SASB STANDARDS

Now part of IFRS Foundation

Software & IT Services

Sustainability Accounting Standard

TECHNOLOGY & COMMUNICATIONS SECTOR

Sustainable Industry Classification System® (SICS®) TC-SI

Under Stewardship of the International Sustainability Standards Board

INDUSTRY STANDARD | VERSION 2023-12

IFRS Sustainability

sasb.org

ABOUT THE SASB STANDARDS

As of August 2022, the International Sustainability Standards Board (ISSB) of the IFRS Foundation assumed responsibility for the SASB Standards. The ISSB has committed to maintain, enhance and evolve the SASB Standards and encourages preparers and investors to continue to use the SASB Standards.

IFRS S1 *General Requirements for Disclosure of Sustainability-related Financial Information* (IFRS S1) requires entities to refer to and consider the applicability of disclosure topics in the SASB Standards when identifying sustainability-related risks and opportunities that could reasonably be expected to affect an entity's prospects. Similarly, IFRS S1 requires entities to refer to and consider the applicability of metrics in the SASB Standards when determining what information to disclose regarding sustainability-related risks and opportunities.

In June 2023, the ISSB amended climate-related topics and metrics in the SASB Standards to align them with the industry-based guidance accompanying IFRS S2 *Climate-related Disclosures*. In December 2023, the ISSB amended the non-climate-related topics and metrics in connection with the International Applicability of SASB Standards project.

Effective Date

This version 2023-12 of the Standard is effective for all entities for annual periods beginning or after January 1, 2025. Early adoption is permitted for all entities.

Table of Contents

INTRODUCTION

Overview of SASB Standards

The SASB Standards are a set of 77 industry-specific sustainability accounting standards ("SASB Standards" or "Industry Standards"), categorised pursuant to the Sustainable Industry Classification System® (SICS®).

SASB Standards include:

1. **Industry descriptions** – which are intended to help entities identify applicable industry guidance by describing the business models, associated activities and other common features that characterise participation in the industry.

2. **Disclosure topics** – which describe specific sustainability-related risks or opportunities associated with the activities conducted by entities within a particular industry.

3. **Metrics** – which accompany disclosure topics and are designed to, either individually or as part of a set, provide useful information regarding an entity's performance for a specific disclosure topic.

4. **Technical protocols** – which provide guidance on definitions, scope, implementation and presentation of associated metrics.

5. **Activity metrics** – which quantify the scale of specific activities or operations by an entity and are intended for use in conjunction with the metrics referred to in point 3 to normalise data and facilitate comparison.

Entities using the SASB Standards as part of their implementation of ISSB Standards should consider the relevant ISSB application guidance.

For entities using the SASB Standards independently from ISSB Standards, the *SASB Standards Application Guidance* establishes guidance applicable to the use of all Industry Standards and is considered part of the Standards. Unless otherwise specified in the technical protocols contained in the Industry Standards, the guidance in the SASB Standards Application Guidance applies to the definitions, scope, implementation, compilation and presentation of the metrics in the Industry Standards.

Historically, the *SASB Conceptual Framework* set out the basic concepts, principles, definitions and objectives that guided the SASB Standards Board in its approach to setting standards for sustainability accounting.

Use of the Standards

SASB Standards are intended to aid entities in disclosing information about sustainability-related risks and opportunities that could reasonably be expected to affect the entity's cash flows, its access to finance or cost of capital over the short, medium or long term. An entity determines which Industry Standard(s) and which disclosure topics are relevant to its business, and which associated metrics to report. In general, an entity should use the SASB Standard specific to its primary industry as identified in SICS® . However, companies with substantial business in multiple SICS® industries should refer to and consider the applicability of the disclosure topics and associated metrics in additional SASB Standards.

The disclosure topics and associated metrics contained in this Standard have been identified as those that are likely to be useful to investors. However, the responsibility for making materiality judgements and determinations rests with the reporting entity.

Industry Description

The Software & Information Technology (IT) Services industry offers products and services globally to retail, business and government customers, and includes entities that develop and sell applications software, infrastructure software and middleware. The industry generally is competitive but with dominant players in some segments. Although relatively immature, the industry is characterised by high-growth entities that place a heavy emphasis on innovation and depend on human and intellectual capital. The industry also includes IT services entities delivering specialised IT functions, such as consulting and outsourced services. New industry business models include cloud computing, software as a service, virtualisation, machine-to-machine communication, big data analysis and machine learning. Additionally, brand value is important for entities in the industry to scale and achieve network effects, whereby wide adoption of a particular software product may result in self-perpetuating growth in sales.

SUSTAINABILITY DISCLOSURE TOPICS & METRICS

Table 1. Sustainability Disclosure Topics & Metrics

TOPIC	METRIC	CATEGORY	UNIT OF MEASURE	CODE
Environmental Footprint of Hardware Infrastructure	(1) Total energy consumed, (2) percentage grid electricity and (3) percentage renewable	Quantitative	Gigajoules (GJ), Percentage (%)	TC-SI-130a.1
	(1) Total water withdrawn, (2) total water consumed; percentage of each in regions with High or Extremely High Baseline Water Stress	Quantitative	Thousand cubic metres (m^3), Percentage (%)	TC-SI-130a.2
	Discussion of the integration of environmental considerations into strategic planning for data centre needs	Discussion and Analysis	n/a	TC-SI-130a.3
Data Privacy & Freedom of Expression	Description of policies and practices relating to targeted advertising and user privacy	Discussion and Analysis	n/a	TC-SI-220a.1
	Number of users whose information is used for secondary purposes	Quantitative	Number	TC-SI-220a.2
	Total amount of monetary losses as a result of legal proceedings associated with user privacy [1]	Quantitative	Presentation currency	TC-SI-220a.3
	(1) Number of law enforcement requests for user information, (2) number of users whose information was requested, (3) percentage resulting in disclosure	Quantitative	Number, Percentage (%)	TC-SI-220a.4
	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring [2]	Discussion and Analysis	n/a	TC-SI-220a.5
Data Security	(1) Number of data breaches, (2) percentage that are personal data breaches, (3) number of users affected [3]	Quantitative	Number, Percentage (%)	TC-SI-230a.1
	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	Discussion and Analysis	n/a	TC-SI-230a.2

continued...

