CONDUENT

2019 SASB Disclosure Table

The Sustainability Accounting Standards Board (SASB) is an independent standards-setting organization dedicated to enhancing the efficiency of the capital markets by fostering high-quality disclosure of financially material sustainability information that meets investor needs. The following table references the Standard for the Software and IT Services industry, as defined by SASB's Sustainable Industry Classification System™ (SICS™), and Conduent's SASB-aligned responses. The data contained herein is as of 12/31/2019.

Topic	Accounting Metric	SASB Code	2019 Disclosure	Additional Comments
Environmental Footprint of Hardware Infrastructure	(1) Total energy consumed, (2) percentage grid electricity, (3) percentage renewable	TC-SI-130a.1	(1) 386,951 GJ energy consumed at 98 sites (2) 100% grid electricity	The company gathered this data using a Capturis system, which utilizes the EPA's eGrid 2018 (Version release 03/09/2020) methodology. The company started the year with 260 sites and ended the year with 208 sites. This data captures 98 sites located in the US-only (some of which are no longer in operational). The data excluded international sites and sites in which utilities are paid directly through the landlord.
	(1) Total water withdrawn, (2) total water consumed, percentage of each in regions with High or Extremely High Baseline Water Stress	TC-SI-130a.2	See additional comment	Water consumption information is not available at this time, as it is not a primary input to Conduent's provided services.
	Discussion of the integration of environmental considerations into strategic planning for data center needs	TC-SI-130a.3	See additional comment	Conduent is committed to taking the appropriate actions to better control our environmental impact. As a result, we have integrated environmental considerations into our strategic planning for data center needs, which include: 1. Using Data Center Infrastructure Management (DCIM) Software to manage data centers energy use 2. Installing BMS system and/or upgrade existing BMS systems in place of having Energy Management software/modules 3. Automating power metering at the device level 4. Leveraging variable speed drives to match energy usage to workload 5. Using alternative cooling methods such as free cooling and direct liquid cooling 6. Matching infrastructure power use to IT workload after virtualization 7. Eliminating "zombie" servers (unused, but powered servers) 8. Benchmarking to track performance over time 9. Purchasing green IT to reduce a facility's energy footprint 10. Developing disaster recovery plans and security awareness curriculums to protect physical and virtual assets 11. Increasing automation capabilities to improve uptime

Data Privacy & Freedom of Expression	Description of policies and practices relating to behavioral advertising and user privacy	TC-SI-220a.1	Conduent's privacy and behavioral advertising policy	
	Number of users whose information is used for secondary purposes	TC-SI-220a.2	0	
	Total amount of monetary losses as a result of legal proceedings associated with user privacy	TC-SI-220a.3	The company's total amount of monetary losses as a result of legal proceedings associated with user privacy is 0.	Additional information on legal proceedings is disclosed in our Annual Report on Form 10-K.
	(1) Number of law enforcement requests for user information, (2) number of users whose information was requested, (3) percentage resulting in disclosure	TC-SI-220a.4	See additional comment	As a “Business-to-Business” provider supporting our clients' end customers, Conduent does not receive requests for user information except in its capacity as a service provider for our client’s customers.
	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring	TC-SI-220a.5	0	

Data Security	(1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of users affected	TC-SI-230a.1	See additional comment	Conduent routinely processes significant volumes of data (including PII and PHI) for a broad, diversified global customer base. Accordingly, we are periodically subjected to unauthorized attempts to compromise or acquire data. To protect Conduent and our customers, we do not broadly disclose specifics regarding these attempts other than in instances where we are legally required to do so. We maintain an information security program that is aligned with the NIST framework and standards as well as applicable industry regulatory requirements. The program is continuously reviewed and strengthened as necessary to ensure responsiveness to and protection against actual and emerging threats.
	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	TC-SI-230a.2	Conduent's security program is aligned with the NIST framework and standards as well as applicable industry regulatory requirements, including but not limited to GDPR, HIPAA, ISO, and PCI. The program encompasses information security and cyber operations capabilities that protect Conduent and our clients. It is continuously reviewed and strengthened as necessary to ensure responsiveness to and protection against emerging threats. Conduent maintains a highly qualified workforce and utilizes external experts to support the program. We administer internal education, training, and communication programs to ensure ongoing awareness and vigilance. We maintain and communicate formal documented policies and standards. We monitor and assess the overall operating effectiveness of our program through risk assessments that include identification and remediation of vulnerabilities and threats. We maintain and test our cyber incident response plan, and undertake various independent reviews in conjunction with PCI DSS, external audits, internal audits and client assurance efforts. Various additional operational protections, controls and processes exist, including but not limited to malware protection, intrusion prevention and detection protocols, user access reviews, network segmentation, implementation and maintenance of network and application firewalls, vulnerability scanning, data encryption, penetration testing and patching.	

