SASB STANDARDS

Now part of IFRS Foundation

Aerospace & Defence

Sustainability Accounting Standard

RESOURCE TRANSFORMATION SECTOR

Sustainable Industry Classification System® (SICS®) RT-AE

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

Entities in the Aerospace & Defence industry include manufacturers of commercial aircraft, aircraft parts, aerospace and defence products, as well as defence prime contractors. Commercial aircraft manufacturers represent approximately one quarter of industry revenue and sell mainly to commercial airlines and governments. Aerospace and defence parts manufacturers represent the largest segment of the industry by total revenue, selling primarily to governments. Both aerospace and defence manufacturers operate globally and serve a global customer base. Defence primes represent approximately one quarter of total industry revenue and manufacture products including military aircraft, space vehicles, missile systems, ammunition, small arms, naval ships, and other commercial and military vehicles. Their customers consist of various government agencies and related businesses with global operations. The defence prime category also includes firearms manufacturers that sell to law enforcement agencies, businesses, distributors, retailers and consumers. Important sustainability topics within the industry include the energy efficiency and emissions profile of products and management of manufacturing energy and waste.

SUSTAINABILITY DISCLOSURE TOPICS & METRICS

Table 1. Sustainability Disclosure Topics & Metrics

TOPIC	METRIC	CATEGORY	UNIT OF MEASURE	CODE
Energy Management	(1) Total energy consumed, (2) percentage grid electricity and (3) percentage renewable	Quantitative	Gigajoules (GJ), Percentage (%)	RT-AE-130a.1
Hazardous Waste Management	(1) Amount of hazardous waste generated, (2) percentage recycled	Quantitative	Metric tonnes (t), Percentage (%)	RT-AE-150a.1
	(1) Number and aggregate quantity of reportable spills, (2) quantity recovered [1]	Quantitative	Number, Kilogrammes (kg)	RT-AE-150a.2
Data Security	(1) Number of data breaches, (2) percentage involving confidential information [2]	Quantitative	Number, Percentage (%)	RT-AE-230a.1
	Description of approach to identifying and addressing data security risks in (1) entity operations and (2) products	Discussion and Analysis	n/a	RT-AE-230a.2
Product Safety	(1) Number of recalls issued, (2) total units recalled [3]	Quantitative	Number	RT-AE-250a.1
	(1) Number of counterfeit parts detected, (2) percentage avoided	Quantitative	Number, Percentage (%)	RT-AE-250a.2
	(1) Number of Airworthiness Directives received, (2) total units affected [4]	Quantitative	Number	RT-AE-250a.3
	Total amount of monetary losses as a result of legal proceedings associated with product safety [5]	Quantitative	Presentation currency	RT-AE-250a.4
Fuel Economy & Emissions in Use-phase	Revenue from alternative energy-related products	Quantitative	Presentation currency	RT-AE-410a.1
	Description of approach and discussion of strategy to address fuel economy and greenhouse gas (GHG) emissions of products	Discussion and Analysis	n/a	RT-AE-410a.2

continued...

1 Note to **RT-AE-150a.2** – The entity shall discuss long-term activities to remediate spills that occurred in years prior to the reporting period but for which remediation activities are ongoing.

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

3 Note to **RT-AE-250a.1** – The disclosure shall include a discussion of notable recalls, such as those that affected a significant number of units or those related to serious injuries or fatalities.

4 Note to **RT-AE-250a.3** – The entity shall discuss notable Airworthiness Directives, such as those that resulted in an Emergency Airworthiness Directive, affected a significant number of products, or were associated with plane groundings or accidents.

