

CSG Systems Sustainability Accounting Standards Board Index



Table of Contents

About Us.....	3
Reporting Overview.....	3
SASB Disclosures.....	4
Cautionary Statement Regarding Forward-Looking Statements & Disclaimers	14



About Us

CSG is a leader in innovative customer engagement, revenue management and payments solutions that make ordinary customer experiences extraordinary. Our cloud-first architecture and customer-obsessed mindset help companies around the world launch new digital services, expand into new markets, and create dynamic experiences that capture new customers and build brand loyalty. For 40 years, CSG's technologies and people have helped some of the world's most recognizable brands solve their toughest business challenges and evolve to meet the demands of today's digital economy with future-ready solutions that drive exceptional customer experiences. With 5,000 employees in over 20 countries, CSG is the trusted technology provider for leading global brands in telecommunications, retail, financial services, and healthcare. Our solutions deliver real world outcomes to more than 900 customers in over 120 countries.

Reporting Overview

This document outlines CSG's Environmental, Social & Governance ("ESG") disclosure of the Value Reporting Foundation's Sustainability Accounting Standards Board ("SASB"). CSG is a member of the Technology & Communications sector in the Software & IT services industry as defined by SASB's Sustainable Industry Classification System ("SICS"). The information contained within is dated as of the end of our Fiscal Year (December 31, 2021) unless otherwise noted. For more information on CSG's ESG program, please visit: <https://ir.csgi.com/investors/ESG/default.aspx>

SASB CODE	DESCRIPTION	DISCLOSURE
Environment		
Energy Management		
TC-SI-130a.3	Discussion of the integration of environmental considerations into strategic planning for data center needs.	<p>Describe the integration of environmental considerations into strategic planning for data centers: CSG's strategic planning considers environmental aspects when selecting and monitoring data center providers hosting CSG's global workloads for both internal enterprise as well as Software-as-a-Service ("SaaS") solutions hosting that CSG provides to its customers at each location. Energy efficiency, as well as the sources of energy supplying CSG's data centers, is reviewed based on the geographic location during provider selection and at periodic intervals during the relationship to ensure alignment of results to our original strategic plan.</p> <p>Discuss how environmental factors impact decisions regarding the siting, design, construction, refurbishment, and operations of data centers: CSG continually partners with our suppliers of data center and hosting services supporting our enterprise and SaaS hosting solutions globally on the energy efficiency of their data centers and all infrastructure components within, sourcing of power, modern cooling systems, and contemporary efficiency design principles.</p> <p>Discuss considerations for existing owned data centers, development of new data centers, and outsourcing of data center services: CSG continually partners with our data center providers and hosting services supporting our enterprise and SaaS solutions globally on the energy efficiency of their data centers and all infrastructure components within, sourcing of power, modern cooling systems, and contemporary efficiency design principles.</p> <p>Discuss how the environmental considerations you identified were incorporated into decisions related to data centers that were made during the reporting period: CSG has modernized multiple global locations with foresight into energy consumption and efficiencies by deploying the latest generations of power efficient network, storage, and compute infrastructure components. CSG continues to review and relocate workloads to more energy efficient facilities and providers.</p>

Social Capital		
Customer Privacy		
TC-SI-220a.1	Description of policies and practices relating to behavioral advertising and customer privacy.	<p>Describe the nature, scope, and implementation of policies and practices related to customer privacy, with a focus on how you address the collection, usage, and retention of customer information:</p> <p>The nature and scope of CSG's privacy policies and practices are established to maintain a comprehensive and global privacy program that includes all the legal requirements of applicable law for each applicable territory.</p> <p>To implement the privacy program, CSG has internal privacy and security policies and practices that are an integral component of CSG's code of conduct. CSG provides annual privacy and security awareness training to employees and within 90 days of start date for new hires.</p> <p>CSG collects, uses and retains customer information in accordance with the applicable agreement with the customer, applicable law and its internal policies and processes.</p> <p>Describe the information "lifecycle" and how handling at each stage affect individual's privacy:</p> <p>CSG has a comprehensive approach to information handling and to prevent the compromise or misuse of CSG's information, applications, networks and computer systems. CSG has a process in place for categorizing information types and defining how they are protected, commensurate with their business value and impact. With regards to the customer lifecycle, once CSG receives consent from a customer to provide CSG with personally identifiable information, CSG then employs a rigorous information protection sequence that consists of: (1) classifying the information, (2) proper handling of that information, (3) adequately retaining that information for a proper amount of time and (4) the possible destruction of that information at an appropriate time.</p> <p>This applies to entities or individuals with access to information controlled or processed by CSG. This includes CSG entities, employees, contingent workers, contractors as well as external parties, including but not limited to CSG business partners, vendors, suppliers, and outsource service providers. This standard applies to all information controlled or processed by CSG.</p> <p>All information is protected according to the requirements set for each classification in accordance with policies and practices and monitored by information owners. The information classification and its level of protection will be consistent when the information is reproduced as it flows through CSG.</p> <p>Information owners must determine the information classification and must ensure that the information custodian is protecting the information in a manner appropriate to its classification.</p> <p>No CSG-owned system or network may connect to the internet without the means to protect the information on those systems consistent with its information classification. High-impact information is not retained in any public zone. Protected health information, credit card numbers, or other account numbers are</p>