[1] Note to **TC-SI-220a.3** – The entity shall briefly describe the nature, context and any corrective actions taken because of monetary losses.

[2] Note to **TC-SI-220a.5** – The disclosure shall include a description of the extent of the effect in each case and, where relevant, a discussion of the entity's policies and practices related to freedom of expression.

[3] Note to **TC-SI-230a.1** – The disclosure shall include a description of corrective actions implemented in response to data breaches.

...continued

TOPIC	METRIC	CATEGORY	UNIT OF MEASURE	CODE
Recruiting & Managing a Global, Diverse & Skilled Workforce	Percentage of employees that require a work visa [4]	Quantitative	Percentage (%)	TC-SI-330a.1
	Employee engagement as a percentage [5]	Quantitative	Percentage (%)	TC-SI-330a.2
	Percentage of (1) gender and (2) diversity group representation for (a) executive management, (b) non-executive management, (c) technical employees, and (d) all other employees [6]	Quantitative	Percentage (%)	TC-SI-330a.3
Intellectual Property Protection & Competitive Behaviour	Total amount of monetary losses as a result of legal proceedings associated with anti-competitive behaviour regulations [7]	Quantitative	Presentation currency	TC-SI-520a.1
Managing Systemic Risks from Technology Disruptions	Number of (1) performance issues and (2) service disruptions; (3) total customer downtime [8]	Quantitative	Number, Days	TC-SI-550a.1
	Description of business continuity risks related to disruptions of operations	Discussion and Analysis	n/a	TC-SI-550a.2

Table 2. Activity Metrics

ACTIVITY METRIC	CATEGORY	UNIT OF MEASURE	CODE
(1) Number of licences or subscriptions, (2) percentage cloud-based	Quantitative	Number, Percentage (%)	TC-SI-000.A
(1) Data processing capacity, (2) percentage outsourced[9]	Quantitative	See note	TC-SI-000.B
(1) Amount of data storage, (2) percentage outsourced[10]	Quantitative	Petabytes, Percentage (%)	TC-SI-000.C

[4] Note to **TC-SI-330a.1** – The disclosure shall include a description of any potential risks of recruiting employees that require a work visa, and how the entity manages these risks.

[5] Note to **TC-SI-330a.2** – The disclosure shall include a description of method employed.

[6] Note to **TC-SI-330a.3** – The entity shall describe its policies and programmes for fostering equitable employee representation across its global operations.

[7] Note to **TC-SI-520a.1** – The entity shall briefly describe the nature, context and any corrective actions taken because of monetary losses.

[8] Note to **TC-SI-550a.1** – Disclosure shall include a description of each significant performance issue or service disruption and any corrective actions taken to prevent future disruptions.

[9] Note to **TC-SI-000.B** – Data processing capacity shall be reported in units of measure typically tracked by the entity or used as the basis for contracting software and information technology (IT) services, such as million service units (MSUs), million instructions per second (MIPS), mega floating-point operations per second (MFLOPS), compute cycles or other. Alternatively, the entity may disclose owned and outsourced data processing needs in other units of measure, such as rack space or data centre floor area. The percentage outsourced shall include on-premise cloud services, those that are hosted on public cloud, and those that are residing in co-location data centres.

[10] Note to **TC-SI-000.C** – The percentage outsourced shall include on-premise cloud services, those that are hosted on public cloud, and those that are residing in co-location data centres.

Environmental Footprint of Hardware Infrastructure

Topic Summary

With the growth of cloud-based service offerings, entities in this industry own, operate or rent increasingly more data centres and other hardware. Thus, managing the energy and water use associated with IT hardware infrastructure is relevant to value creation. Data centres must be powered continuously, and disruptions to the energy supply can have a material effect on operations, depending on the magnitude and timing of the disruption. Entities face a trade-off between energy and water consumption because of data centre cooling needs. Cooling data centres with water instead of chillers improves energy efficiency, but this method may create dependence on significant local water resources. Data centre specification decisions are important for managing costs, obtaining a reliable supply of energy and water, and reducing reputational risks, particularly with the increasing global regulatory focus on climate change and the opportunities arising from energy efficiency and renewable energy innovations.

Metrics

TC-SI-130a.1. (1) Total energy consumed, (2) percentage grid electricity and (3) percentage renewable

1 The entity shall disclose (1) the total amount of energy it consumed as an aggregate figure, in gigajoules (GJ).

1.1 The scope of energy consumption includes energy from all sources, including energy purchased from external sources and energy produced by the entity itself (self-generated). For example, direct fuel usage, purchased electricity, and heating, cooling and steam energy are all included within the scope of energy consumption.

1.2 The scope of energy consumption includes only energy directly consumed by the entity during the reporting period.

1.3 In calculating energy consumption from fuels and biofuels, the entity shall use higher heating values (HHV), also known as gross calorific values (GCV), which are measured directly or taken from the Intergovernmental Panel on Climate Change (IPCC).