5 Note to **RT-AE-250a.4** – 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
Materials Sourcing	Description of the management of risks associated with the use of critical materials	Discussion and Analysis	n/a	RT-AE-440a.1
Business Ethics	Total amount of monetary losses as a result of legal proceedings associated with incidents of corruption, bribery or illicit international trade [6]	Quantitative	Presentation currency	RT-AE-510a.1
	Revenue from countries ranked in the 'E' or 'F' Band of Transparency International's Government Defence Anti-Corruption Index	Quantitative	Presentation currency	RT-AE-510a.2
	Discussion of processes to manage business ethics risks throughout the value chain	Discussion and Analysis	n/a	RT-AE-510a.3

Table 2. Activity Metrics

ACTIVITY METRIC	CATEGORY	UNIT OF MEASURE	CODE
Production by reportable segment[7]	Quantitative	Number	RT-AE-000.A
Number of employees	Quantitative	Number	RT-AE-000.B

[6] Note to **RT-AE-510a.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, bribing an official) of all monetary losses resulting from legal proceedings.

[7] Note to **RT-AE-000.A** – Production should be disclosed as the number of units produced by product category, where relevant product categories include (1) ground vehicles, (2) aircraft, (3) marine vehicles, (4) vehicle and aircraft components and (5) space and weapons systems.

Energy Management

Topic Summary

Energy is a critical input to aerospace and defence manufacturing processes. Purchased electricity is the largest share of the industry's energy expenditures, followed by purchased fuels. The type of energy used, magnitude of consumption and energy management strategies depend on the type of products manufactured. An entity's energy mix, including electricity generated on-site, grid-sourced electricity and alternative energy, may influence the cost and reliability of energy supply and, ultimately, affect the entity's cost structure and regulatory risk.

Metrics

RT-AE-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 that is outside of 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).

Hazardous Waste Management

Topic Summary

Aerospace and defence product manufacturing may generate hazardous process waste, which may include heavy metals and wastewater treatment sludge. Entities face regulatory and operational challenges in managing waste, since some wastes are subject to regulations pertaining to their transport, treatment, storage and disposal. Waste management strategies include reduced generation, effective treatment and disposal, and recycling and recovery, when possible. Such activities, although requiring initial investment or operating costs, may reduce an entity's long-term cost structure and mitigate remediation liabilities or regulatory penalties.

Metrics

RT-AE-150a.1. (1) Amount of hazardous waste generated, (2) percentage recycled

1 The entity shall calculate and disclose (1) the total weight of hazardous waste generated, in metric tonnes.

1.1 Hazardous wastes are defined in accordance with the applicable jurisdictional legal or regulatory frameworks where the waste was generated.

2 The entity shall disclose (2) the percentage of hazardous waste recycled, which is calculated as the weight of hazardous waste generated that was recycled, divided by the total weight of hazardous waste generated.

2.1 Hazardous waste that is reused, reclaimed or remanufactured shall be considered within the scope of recycled.

2.2 Recycled, reused, reclaimed and remanufactured hazardous waste is defined in accordance with the applicable jurisdictional legal or regulatory frameworks where the waste was generated.

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

2.3.1 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.

2.3.2 The entity may choose to separately disclose the percentage of hazardous waste generated that was incinerated.

3 The entity may use the United Nations Environmental Programme (UNEP) *Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and their Disposal* for the purposes of defining hazardous waste or recycled hazardous waste for operations located in jurisdictions that lack applicable legal or regulatory definitions.

4 The entity shall disclose the frameworks used to define hazardous waste and recycled hazardous waste, and the amounts and percentages defined in accordance with each applicable framework.

RT-AE-150a.2. (1) Number and aggregate quantity of reportable spills, (2) quantity recovered

1 The entity shall disclose (1) the total number and quantity (in kilogrammes) of reportable spills, where:

1.1 Reportable spills are defined as any release of a hazardous substance in an amount greater than or equal to the threshold required to be reported to applicable jurisdictional legal or regulatory authorities.

1.1.1 Hazardous substance is defined as a substance or material that an applicable jurisdictional legal or regulatory authority has determined may pose an unreasonable risk to health, safety and property and has been designated as hazardous in accordance with applicable jurisdictional hazardous materials law.

