SASB STANDARDS

Now part of IFRS Foundation

Telecommunication Services

Sustainability Accounting Standard

TECHNOLOGY & COMMUNICATIONS SECTOR

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

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

Telecommunication Services industry entities provide a range of services from wireless and wireline telecommunications to cable and satellite services. The wireless services segment provides direct communication through radio-based cellular networks and operates and maintains the associated switching and transmission facilities. The wireline segment provides local and long-distance voice communication via the Public Switched Telephone Network. Wireline carriers also offer voice over internet protocol (VoIP) telephone, television and broadband internet services over an expanding network of fibre optic cables. Cable providers distribute television programming from cable networks to subscribers. They typically also provide consumers with video services, high-speed internet service and VoIP. Traditionally, these services are bundled into packages that charge subscribers a single payment. Satellite entities distribute TV programming through broadcasting satellites orbiting the earth or through ground stations. Entities serve customers primarily in their domestic markets, although some entities operate in more than one country.

SUSTAINABILITY DISCLOSURE TOPICS & METRICS

Table 1. Sustainability Disclosure Topics & Metrics

TOPIC	METRIC	CATEGORY	UNIT OF MEASURE	CODE
Environmental Footprint of Operations	(1) Total energy consumed, (2) percentage grid electricity and (3) percentage renewable	Quantitative	Gigajoules (GJ), Percentage (%)	TC-TL-130a.1
Data Privacy	Description of policies and practices relating to targeted advertising and customer privacy	Discussion and Analysis	n/a	TC-TL-220a.1
	Number of customers whose information is used for secondary purposes	Quantitative	Number	TC-TL-220a.2
	Total amount of monetary losses as a result of legal proceedings associated with customer privacy [1]	Quantitative	Presentation currency	TC-TL-220a.3
	(1) Number of law enforcement requests for customer information, (2) number of customers whose information was requested, (3) percentage resulting in disclosure	Quantitative	Number, Percentage (%)	TC-TL-220a.4
Data Security	(1) Number of data breaches, (2) percentage that are personal data breaches, (3) number of customers affected [2]	Quantitative	Number, Percentage (%)	TC-TL-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-TL-230a.2
Product End-of-life Management	(1) Materials recovered through take-back programmes, percentage of recovered materials that were (2) reused, (3) recycled, and (4) landfilled	Quantitative	Metric tonnes (t), Percentage (%)	TC-TL-440a.1
Competitive Behaviour & Open Internet	Total amount of monetary losses as a result of legal proceedings associated with anti-competitive behaviour regulations [3]	Quantitative	Presentation currency	TC-TL-520a.1
	Average actual sustained download speed of (1) owned and commercially-associated content and (2) non-associated content	Quantitative	Megabits per second (Mbps)	TC-TL-520a.2
	Description of risks and opportunities associated with net neutrality, paid peering, zero-rating, and related practices	Discussion and Analysis	n/a	TC-TL-520a.3

continued...

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

2 Note to **TC-TL-230a.1** – The disclosure shall include a description of corrective actions implemented in response to data breaches.

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

...continued

TOPIC	METRIC	CATEGORY	UNIT OF MEASURE	CODE
Managing Systemic Risks from Technology Disruptions	(1) System average interruption duration, (2) system average interruption frequency and (3) customer average interruption duration [4]	Quantitative	Minutes, Number	TC-TL-550a.1
	Discussion of systems to provide unimpeded service during service disruptions	Discussion and Analysis	n/a	TC-TL-550a.2

Table 2. Activity Metrics

ACTIVITY METRIC	CATEGORY	UNIT OF MEASURE	CODE
Number of wireless subscribers[5]	Quantitative	Number	TC-TL-000.A
Number of wireline subscribers[6]	Quantitative	Number	TC-TL-000.B
Number of broadband subscribers[7]	Quantitative	Number	TC-TL-000.C
Network traffic	Quantitative	Petabytes	TC-TL-000.D

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

[5] Note to **TC-TL-000.A** – Wireless subscribers are defined as those customers that contract with the entity for mobile services, which include cellular phone service or wireless data service.