2 The entity shall disclose (2) the percentage of energy it consumed that was supplied from grid electricity.

2.1 The percentage shall be calculated as purchased grid electricity consumption divided by total energy consumption.

3 The entity shall disclose (3) the percentage of energy it consumed that was renewable energy.

3.1 Renewable energy is defined as energy from sources that are replenished at a rate greater than or equal to their rate of depletion, such as geothermal, wind, solar, hydro and biomass.

3.2 The percentage shall be calculated as renewable energy consumption divided by total energy consumption.

3.3 The scope of renewable energy includes renewable fuel the entity consumed, renewable energy the entity directly produced and renewable energy the entity purchased, if purchased through a renewable power purchase agreement (PPA) that explicitly includes renewable energy certificates (RECs) or Guarantees of Origin (GOs), a Green-e Energy Certified utility or supplier programme, or other green power products that explicitly include RECs or GOs, or for which Green-e Energy Certified RECs are paired with grid electricity.

3.3.1 For any renewable electricity generated on site, any RECs and GOs shall be retained (not sold) and retired or cancelled on behalf of the entity for the entity to claim them as renewable energy.

3.3.2 For renewable PPAs and green power products, the agreement shall explicitly include and convey that RECs and GOs be retained or replaced and retired or cancelled on behalf of the entity for the entity to claim them as renewable energy.

3.3.3 The renewable portion of the electricity grid mix outside the control or influence of the entity is excluded from the scope of renewable energy.

3.4 For the purposes of this disclosure, the scope of renewable energy from biomass sources is limited to materials certified to a third-party standard (for example, Forest Stewardship Council, Sustainable Forest Initiative, Programme for the Endorsement of Forest Certification or American Tree Farm System), materials considered eligible sources of supply according to the *Green-e Framework for Renewable Energy Certification, Version 1.0* (2017) or Green-e regional standards, or materials eligible for an applicable jurisdictional renewable portfolio standard.

4 The entity shall apply conversion factors consistently for all data reported under this disclosure, such as the use of HHVs for fuel use (including biofuels) and conversion of kilowatt hours (kWh) to GJ (for energy data including electricity from solar or wind energy).

5 The entity may disclose the trailing 12-month (TTM) weighted average power usage effectiveness (PUE) for its data centres.

5.1 PUE is defined as the ratio of the total amount of power used by a computer data centre facility to the amount of power delivered to computing equipment.

5.2 If disclosing PUE, the entity shall follow the guidance and calculation methodology described in *PUE™: A Comprehensive Examination of the Metric* (2014), published by ASHRAE and The Green Grid Association.

TC-SI-130a.2. (1) Total water withdrawn, (2) total water consumed; percentage of each in regions with High or Extremely High Baseline Water Stress

1 The entity shall disclose the amount of water, in thousands of cubic metres, withdrawn from all sources.

1.1 Water sources include surface water (including water from wetlands, rivers, lakes and oceans), groundwater, rainwater collected directly and stored by the entity, and water and wastewater obtained from municipal water supplies, water utilities or other entities.

2 The entity may disclose portions of its supply by source if, for example, significant portions of withdrawals are from non-freshwater sources.

2.1 Fresh water may be defined according to the local laws and regulations where the entity operates. If no legal definition exists, fresh water shall be considered to be water that has less than 1,000 parts per million of dissolved solids.

2.2 Water obtained from a water utility in compliance with jurisdictional drinking water regulations can be assumed to meet the definition of fresh water.

3 The entity shall disclose the amount of water, in thousands of cubic metres, consumed in operations.

3.1 Water consumption is defined as:

3.1.1 Water that evaporates during withdrawal, use and discharge

3.1.2 Water that is directly or indirectly incorporated into the entity's product or service

3.1.3 Water that does not otherwise return to the same catchment area from which it was withdrawn, such as water returned to another catchment area or the sea

4 The entity shall analyse all its operations for water risks and identify activities that withdraw and consume water in locations with High (40–80%) or Extremely High (>80%) Baseline Water Stress as classified by the World Resources Institute's (WRI) Water Risk Atlas tool, Aqueduct.

5 The entity shall disclose water withdrawn in locations with High or Extremely High Baseline Water Stress as a percentage of the total water withdrawn.

6 The entity shall disclose water consumed in locations with High or Extremely High Baseline Water Stress as a percentage of the total water consumed.

TC-SI-130a.3. Discussion of the integration of environmental considerations into strategic planning for data centre needs

1 The entity shall describe how it integrates environmental considerations, including energy and water use, into strategic planning for data centres.

2 Discussion shall include, but is not limited to, how environmental factors impact the entity's decisions regarding the siting, design, construction, refurbishment, and operations of data centres.

2.1 Environmental factors and criteria may include:

2.1.1 Location-based environmental factors, such as regional humidity, average temperature and water availability.

2.1.2 Environmental regulations, such as energy efficiency standards and national- or state-level carbon legislation on pricing, and carbon intensity of grid electricity.

3 The scope of disclosure includes considerations for existing owned data centres, development of new data centres and outsourcing of data centre services, where relevant.

Data Privacy & Freedom of Expression

Topic Summary

As Software & IT Services entities increasingly deliver products and services over the Internet and through mobile devices, they must carefully manage two separate and often conflicting priorities. First, entities use customer data to innovate and provide customers with new products and services to generate revenues. Second, entities have access to a wide range of customer data, such as personal, demographic, content and behavioural data creating associated privacy concerns. This dynamic may result in increased regulatory scrutiny in many countries. The delivery of cloud-based software and IT services also raises concerns about potential access to user data by governments that may use it to limit the citizens' freedoms. Effective management in this area may reduce regulatory and reputational risks that may result in decreased revenues, reduced market share and increased regulatory actions involving potential fines and other legal costs.