1.1.2 The scope of hazardous substances includes hazardous materials, hazardous wastes, marine pollutants, elevated temperature materials and materials designated as hazardous by the applicable jurisdictional, legal and regulatory framework(s) where the materials are generated.

1.1.3 The entity may use definitions of hazardous waste from the United Nations Environment Programme (UNEP) *Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and their Disposal*.

1.2 The number of reportable spills shall include any leaks, emissions, discharges, injections, disposals and abandonment releases over time, counted once at the time identified.

1.3 The aggregate quantity reported shall represent the total quantity of material released to the environment, and it shall not be reduced by the amount of such hazardous substances that are subsequently recovered, evaporated or otherwise lost.

1.4 The scope of the disclosure includes all spills, across all jurisdictions in which the entity operates.

2 The entity shall disclose (2) the quantity of spills recovered, which is calculated as the quantity of spilled hazardous substances (in kilogrammes) removed from the environment through short-term (less than one year from time of spill) release response activities, excluding:

2.1 amounts recovered during longer-term (more than one year from time of spill) remediation at spill sites; and

2.2 amounts evaporated, burned or dispersed.

3 The entity may disclose releases to soil and water separately.

3.1 A release that qualifies as a release to both soil and water may be reported as a single release to water, with the quantity of the release properly apportioned to soil and water.

Note to **RT-AE-150a.2**

1 If applicable, the entity shall discuss its activities to remediate spills that occurred in years prior to the reporting period but for which remediation activities are ongoing and long-term.

2 Relevant activities may include land-use controls, site monitoring, site maintenance and continued clean-up.

Data Security

Topic Summary

Entities in the Aerospace & Defence industry may develop sensitive military and advanced aviation products, and entities in this industry therefore may be at risk for cyber-attacks. A data security breach may be costly for an entity and its clients when information systems are compromised. Ensuring data security may require aerospace and defence entities to invest in research and development and increase capital expenditures in the short to medium term to improve the security of systems and products. Significant or frequent disruptions or security breaches may result in regulatory action, legal action, or adversely affect revenues and brand value.

Metrics

RT-AE-230a.1. (1) Number of data breaches, (2) percentage involving confidential information

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

1.1 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 in which confidential information was subject to the data breach, where confidential information includes confidential business information, classified national security information and personal data.

2.1 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 have the effect of causing substantial harm to the competitive position of the person, partnership or entity from which the information was obtained.

2.2 Classified national security information is defined pursuant to applicable jurisdictional laws or regulations.

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

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 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 **RT-AE-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.

RT-AE-230a.2. Description of approach to identifying and addressing data security risks in (1) entity operations and (2) products

1 The entity shall describe its approach to identifying information system vulnerabilities within (1) entity operations and, separately, (2) its products 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, products, 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 data security risks and vulnerabilities separately for (1) entity operations and (2) products.

2.1 In the discussion of data security risks in (1) operations, the entity shall describe its approach to managing identified data security risks and vulnerabilities which may include operational procedures, management processes, selection of business partners, employee training and use of technology.

2.2 In its discussion of data security risks in (2) products, the entity shall include a discussion of all stages of the product lifecycle, as relevant, such as product design, the manufacturing supply chain, product distribution, the product use-phase and end-of-life management.

2.2.1 Examples of data security risks in the supply chain may include weaknesses in supplier information systems, risk of 'backdoors' being inserted into products, or counterfeit products, components or parts that present a data security risk.

2.2.2 Examples of approaches to address data security risks in the manufacturing supply chain may include hardware-based security considerations integrated into the product design and development process, management systems required of suppliers, the use of cybersecurity specialists, 'ethical hacking', and supply chain controls.

3 The entity shall discuss how it manages data security flaws, bugs and systems weaknesses detected in its products after product distribution and use.

3.1 The disclosure may include a discussion of the effects of such incidents, including costs for remediation and impacts on future business.