		<p>not stored on a server connected to the internet. Cardholder data is retained as needed and defined per CSG's clients, in a configurable fashion until the client decides to add, modify or delete individual Primary Account Number (PAN) or entire accounts to meet their business requirements.</p> <p>Information owners are responsible for creating information repositories and data transfer procedures, which protect information in the manner appropriate to its classification.</p> <p>All appropriate information is backed up, and the backups tested periodically, as part of a documented regular process. Backups of data must be handled with the same security precautions as the data itself.</p> <p>When systems are disposed of, or repurposed, data must be certified deleted, or disks destroyed consistent with industry best practices based on the classification of the information.</p> <p>These processes must comply with CSG's Data Retention and Destruction Policy.</p> <p>CSG maintains a data subject request portal for individuals to inquire and/or request information, access, deletion or modification of information. Data subject requests are processed according to the requirements under applicable law and CSG's internal policies and processes.</p> <p>Discuss policies and practices related to children's privacy, including relations to COPPA:</p> <p>CSG does not knowingly collect or solicit personal information of anyone under the age of 18. CSG maintains a code of business conduct that outlines CSG's expectations for employees and contractors.</p> <p>Discuss how behavioral advertising is addressed, using the Self-Regulatory Principles for Online Behavioral Advertising:</p> <p>CSG includes its cookie policy in its website privacy notice which is in accordance with applicable privacy laws (i.e. the GDPR). For users of CSG's website, csgi.com, CSG or third parties may place advertising cookies on a user's computer or mobile device to enable third party ad networks to recognize a unique cookie. The information that is collected and shared by these types of cookies may also be linked to the device identifier of the device users are using to allow us to keep track of all the websites users have visited that are associated with the ad network. This information may be used for the purpose of targeting advertisements on our website and third-party sites based on those interests.</p> <p>If the cookie lifespan is not disclosed in the cookie settings, we use a default life span of thirteen months, unless a shorter period is required by law.</p>
--	--	---