Metrics

TC-SI-220a.1. Description of policies and practices relating to targeted advertising and user privacy

1 The entity shall describe the nature, scope and implementation of its policies and practices related to user privacy, including its targeted advertising practices, with a specific focus on how it manages the collection, use and retention of user information.

1.1 User information is defined as information that pertains to a user's attributes or actions which may include account statements, transaction records, records of communications, content of communications, demographic data, behavioural data, location data and personal data.

1.1.1 Demographic data is defined as information that identifies and distinguishes a given population. Examples of demographic data include gender, age, race/ethnicity, language, disabilities, mobility, home ownership and employment status.

1.1.2 Behavioural data is defined as information that tracks, measures and records individual behaviours, such as online browsing patterns, buying habits, brand preferences and product usage patterns.

1.1.3 Location data is defined as information that describes the physical location or movement patterns of an individual, such as Global Positioning System (GPS) coordinates or other related data that would enable identifying and tracking an individual's physical location.

1.1.4 Personal data is defined as any information that relates to an identified or identifiable living individual. Various pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

1.1.5 The entity may define personal data based on applicable jurisdictional laws or regulations. In such cases, the entity shall disclose the applicable jurisdictional standard or definition used.

1.2 Targeted advertising is defined as the practice of selecting and displaying advertisements to individual users based on their user information.

2 The entity shall describe the information 'lifecycle' (collection, usage, retention, processing, disclosure and destruction of information) and how information-handling practices at each stage may affect individuals' privacy.

2.1 With respect to data collection, the entity may discuss the data or types of data it collects without the consent of an individual, data that requires opt-in consent, and data that requires opt-out action from the individual.

2.2 With respect to data use, the entity may discuss the data or types of data it uses internally, and under which circumstances the entity shares, sells, rents, or otherwise distributes data or information to third parties.

2.3 With respect to retention, the entity may discuss which data or types of data it retains, the duration of retention, and practices used to ensure that data is stored securely.

3 The entity shall discuss its use of privacy impact assessments (PIAs), data protection impact assessments (DPIAs) or similar assessments.

3.1 A PIA or DPIA is an analysis of how information is handled that ensures handling conforms to applicable jurisdictional legal, regulatory and policy requirements regarding privacy; determines the risks and effects of collecting, maintaining and disseminating information in an identifiable form in an electronic information system; and examines and evaluates protections and alternative processes for handling information to mitigate potential privacy risks.

4 The entity shall discuss how its policies and practices related to privacy of user information address children's privacy, including the provisions of applicable jurisdictional children's privacy laws or regulations.

5 The scope of the disclosure includes both first- and third-party advertising.

TC-SI-220a.2. Number of users whose information is used for secondary purposes

1 The entity shall disclose the total number of unique users whose information is used for secondary purposes.

1.1 User information is defined as data that pertains to a user's attributes or actions, which may include account statements, transaction records, records of communications, content of communications, demographic data, behavioural data, location data and personal data.

1.1.1 Demographic data is defined as information that identifies and distinguishes a given population. Examples of demographic data include gender, age, race/ethnicity, language, disabilities, mobility, home ownership and employment status.

1.1.2 Behavioural data is defined as information that tracks, measures and records individual behaviours, such as online browsing patterns, buying habits, brand preferences and product usage patterns.

1.1.3 Location data is defined as information that describes the physical location or movement patterns of an individual, such as Global Positioning System (GPS) coordinates or other related data that identifies and tracks an individual's physical location.

1.1.4 Personal data is defined as information that relates to an identified or identifiable living individual. Various pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

1.1.5 The entity may define personal data based on applicable jurisdictional laws or regulations. In such cases, the entity shall disclose the applicable jurisdictional standard or definition used.

1.2 A secondary purpose is defined as the entity intentionally using data outside the primary purpose for which the data was collected. Examples of secondary purposes may include selling targeted advertisements and transferring data or information to a third party through sale, rental or sharing.

1.3 User accounts that the entity cannot verify as belonging to the same individual shall be disclosed separately.

2 The scope of the disclosure shall include the users whose information is used by the entity itself for secondary purposes, as well as the users whose information is provided to third parties, including those that directly or indirectly control, are controlled by, or are under common control with the entity, to use for secondary purposes.

TC-SI-220a.3. Total amount of monetary losses as a result of legal proceedings associated with user privacy

1 The entity shall disclose the total amount of monetary losses incurred during the reporting period resulting from legal proceedings associated with incidents relating to user privacy.

2 The legal proceedings shall include any adjudicative proceeding involving the entity, whether before a court, a regulator, an arbitrator or otherwise.

3 The losses shall include all monetary liabilities to the opposing party or to others (whether as the result of settlement, verdict after trial or otherwise), including fines and other monetary liabilities incurred during the reporting period as a result of civil actions (for example, civil judgements or settlements), regulatory proceedings (for example, penalties, disgorgement or restitution) and criminal actions (for example, criminal judgements, penalties or restitution) brought by any entity (for example, governmental, business or individual).

4 The scope of monetary losses shall exclude legal and other fees and expenses incurred by the entity in its defence.

5 The scope of the disclosure shall include legal proceedings associated with the enforcement of applicable jurisdictional laws or regulations.

Note to **TC-SI-220a.3**

1 The entity shall briefly describe the nature (for example, judgement or order issued after trial, settlement, guilty plea, deferred prosecution agreement or non-prosecution agreement) and context (for example, unauthorised monitoring, sharing of data or children's privacy) of all monetary losses resulting from legal proceedings.

2 The entity shall describe any corrective actions implemented in response to the legal proceedings. This may include specific changes in operations, management, processes, products, business partners, training or technology.