3.2 The disclosure may include a discussion of the management process for corrective actions.

4 If relevant, the entity may describe its products and services that specifically enable enhanced data security for customers, or features it integrates into existing products to specifically enhance data security.

4.1 Examples of security-related products and services include hardware-based encryption products, multi-factor authentication devices (such as security tokens or biometric scanners), information assurance systems, secure communications systems, intelligence-driven computer network defence systems, penetration testing and threat monitoring.

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

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

6.1 the ISO/IEC 27000 series; and

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

7 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 Safety

Topic Summary

Product safety is an important consideration for aerospace and defence entities given the industry's important role in commercial aviation and military operations. Product safety incidents could result in financial impacts, including increased costs, regulatory penalties or brand-value impacts that could affect market share adversely. Additionally, counterfeit components have been found in the aerospace and defence supply chain, increasing the risk of safety incidents because of low product quality. Through product design, supplier vetting and customer engagement involving maintenance and accident investigations, entities in this industry may ensure the safety of their products over the long term, mitigating potential financial consequences such as revenue loss because of repeated safety incidents or recalls.

Metrics

RT-AE-250a.1. (1) Number of recalls issued, (2) total units recalled

1 The entity shall disclose (1) the total number of product-safety-related recalls it issued, including voluntary and involuntary recalls.

1.1 A recall is defined as any repair, replacement, refund or notice/warning program intended to protect consumers from products that present a safety risk.

1.2 Involuntary recalls are those requested or mandated by applicable jurisdictional legal or regulatory agencies, and they are issued when a product does not comply with regulatory safety standards or when a safety-related defect in a product is identified.

1.3 Voluntary recalls are those initiated by the entity to remove products from the market for safety-related concerns.

2 The entity shall disclose (2) the total number of units recalled during the reporting period.

3 The scope of the disclosure excludes products provided to customers for the explicit purpose of testing, such as those products created for prototype testing related to governmental contracts.

4 The entity may separately disclose the percentage of recalls that were (a) voluntary and (b) involuntary.

Note to **RT-AE-250a.1**

1 The entity shall discuss notable recalls, such as those that affected a significant number of products or those related to potential or actual serious injuries or fatalities.

1.1 A recall may be considered notable if it is mentioned in periodic jurisdictional recall reports.

2 For such recalls, the entity may provide:

2.1 corrective actions;

2.2 description and cause of the recall issue;

2.3 total cost to remedy the issue;

2.4 total number of units recalled;

2.5 whether the recall was voluntary or involuntary; and

2.6 other significant outcomes (for example, legal proceedings or fatalities).

RT-AE-250a.2. (1) Number of counterfeit parts detected, (2) percentage avoided

1 The entity shall disclose (1) the total number of counterfeit parts or suspected counterfeit parts detected in its operations, in which:

1.1 Counterfeit parts are defined as an unlawful or unauthorised reproduction, substitution or alteration knowingly mismarked, misidentified or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorised aftermarket manufacturer. Unlawful or unauthorised substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code or performance characteristics.

1.2 Suspect counterfeit electronic parts are defined as an electronic part for which credible evidence (including visual inspection or testing) provides reasonable doubt that the electronic part is authentic.

1.3 The number of counterfeit parts detected includes those of which the entity, its business partners, or its customers become aware, or any electronic part or end item, component, part, or assembly that gives the entity, its business partners or its customers any reason to suspect it contains counterfeit electronic parts.

1.4 The scope of the disclosure includes: those parts detected before procurement, and therefore avoided; those detected during manufacturing, assembly and testing; and those detected after sale to the entity's customer(s).

2 The entity shall disclose (2) the percentage avoided, which is calculated as the number of counterfeit or suspect counterfeit parts detected prior to the sale and delivery of the part to a customer divided by the total number of counterfeit or suspect counterfeit parts detected, in which:

2.1 detection prior to sale and delivery includes any counterfeit or suspect counterfeit part detected during procurement, manufacturing, assembly or testing and counterfeit or suspect counterfeit parts not purchased by the entity but could have been purchased, except that they were detected.