TC-SI-220a.3	Total amount of monetary losses as a result of legal proceedings associated with customer privacy.	<table><tr><th colspan="2">Reporting Currency: Annual</th></tr><tr><td>Total monetary losses incurred during the reporting period as a result of legal proceedings associated with incidents relating to customer privacy:</td><td>\$0.00</td></tr><tr><td>Monetary losses from adjudicative proceedings in which you were evolved, whether before a court, a regulator, an arbitrator, or otherwise:</td><td>\$0.00</td></tr><tr><td>Monetary liabilities to opposing parties or others, including fines and other monetary liabilities incurred during the reporting period as a result of civil actions, regulatory proceedings, and criminal actions brought by any entity:</td><td>\$0.00</td></tr></table> <p>Additional Comments: CSG has not been involved in any proceeding related to customer privacy resulting in monetary damages during the reporting period.</p>	Reporting Currency: Annual		Total monetary losses incurred during the reporting period as a result of legal proceedings associated with incidents relating to customer privacy:	\$0.00	Monetary losses from adjudicative proceedings in which you were evolved, whether before a court, a regulator, an arbitrator, or otherwise:	\$0.00	Monetary liabilities to opposing parties or others, including fines and other monetary liabilities incurred during the reporting period as a result of civil actions, regulatory proceedings, and criminal actions brought by any entity:	\$0.00
Reporting Currency: Annual										
Total monetary losses incurred during the reporting period as a result of legal proceedings associated with incidents relating to customer privacy:	\$0.00									
Monetary losses from adjudicative proceedings in which you were evolved, whether before a court, a regulator, an arbitrator, or otherwise:	\$0.00									
Monetary liabilities to opposing parties or others, including fines and other monetary liabilities incurred during the reporting period as a result of civil actions, regulatory proceedings, and criminal actions brought by any entity:	\$0.00									
TC-SI-220a.5	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring.	<table><tr><th colspan="2">Government, judicial, or law enforcement content limiting requirements:</th></tr><tr><td>List of the countries where products and services are monitored, blocked, or content is filtered or censored. Include locations where company operations have been discontinued, or were never offered, due to such government activity:</td><td>This is not applicable to CSG. CSG does not have products nor services subject to government-required monitoring, blocking, content filtering or censoring.</td></tr></table> <p>Additional Comments: https://www.csqi.com/company/certifications/</p>	Government, judicial, or law enforcement content limiting requirements:		List of the countries where products and services are monitored, blocked, or content is filtered or censored. Include locations where company operations have been discontinued, or were never offered, due to such government activity:	This is not applicable to CSG. CSG does not have products nor services subject to government-required monitoring, blocking, content filtering or censoring.				
Government, judicial, or law enforcement content limiting requirements:										
List of the countries where products and services are monitored, blocked, or content is filtered or censored. Include locations where company operations have been discontinued, or were never offered, due to such government activity:	This is not applicable to CSG. CSG does not have products nor services subject to government-required monitoring, blocking, content filtering or censoring.									
Data Security										
TC-SI-230a.1	(1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of customers affected.	<p>Describe the corrective actions taken in response to data breaches: CSG has an overarching Incident Management Policy, which is operated by our Chief Information Security Officer ("CISO"), that is used to manage any IT incident no matter how it is reported. A specific set of Security Incident Response procedures are followed if the incident has the potential to be a security issue. These procedures ensure that the appropriate security and technical teams are engaged to evaluate and communicate remediation needs to the Security Incident Response Team including Security, Audit, Legal and Compliance. As part of this process, the Security Team</p>								

		<p>provides an Incident Report that is communicated through this team detailing timelines, business and customer impact, risk, solution/remediation efforts, and security recommendations.</p> <p>Disclose policy for disclosing data breaches to affected customers in a timely manner: CSG's CISO maintains a security program to address data security risks, including the use of third-party cybersecurity standards. CSG takes matters of security very seriously. As such, CSG strives to be as transparent as possible with our customers and consumers regarding security. At a minimum, CSG will follow all contractual, legal, and regulatory requirements for reporting and strives to go above and beyond those requirements whenever possible.</p>
TC-SI-230a.2	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards.	<p>Describe the approach to identifying vulnerabilities in the systems that pose a data security risk: CSG utilizes independent third parties and services, including the best of breed discovery tools, to look at software/applications, network infrastructure and logged traffic to prevent, detect and respond against vulnerabilities.</p> <p>CSG's network security employs 24/7 infrastructure monitoring that leverages industry leading firewalls, network intrusion prevention systems (IDS/IPS), content filtering solutions and application firewalls in a Demilitarized Zone ("DMZ") configuration designed to protect public and private data, and to surveil all traversing network communications.</p> <p>Consolidated log monitoring capabilities are utilized to identify anomalies and security events. Events are derived from multiple areas including network infrastructure (IDS/IPS, firewall, router, switches), operating systems and applications. CSG incorporates enterprise anti-virus software to secure systems and prevent malware spread. A combination of protection and monitoring is performed that includes remotely deployed updates to each system, as well as malware/software reports to a central location for analysis. CSG-owned servers, workstations and email systems are all protected with these controls.</p> <p>CSG also incorporates Product and Services code scanning and vulnerability testing to address concerns in development and post development for CSG's customer offered applications and services. CSG's Vulnerability Management Program oversees this.</p> <p>Describe the approach to addressing identified risks and vulnerabilities related to data security: CSG utilizes a Security Incident Response Team ("SIRT") to manage any security incident. The SIRT and technical teams are organized to evaluate and communicate any forensic or remediation needs to be reviewed and approved by the Chief Information Security Officer ("CISO"). The SIRT also provides an incident report that follows a rigorous MSIRT process, executive oversight and CSG's Audit Committee review which is communicated by the CISO detailing timelines, business and customer impact, risk, solution/remediation efforts and security recommendations.</p>