TC-SI-220a.4. (1) Number of law enforcement requests for user information, (2) number of users whose information was requested, (3) percentage resulting in disclosure

1 The entity shall disclose (1) the total number of unique requests for user information, including users' content and non-content data, from government or law enforcement agencies.

1.1 Content data includes user-generated information such as emails, texts and recorded phone conversations.

1.2 Non-content data includes information such as email addresses, names, countries of residence, gender, and system-generated data such as IP addresses and traffic data.

1.3 Both content and non-content data can include personal data.

1.3.1 Personal data is defined as any information that relates to an identified or identifiable living individual. Various pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

1.3.2 The entity may define personal data based on applicable jurisdictional laws or regulations. In such cases, the entity shall disclose the applicable jurisdictional standard or definition used.

2 The entity shall disclose (2) the total number of unique users whose information was requested by governmental authorities or law enforcement agencies.

2.1 The number of records requested shall be calculated as the sum of unique users whose user information was requested in all requests for information received from government or law enforcement agencies during the reporting period.

2.1.1 If the entity is unable to verify that two records (user information) belong to the same user, the entity shall consider this as two users.

3 The entity shall disclose (3) the percentage of governmental authorities and law enforcement requests that resulted in disclosure to the requesting party.

3.1 The percentage shall be calculated as the number of unique requests that resulted in disclosure to the requesting party divided by the total number of unique requests received.

3.2 The scope of requests that resulted in disclosure shall include requests that resulted in either full or partial compliance with the disclosure request within the reporting period.

3.3 The scope of requests that resulted in disclosure shall include disclosure of aggregated, de-identified and anonymised data, which is intended to prevent the recipient from reconfiguring the data to identify an individual's actions or identity.

3.3.1 The entity may discuss whether these characteristics apply to a portion of its data releases if this discussion would provide necessary context for interpretation of the entity's disclosure.

4 The entity additionally may disaggregate its disclosure by region or country.

5 The entity may describe its policy for determining whether to comply with a request for user data, including under what conditions it will release user data, what requirements must be met in the request, and the level of management approval required.

6 The entity may describe its policy for notifying users about such requests, including the timing of notification.

TC-SI-220a.5. List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring

1 The entity shall disclose a list of the countries where its products and services are monitored or blocked, or where its content is filtered or censored because of governmental, judicial, or law enforcement requests or requirements.

1.1 Monitoring occurs when a government authority or law enforcement agency has routine access to content or non-content data of some or of all users of a particular product or service.

1.2 Blocking occurs when the entity is prohibited by law or government authority from providing some or all of the entity's products or services in a country or region.

1.3 Content filtering or censoring occurs when a government authority alters access to, or display of, the content of a product or service either directly by overriding service provision, or indirectly by requiring that an entity remove specific content. An example is content considered politically or culturally sensitive.

2 The scope of this disclosure includes entity operations that are discontinued, or that were never offered, in a region because of government activity related to monitoring, blocking, content filtering or censoring.

Note to **TC-SI-220a.5**

1 The entity shall describe the extent of monitoring, blocking, content filtering or censorship across its product or service lines, including the specific products affected, nature and duration of filtering or censorship, and percentage of customers affected.

2 The entity may discuss the implications of blocking or censorship, such as adverse effects on the ability to grow market share or increased costs to comply with these restrictions.

3 For products and services modified in a manner material to their functionality, the entity shall identify the product or service affected and discuss the nature of the modification, indicating whether modification was undertaken to avoid monitoring or blocking, or to enable monitoring or blocking. The entity shall describe how the modified product or service differs from the product or service offering in its home country or other significant markets.

4 If relevant, the entity shall discuss its policies and practices related to freedom of expression, including how they influence its decision making for operations in countries that may request or require some form of monitoring, blocking, content filtering or censoring of the entity's content.

Data Security

Topic Summary

Software & IT Services entities are targets of growing data security threats from cyberattacks, which puts their own data and their customers' data at risk. Inadequate prevention, detection and remediation of data security threats may influence customer acquisition and retention and result in decreased market share and reduced demand for the entity's products. In addition to reputational damage and increased customer turnover, data breaches also may result in increased expenses, commonly associated with remediation efforts such as identity protection offerings and employee training on data protection. Meanwhile, new and emerging data security standards and regulations may affect operating expenses through increased compliance costs. Additionally, entities in this industry may be well-positioned to capture revenue opportunities by providing secure software and services to meet the demand for ensuring data is kept secure.

Metrics

TC-SI-230a.1. (1) Number of data breaches, (2) percentage that are personal data breaches, (3) number of users affected

1 The entity shall disclose (1) the total number of data breaches identified during the reporting period.

1.1 A data breach is defined as an unauthorised occurrence on, or conducted through, an entity's information systems that jeopardises the confidentiality, integrity or availability of an entity's information systems or any information contained therein.

1.1.1 Information systems are defined as information resources, owned or used by the entity, including physical or virtual infrastructure controlled by such information resources, or components thereof, organised for the collection, processing, maintenance, use, sharing, dissemination or disposition of an entity's information to maintain or support operations.

1.2 The scope of the disclosure excludes occurrences in which an entity has reasonable and supportable belief that the occurrence (i) does not pose a risk of damage to the entity's business performance or prospects and (ii) does not pose a risk of economic or social disadvantage to individuals.

2 The entity shall disclose (2) the percentage of data breaches that were personal data breaches.

2.1 A personal data breach is defined as a data breach resulting in the accidental or unauthorised destruction, loss, alteration, disclosure of or access to personal data transmitted, stored or otherwise processed.