3 The entity may discuss at which point it detected the counterfeit parts (for example, whether the parts were detected by the entity's business partners, the entity's testing systems prior to production or after production, or if the entity was notified by customers).

4 The entity may discuss its compliance with the provisions of the SAE International Standard, SAE AS5553 C*ounterfeit Electrical, Electronic Parts, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition*.

RT-AE-250a.3. (1) Number of Airworthiness Directives received, (2) total units affected

1 The entity shall disclose (1) the number of unique Airworthiness Directives received from aviation authorities and the total number of units affected, in which:

1.1 an Airworthiness Directive is a legally enforceable rule issued under applicable jurisdictional laws or regulations that apply to aircraft, aircraft engines, propellers and appliances.

2 The entity shall disclose (2) the total number of units affected by each Airworthiness Directive, in which:

2.1 the total number of units affected is defined as the combined quantity of products and parts subject to part of any Airworthiness Directive that the entity received during the reporting period.

Note to **RT-AE-250a.3**

1 The entity shall discuss notable Airworthiness Directives, such as those that resulted in an Emergency Airworthiness Directive, affected a significant number of products or were associated with plane groundings or accidents.

2 For such Airworthiness Directives, the entity may provide:

2.1 a description and cause of the issue;

2.2 corrective actions;

2.3 cost to remedy the issue;

2.4 total number of units affected; and

2.5 any other significant outcomes (for example, legal proceedings or fatalities).

RT-AE-250a.4. Total amount of monetary losses as a result of legal proceedings associated with product safety

1 The entity shall disclose the total amount of monetary losses incurred during the reporting period resulting from legal proceedings associated with product safety.

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 or 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 **RT-AE-250a.4**

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, violation of safety standards) of all monetary losses resulting from legal proceedings.

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

Fuel Economy & Emissions in Use-phase

Topic Summary

Customer preferences and regulatory incentives are increasing the demand for energy-efficient and reduced-emissions products in the Aerospace & Defence industry. Many of the industry's products are powered by fossil fuels and release greenhouse gases (GHGs) and other air emissions during use. As the designers and manufacturers of most of the global aerospace and defence transportation fleet, entities in this industry have a unique opportunity to support many industries and government agencies that are striving to meet GHG emissions and fuel-management goals and imperatives. Products with higher fuel economy and lower use-phase emissions may capture expanding market share and adapt to changing customer preferences and regulations around fuel economy and emissions more effectively.

Metrics

RT-AE-410a.1. Revenue from alternative energy-related products

1 The entity shall disclose total revenue from the sale of alternative energy-related products, where:

1.1 Alternative energy-related products include products such as vehicles, vehicle components and stationary power generation equipment that rely on alternative fuel or energy as a primary means of propulsion or energy production.

1.2 Alternative energy and fuel includes:

1.2.1 Renewable fuel and energy, which is defined as deriving from sources capable of being replenished quickly through ecological cycles, such as geothermal, wind, solar, hydroelectric and biomass (including ethanol, first-generation biofuels and advanced biofuels)

1.2.2 Hydrogen fuel and fuel cells including those that operate using natural gas, propane and methanol

1.3 Electric, hybrid electric and dual-fuelled products for which one of the fuel sources is an alternative fuel shall be considered within the scope of disclosure.

RT-AE-410a.2. Description of approach and discussion of strategy to address fuel economy and greenhouse gas (GHG) emissions of products

1 The entity shall describe its approach and discuss its strategies for improving the fuel economy and reducing the use-phase greenhouse gas (GHG) emissions of its products.

2 Relevant aspects of the approach and strategy include improvements to existing products and technologies, the introduction of new technologies, research and development efforts into advanced technologies, and partnerships with peers, academic institutions or customers (including governmental customers).

