SASB STANDARDS

Now part of IFRS Foundation

Professional & Commercial Services

Sustainability Accounting Standard

SERVICES SECTOR

Sustainable Industry Classification System® (SICS®) SV-PS

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

Professional & Commercial Services industry entities rely on the skills and knowledge of their employees to serve a wide range of clients. Services often are provided on an assignment basis, where an individual or team is responsible for the delivery of client services. Offerings may include management and administration consulting services, such as staffing and executive search services; legal, accounting and tax preparation services; and financial and non-financial information services. Non-financial information service providers may specialise in an array of sectors such as energy, healthcare, real estate, technology and science. Financial information service entities include credit and rating agencies as well as data and portfolio analytics providers. Customers of professional and commercial service providers include private and public for-profit institutions and non-profit organisations.

SUSTAINABILITY DISCLOSURE TOPICS & METRICS

Table 1. Sustainability Disclosure Topics & Metrics

TOPIC	METRIC	CATEGORY	UNIT OF MEASURE	CODE
Data Security	Description of approach to identifying and addressing data security risks	Discussion and Analysis	n/a	SV-PS-230a.1
	Description of policies and practices relating to collection, usage, and retention of customer information	Discussion and Analysis	n/a	SV-PS-230a.2
	(1) Number of data breaches, (2) percentage that (a) involve customers' confidential business information and (b) are personal data breaches, (3) number of (a) customers and (b) individuals affected [1]	Quantitative	Number, Percentage (%)	SV-PS-230a.3
Workforce Diversity & Engagement	Percentage of (1) gender and (2) diversity group representation for (a) executive management, (b) non-executive management, and (c) all other employees [2]	Quantitative	Percentage (%)	SV-PS-330a.1
	(1) Voluntary and (2) involuntary turnover rate for employees	Quantitative	Percentage (%)	SV-PS-330a.2
	Employee engagement as a percentage [3]	Quantitative	Percentage (%)	SV-PS-330a.3
Professional Integrity	Description of approach to ensuring professional integrity	Discussion and Analysis	n/a	SV-PS-510a.1
	Total amount of monetary losses as a result of legal proceedings associated with professional integrity [4]	Quantitative	Presentation currency	SV-PS-510a.2

Table 2. Activity Metrics

ACTIVITY METRIC	CATEGORY	UNIT OF MEASURE	CODE
Number of employees by: (1) full-time and part-time, (2) temporary, and (3) contract	Quantitative	Number	SV-PS-000.A
Employee hours worked, percentage billable	Quantitative	Hours, Percentage (%)	SV-PS-000.B

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

[2] Note to **SV-PS-330a.1** – The entity shall describe its policies and programmes for fostering equitable employee representation across its global operations.

[3] Note to **SV-PS-330a.3** – The disclosure shall include a description of the method employed.

[4] Note to **SV-PS-510a.2** – The entity shall briefly describe the nature, context and corrective actions taken because of monetary losses.

Data Security

Topic Summary

Entities in every segment of the industry are entrusted with customer data. Employment and temporary staffing agencies as well as data providers and consulting entities store, process and transmit increasing amounts of sensitive personal data about employees, clients and candidates. In addition, the clients of financial and non-financial services providers may handle sensitive information and share this information with professional and commercial services entities. The exposure of sensitive customer information through cybersecurity breaches, other malicious activities or employee negligence may result in significant risks such as identity fraud and theft. Data breaches may compromise client perception of the effectiveness of a service provider's security measures, which may result in reputational damage and affect an entity's ability to attract and retain clients adversely.

Metrics

SV-PS-230a.1. Description of approach to identifying and addressing data security risks

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

4 The entity may describe the degree to which its approach is aligned with an external standard or framework, or applicable jurisdictional legal or regulatory framework for managing data security, such as:

4.1 the ISO/IEC 27000-series; and

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

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.

SV-PS-230a.2. Description of policies and practices relating to collection, usage, and retention of customer information

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

1.1 Customer information includes information that pertains to a customer's attributes or actions, which may include records of communications, content of communications, demographic data, personally identifiable information or confidential business information.

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

1.3 Confidential business information is defined as information that concerns or relates to trade secrets, processes, operations, identification of customers, inventories or other information of commercial value, the disclosure of which is likely to cause substantial harm to the competitive position of the person, partnership or entity from which the information was obtained.

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.

1.4.1 The entity may define personal data based on an applicable jurisdictional legal or regulatory definition. In such cases, the entity shall disclose the applicable jurisdictional standard or definition used.

2 The entity shall describe the information 'lifecycle' (collection, use, 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 usage, the entity may discuss the data or types of data used internally, and under which circumstances the entity shares, sells, rents or otherwise distributes data or information to third parties.

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

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

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

SV-PS-230a.3. (1) Number of data breaches, (2) percentage that (a) involve customers' confidential business information and (b) are personal data breaches, (3) number of (a) customers and (b) individuals 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, (ii) does not pose a risk of damage to the interests of its customers and (iii) does not pose a risk of economic or social disadvantage to individuals.

2 The entity shall disclose (2) the percentage of data breaches that (a) involve customers' confidential business information and (b) are personal data breaches.