2.2 Personal data is defined as any information that relates to an identified or identifiable living individual. Various pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

2.2.1 The entity may define personal data based on applicable jurisdictional laws or regulations. In such cases, the entity shall disclose the applicable jurisdictional standard or definition used.

2.3 The scope of the disclosure shall include incidents during which encrypted data was acquired with an encryption key that also was acquired, as well as whether a reasonable belief exists that encrypted data could be converted readily to plaintext.

2.3.1 Encryption is defined as the process of transforming plaintext into ciphertext.

3 The entity shall disclose (3) the total number of unique users affected by personal data breaches.

3.1 Accounts that the entity cannot verify as belonging to the same user shall be disclosed separately.

4 The entity may delay disclosure if a law enforcement agency has determined that notification impedes a criminal investigation and may be delayed until the law enforcement agency determines that such notification does not compromise the investigation.

Note to **TC-SI-230a.1**

1 The entity shall describe any corrective actions taken in response to data breaches, such as changes in operations, management, processes, products, business partners, training or technology.

2 All disclosure shall be sufficient such that it is specific to the risks the entity faces, but disclosure itself would not compromise the entity's ability to maintain data privacy and security.

3 The entity may disclose its policy for disclosing data breaches to affected users in a timely manner.

TC-SI-230a.2. Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards

1 The entity shall describe its approach to identifying information system vulnerabilities that may pose a data security risk.

1.1 Vulnerability is defined as a weakness in an information system, implementation, system security procedure or internal control that could be exploited.

1.2 Data security risk is defined as the risk of any circumstance or event with the potential to affect organisational operations (including mission, functions, image or reputation), assets, individuals, or other organisations or governments through an information system via unauthorised access, destruction, disclosure, modification of information or denial of service.

2 The entity shall describe its approach to managing identified data security risks and vulnerabilities, which may include operational procedures, management processes, structure of products, selection of business partners, employee training and use of technology.

3 The entity shall describe its use of third-party cybersecurity risk management standards.

3.1 Third-party cybersecurity risk management standards are defined as standards, frameworks or guidance developed by a third party with the explicit purpose of aiding entities in identifying cybersecurity threats, or preventing, or remediating or responding to cybersecurity incidents.

3.2 Examples of third-party cybersecurity risk management standards include:

3.2.1 the American Institute of Certified Public Accountants' (AICPA) Service Organisation Controls (SOC) for Cybersecurity;

3.2.2 ISACA's COBIT 5;

3.2.3 the ISO/IEC 27000-series; and

3.2.4 the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*, 2018.

3.3 The disclosure shall include:

3.3.1 identification of the specific cybersecurity risk management standards implemented or otherwise in use;

3.3.2 description of the extent of its use of cybersecurity risk management standards, such as by applicable operations, business unit, geography, product or information system;

3.3.3 the role of cybersecurity risk management standards in the entity's overall approach to identifying vulnerabilities in its information systems and addressing data security risks and vulnerabilities;

3.3.4 whether third-party verification of the use of cybersecurity risk management standards is conducted, including independent examinations or audits; and

3.3.5 activities and initiatives related to increasing the use of cybersecurity risk management standards, even if such standards are not currently in use.

4 The entity may discuss observed trends in type, frequency and origination of attacks on its data security and information systems.

5 All disclosure shall be sufficient such that it is specific to the risks the entity faces but disclosure itself would not compromise the entity's ability to maintain data privacy and security.

Recruiting & Managing a Global, Diverse & Skilled Workforce

Topic Summary

Employees are important contributors to value creation in the Software & IT Services industry. Entities commonly find recruiting qualified employees to fill these positions difficult. A shortage in technically skilled employees can create intense competition to acquire highly skilled employees globally, contributing to high employee turnover rates. Some entities contribute to relevant education and training programmes to expand the availability of domestic, skilled employees. Entities offer significant monetary and non-monetary benefits to improve employee engagement and therefore retention and productivity. Initiatives to improve employee engagement and work-life balance may influence the recruitment and retention of a diverse workforce. Since the industry is characterised by relatively low representation from women and minority groups, efforts to recruit and develop globally diverse talent pools may address the talent shortage and improve the value of entity offerings. Greater workforce diversity is important for innovation and helps entities understand the needs of a diverse and global customer base.

Metrics

TC-SI-330a.1. Percentage of employees that require a work visa

1 The entity shall disclose the percentage of employees that require a work visa in the country in which they are employed as of the close of the reporting period.

1.1 A work visa is defined as any non-immigrant visa, permit or other associated documentation issued by the applicable jurisdictional legal or regulatory immigration authorities to permit an employee who is a foreign national to work temporarily in the country in which they are employed. Work visas exclude permanent work and residence authorizations granted to foreign nationals (for example, permanent leave to remain or permanent resident status).

1.2 The percentage shall be calculated as the number of employees requiring a work visa divided by the total number of the entity's employees at the close of the reporting period.

2 The scope of employees includes those directly employed by the entity and excludes contractors and outsourced employees.

3 The scope of employees includes both full- and part-time employees.

Note to **TC-SI-330a.1**

1 The entity shall describe potential risks from recruiting employees that require a work visa, which may arise from immigration, naturalisation and visa regulations.

2 The entity shall describe how it manages the identified risks related to recruiting employees that require a work visa.

TC-SI-330a.2. Employee engagement as a percentage

1 The entity shall disclose employee engagement as a percentage.

1.1 Types of employee engagement levels may include:

1.1.1 actively engaged;

1.1.2 not engaged;

1.1.3 passive; and

1.1.4 actively disengaged.

1.2 If employee engagement is measured as an index (for example, strength of employee agreement with a survey statement), the entity shall convert the index into a percentage for this disclosure.