3 Relevant technologies to describe may include those related to materials design and engineering, advanced powertrains, renewable fuels, energy storage and batteries, aerodynamic design, and products and fuels that otherwise result in reduced GHG emissions, where:

3.1 Advanced powertrain technologies include vehicles and vehicle components that are electric, hybrid electric, plug-in hybrid, dual-fuel and zero-emissions (for example, fuel cell).

3.2 Renewable fuels and energy technologies are those that operate on sources capable of being replenished quickly through ecological cycles, including geothermal, wind, solar, hydroelectric and biomass (including ethanol, first-generation biofuels and advanced biofuels).

3.3 Products that result in reduced GHG emissions include any vehicle or technology that achieves a significant reduction in petroleum consumption as well as advanced lean burn technology vehicles and technologies.

3.4 Fuels that result in reduced GHG emissions further include denatured alcohol, methanol, mixtures containing up to 85% methanol or denatured ethanol, natural gas and propane (liquefied petroleum gas).

3.5 If relevant, the entity shall discuss the technologies it is prioritising to improve the fuel economy and reduce the GHG emissions of its products, such as the specific type of fuel systems it is developing (for example, hybrid, electric or fuel cell).

4 The entity shall describe the factors influencing these efforts, such as meeting civil customer demand, alignment with industry initiatives, or meeting requirements of federal procurement programmes and initiatives, in which:

4.1 Relevant programmes and initiatives to describe include the International Civil Aviation Organization Resolution A38-18.

5 The entity may describe the benchmarks used to measure product fuel efficiency improvements for relevant vehicles or vehicle system segments, including a description of targets for fuel efficiency improvements.

6 The entity may provide measurements of fuel efficiency and fuel efficiency improvements for its relevant vehicle or vehicle systems segments.

6.1 Measurements of fuel efficiency and fuel efficiency improvements may include:

6.1.1 Inherent fuel efficiency measurements, such as miles per gallon for vehicles and vessels and 1/ Specific Air Range for aerospace vehicles

6.1.2 Year-over-year fuel efficiency improvements

7 The entity may discuss how customer demand and requirements affect fuel efficiency measures and improvements, if relevant.

Materials Sourcing

Topic Summary

Aerospace and defence entities are exposed to supply chain risks when critical materials are used in products. Entities in the industry manufacture products using critical materials with few or no available substitutes, many of which are sourced from only a few countries that may be subject to geopolitical uncertainty. Entities in this industry also face increasing global demand for these materials from other sectors, which may result in price increases and supply risks. Entities that limit the use of critical materials by using alternatives and securing their supply may mitigate the financial impacts stemming from supply disruptions and volatile input prices.

Metrics

RT-AE-440a.1. Description of the management of risks associated with the use of critical materials

1 The entity shall describe how it manages the risks associated with the use of critical materials in its products, including physical limits on availability and access, changes in price, and regulatory and reputational risks, in which:

1.1 a critical material is defined as a material both essential in use and subject to the risk of supply restriction; and

1.2 examples of critical materials may include:

1.2.1 antimony, cobalt, fluorspar, gallium, germanium, graphite, indium, magnesium, niobium, tantalum and tungsten;

1.2.2 platinum group metals (platinum, palladium, iridium, rhodium, ruthenium and osmium);

1.2.3 rare earth elements, which include yttrium, scandium, lanthanum and the lanthanides (cerium, praseodymium, neodymium, promethium, samarium, europium, gadolinium, terbium, dysprosium, holmium, erbium, thulium, ytterbium and lutetium); and

1.2.4 materials with a risk of shortfall in defence-related applications, such as tin, aluminium oxide-fused crude, silicon carbide, bismuth, manganese metal electrolytic, beryllium metal and chromium metal.

2 The entity shall identify the critical materials that present a significant risk to its operations, the type of risks they represent and the strategies the entity uses to mitigate the risks.