[6] Note to **TC-TL-000.B** – Wireline subscribers are defined as those customers that contract with the entity for fixed line phone services.

[7] Note to **TC-TL-000.C** – Broadband subscribers are defined as those customers that contract with the entity for fixed line cable and internet services, which include WiFi connections.

Environmental Footprint of Operations

Topic Summary

Individual Telecommunication Services entities consume substantial amounts of energy. Depending on the source of energy and generation efficiency, electricity consumption by telecom network infrastructure can contribute significantly to environmental externalities, such as climate change, creating sustainability risks for the industry. Although network equipment and data centres are becoming more energy efficient, their overall energy consumption is increasing with the expansion in telecommunications infrastructure and data traffic. How Telecommunication Services entities manage their overall energy efficiency or intensity, reliance on different types of energy, and how they access alternative sources of energy may become increasingly material as the global regulatory focus on climate change increases, creating incentives for energy efficiency and renewable energy as well as pricing of greenhouse gas (GHG) emissions. Because energy expenditures may be significant in the industry, entities that improve operational energy efficiency may increase cost savings and profit margins.

Metrics

TC-TL-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, 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 usage (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.

Data Privacy

Topic Summary

As customers increasingly pay attention to privacy issues associated with cell phone, internet and email services, Telecommunication Services entities must implement strong management practices and guidelines related to their use of customer data. Telecommunication Services entities use growing volumes of customer location, web browsing and demographic data to improve their services as well as generate revenue by selling such data to third parties. Growing public concern about privacy may result in increased regulatory scrutiny over the use, collection and sale of consumer data. These trends increase the importance of Telecommunication Services entities adopting and communicating policies about providing customer data to third parties transparently, including the amount and type of data provided and the nature of its use (for example, use for commercial purposes). Additionally, Telecommunication Services entities receive, and must determine whether to comply with, government requests for customer information. Entities in the industry that fail to manage data privacy may be susceptible to decreased revenues because of lost consumer confidence and churn, as well as to financial effects stemming from legal exposures.

Metrics

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

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

1.1 Customer information is defined as information that pertains to a customer'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 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 an 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 the 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 addressing children's privacy.

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

TC-TL-220a.2. Number of customers whose information is used for secondary purposes

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

1.1 Customer information is defined as data that pertains to a customer'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 Customer 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 customers whose information is used by the entity itself for secondary purposes, as well as the customers 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-TL-220a.3. Total amount of monetary losses as a result of legal proceedings associated with customer 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 customer 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-TL-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-TL-220a.4. (1) Number of law enforcement requests for customer information, (2) number of customers whose information was requested, (3) percentage resulting in disclosure

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

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

1.2 Non-content data includes information such as an 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 customers whose customer information was requested across 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 (customer information) belong to the same customer, the entity shall consider this as two customers.

3 The entity shall disclose (3) the percentage of governmental 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 customer data request, including under what conditions it will release customer 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 customers about such requests, including the timing of notification.

Data Security

Topic Summary

The Telecommunication Services industry is particularly vulnerable to data security threats because entities manage an increasing volume of customer data, including personally identifiable information, as well as demographic, behavioural and location data. Inadequate prevention, detection and remediation of data security threats may influence customer acquisition and retention and result in decreased market share and lower 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. As the providers of critical infrastructure, the ability of entities to combat cyber-attacks may affect reputation and brand value, with a long-term effect on market share and revenue growth potential. Therefore, entities that identify and manage data security risks in a timely manner may be in a better position to protect market share and brand value while also reducing risk exposure to cyber-attacks. Additionally, new and emerging data security standards and regulations may affect the operating expenses of entities through increased costs of compliance.

Metrics

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

3.1 Accounts that the entity cannot verify as belonging to the same customer 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-TL-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 customers in a timely manner.

TC-TL-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, 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 the 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 that have been implemented or are 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 the 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.