2.1 Confidential business information is defined as information that concerns or relates to the trade secrets, processes, operations, identification of customers, inventories or other information of commercial value, the disclosure of which is likely to cause substantial harm to the competitive position of the person, partnership or entity from which the information was obtained.

2.1.1 Confidential business information includes information that is defined as confidential by contractual agreements (such as non-disclosure agreements) between the entity and its customers.

2.2 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.

2.3 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.

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

2.4 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.

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

3 The entity shall disclose (3) the total number of unique (a) customers and (b) individuals affected by data breaches, which includes all those individuals affected by a personal data breach.

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 **SV-PS-230a.3**

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.

Workforce Diversity & Engagement

Topic Summary

Developing a broad base of valued, respected and supported employees throughout an organisation is essential for the long-term growth prospects of professional and commercial services entities. Human capital is the primary source of revenue generation, contributing knowledge, talent, advice and various technical skills. Although financial and non-financial service providers may hire a diverse workforce among lower-level employees, they may lack diversity among senior management. Enhancing workforce diversity, particularly among management positions, may help entities attract and develop the best talent. Significant employee engagement, fair treatment and equitable levels of pay and advancement opportunities for all workers are all likely to contribute to increased productivity and performance through all levels of the entity.

Metrics

SV-PS-330a.1. Percentage of (1) gender and (2) diversity group representation for (a) executive management, (b) non-executive management, and (c) 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 and (c) 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 and (c) 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 All other employees are defined as those employees who are not classified as executive management or non-executive management.

1.5.1 For staffing agencies, disclosure shall additionally be disaggregated by (i) non-contingent staff and (ii) contingent staff (those workers who are placed at client sites, but who remain employees of the staffing agencies).

1.6 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 and (c) 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 representation 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				

continued...

...continued

	WOMEN	MEN	...	N/D*
All Other Employees – Non-Contingent				
All Other Employees – Contingent				

*N/D = not disclosed

Table 4. Diversity Group Representation of U.S. Employees (%)

	GROUP A	GROUP B	GROUP C	...	N/A*
Executive Management					
Non-executive Managment					
All Other Employees – Non-Contingent					
All Other Employees – Contingent					

*N/A = not available or not disclosed

Note to **SV-PS-330a.1**

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.

SV-PS-330a.2. (1) Voluntary and (2) involuntary turnover rate for employees

1 The entity shall disclose the employee turnover rate as a percentage for all employees.

1.1 Turnover shall be disclosed separately for (1) voluntary and (2) involuntary departures.

2 The entity shall calculate (1) the voluntary turnover rate as the number of employee-initiated voluntary separations (for example, resignation or retirement) during the reporting period, divided by the average number of workers employed during the reporting period.

3 The entity shall calculate (2) the involuntary turnover rate as the number of entity-initiated separations (for example, dismissal, downsizing, redundancy or non-renewal of contract) during the reporting period, divided by the average number of workers employed during the reporting period.

4 For staffing agencies, the scope of the disclosure excludes the contingent workforce (those workers who are placed at client sites, but who remain employees of the staffing agencies).

SV-PS-330a.3. 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 **SV-PS-330a.3**

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.

Professional Integrity

Topic Summary

The business model of professional and commercial services entities is dependent on client trust and loyalty. To ensure long-term and mutually beneficial relationships, entities must provide services that meet the highest professional standards of the industry. Professional integrity is an important industry governance issue because the collective actions of professionals inside a single organisation may make the detection and prevention of conflicts of interest, bias or negligence more challenging. Training employees adequately, providing advice and distributing data free from bias and error, and taking other measures to ensure professional integrity, are important both for strengthening an entity's licence to operate as well as for attracting and retaining clients.

Metrics

SV-PS-510a.1. Description of approach to ensuring professional integrity

1 The entity shall describe its policies to ensure professional integrity.

1.1 The scope of the disclosure includes aspects of professional integrity relating to conflict of interest, accuracy of data and corruption.

2 The scope of ensuring professional integrity may include policies, training and implementation of codes of ethics as well as investigations, enforcement and disciplinary procedures relating to:

2.1 avoidance of conflicts of interest, including mitigation and transparency of potential or perceived conflicts;

2.2 oversight of advisory services and recommendations;

2.3 maintenance and reporting of accurate data;

2.4 protection of confidential business information, including accuracy, retention and destruction of business records and documents;

2.5 prevention of billing fraud;

2.6 avoidance of corruption, including identification of suspicious activities and whistle-blower protection programmes;

2.7 privacy guidelines and security clearances for gaining access to sensitive and classified data;

2.8 employee training on relevant regulations;

2.9 mechanisms for internal reporting about violations or concerns regarding business ethics or compliance;

2.10 processes for internal investigations of malpractice or negligence; and

2.11 disciplinary actions for violations of professional integrity policies.

3 The entity may discuss compliance with industry best practices, including codes of conduct and codes of ethics, as a measure of its management approach to ensuring quality of work and professional integrity.

SV-PS-510a.2. Total amount of monetary losses as a result of legal proceedings associated with professional integrity

1 The entity shall disclose the total amount of monetary losses incurred during the reporting period resulting from legal proceedings associated with professional integrity, including negligence, malpractice, breach of contract, fraud, corruption and bribery.

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 (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 **SV-PS-510a.2**

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, negligence) 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.

SASB STANDARDS

Now part of IFRS Foundation