2.1 Relevant strategies may include diversification of suppliers, stockpiling of materials, development or procurement of alternative and substitute materials, and investments in recycling technology for critical materials.

3 All disclosure shall be sufficient such that it is specific to the risks the entity faces, but that disclosure itself would not compromise the entity's ability to maintain confidential information.

3.1 For example, if an entity determines not to identify a specific critical material that presents a significant risk to its operations because of the competitive harm that could result from the disclosure, the entity shall disclose the existence of such risks, the type of risks and the strategies used to mitigate the risks, but the entity is not required to disclose the relevant critical material.

Business Ethics

Topic Summary

Aerospace and defence entities based in jurisdictions with stronger business ethics laws may be vulnerable to regulatory scrutiny of their business ethics because of operations and sales in regions with weaker government enforcement of business ethics laws. Entities in this industry have been found in violation of corruption and anti-bribery laws. Unethical practices may jeopardise future revenue growth and may result in significant legal costs and higher reputational risk. As such, strong governance practices may mitigate the risk of violating business ethics laws and resulting regulatory penalties or brand-value impacts.

Metrics

RT-AE-510a.1. Total amount of monetary losses as a result of legal proceedings associated with incidents of corruption, bribery or illicit international trade

1 The entity shall disclose the total amount of monetary losses incurred during the reporting period resulting from legal proceedings associated with incidents of corruption, bribery or illicit international trade.

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 or 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 **RT-AE-510a.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, bribing an official) of all monetary losses resulting from legal proceedings.

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

RT-AE-510a.2. Revenue from countries ranked in the 'E' or 'F' Band of Transparency International's Government Defence Anti-Corruption Index

1 The entity shall disclose the amount of revenue from countries scored in the 'E' or 'F' Band of Transparency International's *Government Defence Anti-Corruption Index*.

1.1 Transparency International's Government Defence Anti-Corruption Index defines bands E and F respectively, as having 'Very High' and 'Critical' levels of risk of corruption.

2 The entity shall prepare its disclosure according to the scoring in the most current available version of the Government Defence Anti-Corruption Index at the close of its reporting period via Transparency International's publicly accessible website.

3 The entity may provide discussion around operations located in countries with E or F scores in the index but that present low business ethics risks. The entity may provide similar discussion for operations located in countries not scored in the E or F Band of the index but that present unique or high business ethics risks.

RT-AE-510a.3. Discussion of processes to manage business ethics risks throughout the value chain

1 The entity shall discuss its processes and due diligence procedures for assessing and managing risks relating to business ethics within the scope of its own operations and those associated with business partners in its value chain.

2 Relevant processes to discuss may include:

2.1 anti-corruption policies;

2.2 employee awareness programmes;

2.3 internal mechanisms for reporting and following up on suspected violations; and

2.4 participation in the International Forum on Business Ethical Conduct (IFBEC).

3 Relevant business ethics risks include bribery and illicit arms trade, as regulated by applicable jurisdictional laws or regulations.

4 Relevant business partners include customers, suppliers, contractors, subcontractors and joint-venture partners.

5 The entity shall discuss areas of its operations at the highest risk for corruption and bribery, such as those operations in countries with low rankings in Transparency International's *Government Defence Anti-Corruption Index*.

6 The entity may discuss the implementation of the:

6.1 Defence Industry Initiative (DII) on Business Ethics and Conduct principles;

6.2 International Chamber of Commerce (ICC) *Rules of Conduct and Recommendations to Combat Extortion and Bribery*;

6.3 Organisation for Economic Co-operation and Development (OECD) anti-corruption guidelines;

6.4 TRACE International guidelines;

6.5 Transparency International *Business Principles for Countering Bribery*;

6.6 United Nations Global Compact 10th Principle; and

6.7 World Economic Forum (WEF) Partnering Against Corruption Initiative (PACI).

SASB STANDARDS

Now part of IFRS Foundation