Product End-of-life Management

Topic Summary

Because of the rapid obsolescence of communications devices, particularly mobile phones, they represent an increasing proportion of electronic waste (e-waste) going to landfills, driven in part by a low recycling rate. Telecommunication Services entities face growing regulatory risks related to this issue. Numerous jurisdictions have implemented e-waste recycling laws mandating that electronics retailers and manufacturers create a system for recycling, reuse or proper disposal of electronic devices. Although in their early days many of these laws covered a limited scope of products, recent laws extend to mobile devices, requiring entities to finance the collection, treatment, recycling or proper disposal of e-waste, as concerns around e-waste from communications devices increase. E-waste laws often require vendors or manufacturers to pay for waste recycling or product take-back and recycling programmes. Penalties or costs, because of such laws, together with potential revenues generated from refurbishing and re-selling products, increasingly are providing incentives for entities in the industry to manage end-of-life impacts. Many Telecommunication Services entities work in partnership with phone manufacturers to bundle telecom services and mobile devices, and therefore have a shared responsibility for end-of-life management of such devices. Their relationship with customers provides an opportunity for effective management of product recycling, reuse and disposal. Establishing take-back programmes to recover end-of-life materials for further reuse, recycling or remanufacturing may increase cost savings and develop a more resilient supply of manufacturing materials.

Metrics

TC-TL-440a.1. (1) Materials recovered through take-back programmes, percentage of recovered materials that were (2) reused, (3) recycled, and (4) landfilled

1 The entity shall disclose (1) the total weight, in metric tonnes, of materials recovered through product take-back programmes and recycling services.

1.1 The scope of the disclosure shall include products, materials and parts, that are collected at the end of their useful life that would have otherwise been discarded as waste or used for energy recovery.

1.2 The scope of the disclosure shall include both materials physically handled by the entity and materials of which the entity does not take physical possession, but for which it has contracted with a third party the task of collection for the purpose of reuse, recycling or refurbishment.

1.3 The scope of the disclosure excludes products and parts that are in-warranty and have been collected for repairs.

2 The entity shall disclose (2) the percentage of materials recovered, by weight, that were reused.

2.1 Reused materials are defined as those recovered products or components of products used, or intended to be used in the future, by the entity or by a third party for their originally intended purpose.

2.2 Percentage shall be calculated as the weight of the recovered materials reused divided by the total weight of all recovered materials.

2.3 The scope of reused materials includes products donated or refurbished by the entity or third parties.

2.4 The scope of the disclosure includes reuse by the entity or by third parties through direct contract with the entity.

3 The entity shall disclose (3) the percentage of materials recovered, by weight, that were recycled or remanufactured.

3.1 Recycled and remanufactured materials are defined as materials reprocessed or treated through production or manufacturing processes and made into a final product or made into a component to be integrated into a product.

3.2 Percentage shall be calculated as the weight of the recovered materials recycled or remanufactured divided by the total weight of all recovered materials.

3.3 The scope of the disclosure includes recycling conducted by the entity or by third parties through direct contract with the entity.

3.4 Portions of products and materials discarded in landfills are not considered recycled; only the portions of products directly incorporated into new products, co-products or by-products shall be included in the percentage recycled.

3.5 Materials incinerated, including for energy recovery, shall not be considered within the scope of recycled materials.

3.5.1 Energy recovery is defined as the use of combustible waste to generate energy through direct incineration, with or without other waste, but with recovery of the heat.

4 The entity shall disclose (4) the percentage of materials recovered, by weight, that were landfilled.

4.1 Percentage shall be calculated as the weight of the recovered materials that were landfilled divided by the total weight of all recovered materials.

5 Electronic waste material (e-waste) shall be considered recycled only if the entity can demonstrate that this material was transferred to entities with third-party certification to a standard for e-waste recycling such as the e-Stewards® Standard for Responsible Recycling and Reuse of Electronic Equipment or the Responsible Recycling Practices (R2) Standard for Electronic Recyclers.