			Additionally, you can find our privacy policy here: https://www.conduent.com/privacy-policy/	

Recruiting & Managing a Global, Diverse & Skilled Workforce	Percentage of employees that are (1) foreign nationals and (2) located offshore	TC-SI-330a.1	(1) 1.12% of US employees on Visa (2) 55.31% of Total Conduent Employees located offshore	
	Employee engagement as a percentage	TC-SI-330a.2	See additional comment	Conduent conducted an enterprise-wide employee engagement survey in 2018 and 2020. Information will be disclosed, as appropriate, in the 2020 Corporate Social Responsibility Report.
	Percentage of gender and racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees	TC-SI-330a.3	<table><tr><th>Level</th><th>Female</th><th>Male</th><th>Not Disclosed</th></tr><tr><td>Management</td><td>50%</td><td>50%</td><td>0%</td></tr><tr><td>Technical Staff</td><td>31%</td><td>69%</td><td>0%</td></tr><tr><td>All Other Employees</td><td>75%</td><td>25%</td><td>0%</td></tr></table><table><tr><th>Level</th><th>Asian</th><th>Black or African American</th><th>Hispanic or Latino</th><th>White</th><th>Other</th><th>Not Disclosed</th></tr><tr><td>Management</td><td>9%</td><td>16%</td><td>10%</td><td>53%</td><td>2%</td><td>9%</td></tr><tr><td>Technical Staff</td><td>25%</td><td>7%</td><td>6%</td><td>49%</td><td>2%</td><td>12%</td></tr><tr><td>All Other Employees</td><td>3%</td><td>34%</td><td>15%</td><td>22%</td><td>4%</td><td>20%</td></tr></table>	Gender and racial/ethnic data for US based employees only; categories defined by SASB definitions.

Intellectual Property Protection & Competitive Behavior	Total amount of monetary losses as a result of legal proceedings associated with anticompetitive behavior regulations	TC-SI-520a.1	The company's total amount of monetary losses as a result of legal proceedings associated with anticompetitive behavior regulations is 0.	Additional information on legal proceedings is disclosed in our Annual Report on Form 10-K.

Managing Systemic Risks from Technology Disruptions	Number of (1) performance issues and (2) service disruptions; (3) total customer downtime	TC-SI-550a.1	See additional comment	For competitive and security reasons, we chose not to disclose this information at this time. Conduent continuously improves the quality of our solutions and services to maximize uptime and performance.

	Description of business continuity risks related to disruptions of operations	TC-SI-550a.2	Conduent is committed to meeting client, regulatory and stakeholder requirements and expectations, including in instances when business disruption occurs. Accordingly, Conduent maintains Business Continuity, Disaster Recovery and Information/Cyber Security programs with frameworks and methodologies designed to effectively manage business continuity risk. Conduent follows and adheres to ISO 22301 and NIST 800-53 standards as well as Information Technology Infrastructure Library (ITIL) processes. The Business Continuity Management Policy and Standards outline the mandates and minimum requirements that business units must follow to plan for and respond to disruptive events. Business continuity is underpinned by processes and procedures to help ensure the stability of our technology environments. The Disaster Recovery policy and procedures ensure compliance with client contracts and internal standards. Cyber Security policies, protocols and assessments are designed to protect sensitive information and enable effective response to cyber or security threats. Our programs are designed to create a resilient operating environment with preplanned response and recovery strategies in the event of business disruption. These strategies focus on safeguarding our people, assets, information, and clients.	