISA Report - Cybersecurity for SMES Challenges and Recommendations,* 2021
   1.5. *ENISA Cybersecurity guide for SMEs,* 2021
   1.6. *ENISA Report - How to setup CSIRT and SOC,* 2020
2. National Institute of Standards and Technology (NIST)
   2.1. *NIST Special Publication 800-181 Rev 1 Workforce Framework for Cybersecurity (NICE Framework), 2020*
   2.2. *NIST Special Publication NIST SP 800-82r3 ipd Guide to Operational Technology (OT) Security, 2022 [public draft]*
3. Information Systems Audit and Control Association (ISACA)
   3.1. *The Cyberresilient Enterprise: What the Board of Directors Needs to Ask*, 2015
   3.2. *Auditing cyber security: evaluating risk and auditing controls*, 2017
   3.3. *Optimizing risk response*, 2021
   3.4. *Reporting cybersecurity risk to the Board of Directors,* 2020
4. Nationaal Cyber Security Centrum (NCSC)
   4.1. *Aandachtspunten crisismanagement en crisiscommunicatie bij digitale incidenten*, 2022
   4.2. *Handreiking cybersecuritymaatregelen,* 2021
5. Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Managing Cyber Risk in a Digital Age,* 2019

IDRS-5 IT Continuity Management

Authoritative instruments IT continuity management:

1. International Organization for Standardization (ISO):
   1.1. *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements, 2019*

   1.2. *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements;* 2017 [Recently superseded by ISO 27001:2022]
   1.3. *ISO 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity,* 2011
   1.4. *ISO/IEC 29146:2016 Information technology — Security techniques — A framework for access management,* 2016
   1.5. *ISO/IEC 29115:2013 Information technology — Security techniques — Entity authentication assurance framework,* 2013
2. National Institute of Standards and Technology (NIST)
   2.1. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, 2018
   2.2. *NIST Special Publication 800-37 rev. 2: Risk Management Framework for Information Systems and Organizations*, 2018
3. Center for Internet Security (CIS.),
   3.1. *CIS Critical Security Controls (CIS Controls) V8*, 2021
   3.2. *Establishing Essential Cyber Hygiene*, 2022

Additional references IT Continuity management:

1. International Organization for Standardization (ISO):
   1.1. *ISO/IEC 27033-1:2015 Information technology — Security techniques — Network security, 2015*
   1.2. *ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management,* all parts 2016 -2020
   1.3. *ISO 22313:2020 Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301,* 2020
2. National Institute of Standards and Technology (NIST),
   2.1. *NIST Interagency Report NIST IR 8286D Using Business Impact Analysis to Inform Risk Prioritization and Response*, 2022
   2.2. *NIST Special Publication 800-34 Rev.1 Contingency Planning Guide Federal Information Systems,* 2010

IDRS-6 Privacy

- The OECD Privacy framework 2013
- NOREA Privacy Control Framework 2019
- ISO 29001_2011 Privacy framework
- ISO 27701_2019 Privacy information management
- NOREA Guiding Principles Trustworthy AI investigations Guiding principles for investigations of enterprise artificially intelligent algorithmic systems (concept)

- General Data Protection Regulation (EU) 2016/679
- Digital rights and principles (EU) January 2022
- GDPR–CARPA–Criteria–for–certification–v10

Appendix A: Requirements for determining disclosures on material IT topics

This appendix contains the list of requirements that GRI Disclosure 3-3[6] prescribes in order to determine the disclosures per material topic. When using this IDRS, which has been set up in analogy with the GRI reporting framework, organizations are required to determine their disclosures for reporting on their material topics based on their specific situation, using this list of requirements and taking this IDRS into account.

For each material topic reported under Disclosure 3-2, the organization shall:

a. describe the actual and potential, negative and positive impacts on the economy, environment, and people, including impacts on their human rights;

b. report whether the organization is involved with the negative impacts through its activities or as a result of its business relationships, and describe the activities or business relationships;

c. describe its policies or commitments regarding the material topic;

d. describe actions taken to manage the topic and related impacts, including:

   i. actions to prevent or mitigate potential negative impacts;
   ii. actions to address actual negative impacts, including actions to provide for or cooperate in their remediation;
   iii. actions to manage actual and potential positive impacts;

e. report the following information about tracking the effectiveness of the actions taken:

   i. processes used to track the effectiveness of the actions;
   ii. goals, targets, and indicators used to evaluate progress;
   iii. the effectiveness of the actions, including progress toward the goals and targets;
   iv. lessons learned and how these have been incorporated into the organization's operational policies and procedures;

f. describe how engagement with stakeholders has informed the actions taken (3-3-d) and how it has informed whether the actions have been effective (3-3-e).

[6] Courtesy of GRI, see Disclosure 3-3 in GRI 3: Material Topics 2021 for details and guidance.