5.1 The entity shall disclose the standards to which the entities to which it has transferred e-waste are compliant.

Competitive Behaviour & Open Internet

Topic Summary

The Telecommunication Services industry contains classic examples of natural monopolies, where high capital costs allow them to offer the most efficient production. Given the concentrated nature of telecommunications, cable and satellite entities, they must manage their growth strategies within the parameters of a regulatory landscape designed to ensure competition. In addition to natural monopoly, many entities in this industry benefit from terminal access monopolies over the so-called 'last-mile' of their networks, given their contractual relationship with each subscriber and the barriers for subscribers to change service providers. The nature of this relationship is the basis of much of the discussion regarding an open internet, where all data on the internet is treated equally in terms of performance and access. The industry faces legislative and regulatory actions to ensure competition, which may limit the market share and growth potential of some larger players. Merger and acquisition activity by dominant market players has come under regulatory scrutiny. This has resulted in entities abandoning plans to consolidate, affecting their value. Strong reliance on market dominance also may be a source of risk if entities are vulnerable to legal challenges, increasing their risk profile and cost of capital.

Metrics

TC-TL-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-TL-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.

TC-TL-520a.2. Average actual sustained download speed of (1) owned and commercially-associated content and (2) non-associated content

1 The entity shall disclose the average actual sustained download speed in Megabits per second (Mbps), for delivery of (1) owned and commercially-associated content and (2) non-associated content.

1.1 Actual sustained download speed is defined as throughput, in Mbps, using three concurrent TCP connections measured at the 25–30 second interval of a sustained data transfer.

1.1.1 The entity shall disclose its methodology for measuring download speed, such as the period over which the test was conducted, sample size, whether it reflects peak versus non-peak speeds, whether the measurement isolates the effects of transient performance-enhancing features (for example, throttling or 'burst' speeds), and limits on accuracy.

1.2 Owned and commercially-associated content is defined as content owned by the entity directly, such as content created through media-production business segments of the entity, its parent or its subsidiaries, and content owned by entities with whom the entity has commercial agreements, such as pay-for-priority agreements or content delivery network peering agreements.

1.3 Non-associated content is defined as any content not owned by or commercially-associated with the entity, as described above.

2 The average actual sustained download speed is calculated as the sales-weighted aggregate of average actual sustained download speeds of each tier of service on a per-user account basis (weighted by number of user accounts in each tier of service, not actual usage).

3 The entity may disclose its average advertised download speed.

3.1 Average advertised download speed is defined as the download speed advertised for each user account based on the speed of the account type.

3.2 The average advertised speed is calculated as the average of monthly advertised download speeds on a sales-weighted user account basis (weighted by number of user accounts, not actual usage).

TC-TL-520a.3. Description of risks and opportunities associated with net neutrality, paid peering, zero-rating, and related practices

1 The entity shall describe risks and opportunities associated with net neutrality and open internet.

1.1 Net neutrality and open internet refers to the idea, principle or requirement that internet service providers (ISPs) should or must treat all internet data as the same regardless of its kind, source or destination.

1.2 The scope of the disclosure shall include the entity's approach to these concepts:

1.2.1 transparency—whether and how an ISP transparently discloses to its subscribers and users all relevant information as to the policies that govern its network;

1.2.2 blocking—whether and under what circumstances an ISP blocks legal content on its network; and

1.2.3 no unreasonable discrimination—ISPs may not act in a commercially unreasonable manner to harm the internet, including favouring the traffic from an affiliated entity.

1.3 The scope of the disclosure includes a discussion of the risks and opportunities associated with the legal classification of ISPs in the jurisdictions in which the entity operates—such as, for example, whether ISPs are classified similarly to other communications services such as radio or telephone.

1.4 The scope of risks may include risks from actual or potential rules or regulations, potential limitations on an entity's ability to deliver its own content, increased competition from edge providers that stream content, reputational harm with consumers, or possible restrictions on an entity's ability to generate new revenue streams from peering and pay-for-priority agreements, or to earn capital needed to support a growing and evolving broadband infrastructure.

1.5 The scope of opportunities may include growth in delivery of owned and affiliated content, increased market penetration, or improved advertising revenues.

2 The entity shall discuss its policies for engagement in paid peering agreements and settlement-free peering agreements.

2.1 Peering agreement is defined as an arrangement whereby one internet operation connects directly to another so that the two can trade traffic.

3 The entity shall discuss its policies for engagement in zero-rating.

3.1 Zero-rating is defined as an arrangement wherein customer data usage is not billed nor counted toward any customer data plan limit if customers are accessing specific content affiliated with the mobile network operator or internet service provider.