2 The percentage shall be calculated based on the results of an employee engagement survey or research study conducted by the entity, by an external party contracted by the entity to perform such a study, or by an independent third party.

2.1 The percentage shall be calculated as the number of employees who self-describe as actively engaged divided by the total number of employees who completed the survey.

Note to **TC-SI-330a.2**

1 The entity shall briefly describe:

1.1 the source of its survey (for example, third-party survey or entity's own);

1.2 the method used to calculate the percentage; and

1.3 a summary of questions or statements included in the survey or study (for example, those related to goal-setting, support to achieve goals, training and development, work processes, and commitment to the organisation).

2 If the survey method changes compared to previous reporting years, the entity shall provide results based on both the old and new methods for the year in which the change is made.

3 If results are limited to a subset of employees, the entity shall provide the percentage of employees included in the study or survey, and the representativeness of the sample.

4 The entity may disclose results of other survey findings such as the percentage of employees who are: proud of their work/where they work, inspired by their work/co-workers and aligned with corporate strategy and goals.

TC-SI-330a.3. Percentage of (1) gender and (2) diversity group representation for (a) executive management, (b) non-executive management, (c) technical employees, and (d) all other employees

1 The entity shall disclose (1) the percentage of gender representation among its employees for (a) executive management, (b) non-executive management, (c) technical employees and (d) all other employees.

1.1 The entity shall categorise the gender of its employees as women, men or not disclosed.

1.1.1 The entity may disclose additional categories of gender identity or expression.

1.2 The entity shall use these employee categories: (a) executive management, (b) non-executive management, (c) technical employees and (d) all other employees.

1.3 Executive management is defined as chief executives and senior officials who formulate and review the entity's policies, and plan, direct, coordinate and evaluate the overall activities of the entity with the support of other managers.

1.3.1 The entity may refer to the International Standard Classification of Occupations (ISCO) Sub-Major Group 11 or an applicable jurisdictional occupation classification system for a definition of executive management. In such cases, the entity shall disclose the occupation classification standard used to classify executive management.

1.4 Non-executive management is defined as those who plan, direct, coordinate and evaluate the activities of the entity, or of organisational units within it, and formulate and review its policies, rules and regulations, other than executive management.

1.4.1 The entity may refer to the ISCO Major Group 1 (excluding Sub-Major Group 11) or an applicable jurisdictional occupational classification system for a definition of non-executive management. In such cases, the entity shall disclose the occupation classification standard used to classify non-executive management.

1.5 Technical employees are defined as employees who perform highly skilled or highly qualified work generally categorised in the computing, mathematical, architectural, and engineering occupations.

1.5.1 The entity may refer to the ISCO Sub-Major Groups 21 and 25 or an applicable jurisdictional occupation classification system for a definition of technical employees. In such cases, the entity shall disclose the occupation classification system used to classify technical employees.

1.6 All other employees are defined as those employees who are not classified as executive management, non-executive management or technical employees.

1.7 The entity shall calculate the percentage of gender representation for each employee category as the number of employees in each gender category divided by the total number of employees in the respective employee category.

2 The entity shall disclose (2) the percentage of diversity group representation among its employees for (a) executive management, (b) non-executive management, (c) technical staff and (d) all other employees.

2.1 The entity shall identify diversity groups in its workforce.

2.1.1 Diversity is defined as the presence of people from populations who have been underrepresented in a particular field or are otherwise historically marginalised in a particular society.

2.1.2 Diversity groups may be defined by dimensions such as race, ethnicity, disability status, region of origin, migrant status, indigenous background, age, socioeconomic background, religious affiliation, sexual orientation, or gender identity.

2.1.3 Diversity groups may be defined by applicable jurisdictional laws or regulations or third-party frameworks.

2.1.4 The entity may omit diversity groups if collecting data on that group would be prohibited by applicable jurisdictional laws or regulations or would pose a risk of harm to members of the group.

2.2 The entity shall calculate the percentage of diversity group representation for each employee category as the number of employees in each diversity group, divided by the total number of employees in the respective employee category.

3 The entity may provide disclosures on gender or diversity group disaggregated by jurisdiction.

4 The entity may provide supplementary contextual disclosures on factors that significantly influence gender or diversity group representation, such as the jurisdiction in which employees are located.

5 The entity may disclose gender or diversity group representation by employee category in these table formats:

Table 3. Gender Representation of Global Employees (%)

	WOMEN	MEN	...	N/D*
Executive Management				
Non-executive Management				
Technical Employees				
All Other Employees				

*N/D = not disclosed

Table 4. Diversity Group Representation of Global Employees (%)

	GROUP A	GROUP B	GROUP C	...	N/A*
Executive Management					
Non-executive Management					

continued...

...continued

	GROUP A	GROUP B	GROUP C	...	N/A*
Technical Employees					
All Other Employees					

*N/A = not available or not disclosed

Note to **TC-SI-330a.3**

1 The entity shall describe its policies and programmes for fostering equitable employee representation in its global operations.

1.1 Relevant policies may include maintaining transparency of hiring, promotion and wage practices, ensuring equal employment opportunities, developing and disseminating diversity policies, and ensuring management accountability for equitable representation.

1.2 Relevant programmes may include training on diversity, mentorship and sponsorship programmes, partnership with employee resource and advisory groups, and provision of flexible work schedules to accommodate the varying needs of employees.