Managing Systemic Risks from Technology Disruptions

Topic Summary

Given the systemic importance of telecommunications networks, systemic or economy-wide disruption may result if the Telecommunication Services network infrastructure is unreliable and prone to business continuity risks. As the frequency of extreme weather events associated with climate change increases, Telecommunication Services entities may face growing physical threats to network infrastructure, with potentially significant social or systemic impacts. In the absence of resilient and reliable infrastructure, entities may lose revenue associated with service disruptions or face unplanned capital expenditures to repair damaged or compromised equipment. Entities that successfully manage business continuity risks, including identifying critical business operations, and that enhance resilience of the system may substantially reduce their risk exposure and decrease their cost of capital. While implementation of such measures may have upfront costs, entities may gain long-term benefits in terms of lower remediation expenses in cases of high-impact disruptions.

Metrics

TC-TL-550a.1. (1) System average interruption duration, (2) system average interruption frequency and (3) customer average interruption duration

1 The entity shall disclose its (1) system average interruption duration in minutes.

1.1 The system average interruption duration is defined as the total duration of service disruptions for the average customer during the reporting period.

1.2 A service disruption is defined as a significant degradation or interruption in the ability of a significant number of end users to establish and maintain a channel of communications in a particular service offered by the entity (voice, SMS, broadband, mobile data, etc.) because of failure or degradation in the performance of a communications provider's network.

1.3 The entity shall calculate its system average interruption duration as the sum of the number of customers interrupted in each service disruption multiplied by the duration of each service disruption (restoration time), divided by the total number of customers served, written as $\sum(r_i \times N_i) / N_T$.

1.3.1 $\sum$ = Summation function

1.3.2 r_i = Restoration time for each service disruption, in minutes

1.3.3 N_i = Total number of customers interrupted in each service disruption

1.3.4 N_T = Average number of unique customer accounts with active service during the reporting period

2 The entity shall disclose its (2) system average interruption frequency as a number of service disruptions per customer.

2.1 The system average interruption frequency is defined as the average number of times a customer experienced a service disruption during the reporting period.

2.2 The entity shall calculate its system average interruption frequency as the total number of customers interrupted divided by the total number of customers served, written as $\sum(N_i) / N_T$.

2.2.1 $\sum$ = Summation function

2.2.2 N_i = Number of customers interrupted in each service disruption

2.2.3 N_T = Average number of unique customer accounts with active service during the reporting period

3 The entity shall disclose its (3) customer average interruption duration in minutes.

3.1 The customer average interruption duration is defined as the average amount of time required to restore service once a service disruption has occurred.

3.2 The entity shall calculate its customer average interruption duration as the sum of the number of customers interrupted in each incident multiplied by the duration of each service disruption (restoration time), divided by the total number of customers interrupted, written as $\sum(N_i \times r_i) / \sum(N_i)$.

3.2.1 $\sum$ = Summation function

3.2.2 r_i = Restoration time for each service disruption, in minutes

3.2.3 N_i = Number of customers interrupted in each service disruption

4 The scope of disclosure is restricted to:

4.1 Wireline communications services

4.2 Wireless communications services

4.3 Internet service provider (ISP) services

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

1 The system average interruption duration, system average interruption frequency, and customer average interruption duration are related metrics, and one can be derived from the other two. For example, the system average interruption duration (sub-metric 1) can be calculated by multiplying the system average interruption frequency (sub-metric 2) by the customer average interruption duration (sub-metric 3).

2 For each significant service interruption, the entity shall disclose the duration of the disruption, the extent of impact and the root cause, as well as any corrective actions taken to prevent future disruptions.

2.1 If relevant, the entity shall show costs incurred, such as those because of organisational change, training or technology expenditures required for remediation, lost revenue, payment of warranties or costs associated with breach of contract.

TC-TL-550a.2. Discussion of systems to provide unimpeded service during service disruptions

1 The entity shall discuss business continuity risks associated with service disruptions affecting operations.

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

2 The entity shall discuss how it manages business continuity risks, including an identification of critical business operations and redundancies or other measures implemented to enhance resilience of the system or to reduce impact, including insurance against loss.

3 The entity may discuss the 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