Intellectual Property Protection & Competitive Behaviour

Topic Summary

Entities in the Software & IT Services industry spend a significant proportion of their revenues on IP protection, including acquiring patents and copyrights. Although IP protection is inherent to some entity business models and is an important driver of innovation, entities' IP practices sometimes may be a contentious societal issue. Entities sometimes acquire patents and other IP protection to restrict competition and innovation, particularly if they are dominant market players. Because of software complexity, its abstract nature and increasing IP rights protection related to software, entities in the industry must navigate overlapping patent claims to operate. As a result, entities in the industry may find themselves constantly in litigation or subject to regulatory scrutiny either because of allegations of patent violations if they engage in unethical business practices, or are perceived as doing so, or because they engage in IP infringement litigation. Adverse legal or regulatory rulings related to antitrust and IP may expose entities in the industry to costly and lengthy litigations and potential monetary losses as a result. Such rulings also may affect an entity's market share and pricing power if its patents or dominant position in important markets are challenged legally, with potentially significant effects on revenue. Therefore, entities that balance the protection of their IP and its use to spur innovation while ensuring their IP management and other business practices do not unfairly restrict competition, may reduce regulatory scrutiny and legal actions while protecting their market value.

Metrics

TC-SI-520a.1. Total amount of monetary losses as a result of legal proceedings associated with anti-competitive behaviour regulations

1 The entity shall disclose the total amount of monetary losses incurred during the reporting period resulting from legal proceedings associated with anti-competitive behaviour such as those related to price fixing, antitrust behaviour (for example, exclusivity contracts), patent misuse, or network effects, as well as bundling services and products to limit competition.

2 The legal proceedings shall include any adjudicative proceeding involving the entity, whether before a court, a regulator, an arbitrator or otherwise.

3 The losses shall include all monetary liabilities to the opposing party or to others (whether as the result of settlement, verdict after trial or otherwise), including fines and other monetary liabilities incurred during the reporting period as a result of civil actions (for example, civil judgements or settlements), regulatory proceedings (for example, penalties, disgorgement or restitution) and criminal actions (for example, criminal judgements, penalties or restitution) brought by any entity (for example, governmental, business or individual).

4 The scope of monetary losses shall exclude legal and other fees and expenses incurred by the entity in its defence.

5 The scope of the disclosure shall include legal proceedings associated with the enforcement of applicable jurisdictional laws or regulations.

Note to **TC-SI-520a.1**

1 The entity shall briefly describe the nature (for example, judgement or order issued after trial, settlement, guilty plea, deferred prosecution agreement or non-prosecution agreement) and context (for example, price fixing, patent misuse or antitrust) of all monetary losses resulting from legal proceedings.

2 The entity shall describe any corrective actions implemented in response to the legal proceedings. This may include specific changes in operations, management, processes, products, business partners, training or technology.

Managing Systemic Risks from Technology Disruptions

Topic Summary

With trends towards increased cloud computing and Software as a Service (SaaS), software and IT service providers must ensure they have robust infrastructure and policies in place to minimise disruptions to their services. Disruptions such as programming errors or server downtime may generate systemic risks, because computing and data storage functions move from individual entity servers in various industries to data centres of cloud-computing service providers. The risks are increased particularly if the affected customers are in sensitive sectors, such as financial institutions or utilities, which are considered critical national infrastructure. Entities' investments in improving the reliability and quality of their IT infrastructure and services may attract and retain customers, thereby creating revenue and opportunities in new markets.

Metrics

TC-SI-550a.1. Number of (1) performance issues and (2) service disruptions; (3) total customer downtime

1 The entity shall disclose (1) the number of performance issues in software and information technology (IT) services provided to customers.

1.1 Performance issues are defined as any planned or unplanned downtime causing an interruption, of more than 10 minutes but less than or equal to 30 minutes, in the provision of cloud-based services to customers.

1.2 Performance issues may include those caused by technical failures, programming errors, cyber-attacks, weather events or natural disasters at hosting facilities.

2 The entity shall disclose (2) the number of service disruptions in software and IT services provided to customers.

2.1 Service disruptions are defined as any planned or unplanned downtime causing an interruption of more than 30 minutes in provision of cloud-based services to customers.

2.2 Service disruptions may include those caused by technical failures, programming errors, cyber-attacks, weather events or natural disasters at hosting facilities.

3 The entity shall disclose (3) the total customer downtime related to performance issues and service disruptions in software and IT services provided to customers.

3.1 Total customer downtime is defined as the interruption duration of each service disruption multiplied by the number of software and IT services licences affected, reported in licence-days. For context, the entity shall indicate the licensing basis (for example, number of seats, number of CPU cores, number of cloud subscriptions) and whether the licences are consumption-based or capacity-based.

Note to **TC-SI-550a.1**

1 For each significant service disruption, the entity shall disclose the duration of the disruption, the extent of disruption and the root cause, as well as any corrective actions taken to prevent future disruptions. Where material, the entity shall disclose the associated cost incurred, such as remediation costs to correct technology or process issues, as well as any liability costs

2 A service disruption is considered significant if the cost to correct it is material or if it is disruptive to a large number of customers or fundamental business operations in a manner that affects time to market, revenue capture or other material parameters.

TC-SI-550a.2. Description of business continuity risks related to disruptions of operations

1 The entity shall describe potential business continuity risks associated with technology disruptions affecting operations.

1.1 Examples of disruptions may include those caused by technical failures, programming errors, cyber-attacks, weather events or natural disasters at hosting facilities.

2 The entity shall discuss measures implemented to manage business continuity risks, such as technologies or processes that reduce the effects of disruptions, enhance the resilience of systems, insure against loss, or provide redundancies to critical business operations.

3 The entity shall identify which critical business operations support cloud-based services, and the entity shall further note whether those operations are owned or outsourced.

4 The entity may discuss estimated amount of potential loss, probability of that loss and the associated time frame. These estimates may be based on insurance figures or other third-party or internal assessments of potential loss.

SASB STANDARDS

Now part of IFRS Foundation