		<p>Describe the risk management standards for use of third-party cybersecurity: CSG holds third parties to practices and standards that drive CSG's regulatory and self-defined third-party requirements. This is for both the onboarding of a vendor and the vendors continued use by CSG as industry and regulatory items change. CSG's Vendor Program scrutinizes vendors, using a tier system, that is based upon the type of Personally Identifiable Information ("PII") being requested.</p> <p>Discuss observed trends in type, frequency, and origination of data security and information systems attacks: The trend in the last few years has gone from exploiting gaps or vulnerability on the perimeter to more focused user manipulation/exploitation of a company's employees through phishing and ransomware. Malicious intent users look to exploit human nature to gain authorized or undetected access to systems. They then collect and send out data over periods of time to correlate and devise an approach on how to best go after data.</p> <p>Describe the degree to which your approach is aligned with an external standard or framework and/or legal or regulatory framework for managing data security: CSG has a continuous improvement security model and organization led by the Chief Information Security Officer (CISO) and driven by CSG's management team. The model leverages PCI DSS, Privacy laws (including GDPR, HIPAA and ISO-27001) and NIST, and certified against the internationally accepted ISO 27001 security framework.</p> <p>CSG has developed and deployed a CSG Common Control Framework that spans across all current and potentially new frameworks CSG chooses to validate control effectiveness against. These are tested annually by independent assessors and auditors.</p> <p>Additional Comments: All employees, contractors, and contingent workers are required to complete annual Security Awareness training, as well as additional security-centric training pertinent to their specific job roles and any current global events.</p> <p>CSG leverages a Three Lines of Defense model, where control activities are continually performed by operational teams, regularly evaluated by security and governance teams, and, as applicable, reviewed by independent auditors. Penetration testing is performed on critical systems after each release to validate internal and external vulnerability scanning and remediation processes. CSG's Governance and Internal Audit teams perform quarterly and continual monitoring of critical controls, to ensure a consistent level of defense and knowledge base from employees.</p> <p>Annually, external auditors evaluate the effectiveness of critical controls in place for PCI DSS, ISO 27001, SOX and SOCI.</p>
--	--	---

Human Capital																
Employee Engagement, Diversity & Inclusion																
TC-SI-330a.1	Percentage of employees that are (1) foreign nationals and (2) located offshore.	<table><tr><td>Percentage of Employees that are Foreign Nationals (%):</td><td>4%</td></tr><tr><th>Region:</th><th>Percentage of Employees Located Offshore (%):</th></tr><tr><td>APAC</td><td>39%</td></tr><tr><td>CASA</td><td>5%</td></tr><tr><td>EMEA</td><td>10%</td></tr><tr><td>North America</td><td>2%</td></tr><tr><td>Total</td><td>56%</td></tr></table> <p>Additional Comments: We are committed to becoming a globally inclusive organization that is locally relevant to the regions, countries, and areas in which we operate, and have plans within our DEI strategy to develop and nurture approaches to channel the power of all and mature our DEI program. To further our DEI goals, CSG joined the United Nations Global Compact initiative — a voluntary leadership platform for the development, implementation, and disclosure of responsible business practices. At the heart of the Global Compact is a conviction that business practices help the global marketplace be more socially and economically inclusive, and thus advance collective goals of international cooperation, peace, and development.</p>	Percentage of Employees that are Foreign Nationals (%):	4%	Region:	Percentage of Employees Located Offshore (%):	APAC	39%	CASA	5%	EMEA	10%	North America	2%	Total	56%
Percentage of Employees that are Foreign Nationals (%):	4%															
Region:	Percentage of Employees Located Offshore (%):															
APAC	39%															
CASA	5%															
EMEA	10%															
North America	2%															
Total	56%															
TC-SI-330a.2	Employee engagement as a percentage.	<table><tr><td>Employee Engagement Percentage (%):</td><td>79</td></tr></table> <p>Describe the source of your survey, the methodology used to calculate the percentage, and a summary of questions or statements included in the survey or study: CSG uses a third-party provider for employee surveys.</p> <p>The two questions that make up eSat (Employee Satisfaction Score)+ are:</p> <p>1. I would recommend CSG as a great place to work 2. How happy are you working at CSG?</p> <p>What is an Engagement score? Engagement score is calculated by computing the average score for eSat (Employee Satisfaction) and recommend.</p> <p>The overall engagement score has proven to have the highest correlation with the drivers of engagement, along with outcomes such as productivity and retention. This overall score can help Managers understand, at the highest level, how happy their team is at work. The engagement score is where the team's engagement story begins.</p> <p>Understanding how the engagement score is calculated is important. Note that while the survey is on a 5-point scale, you'll see that the reports are converted and distributed on a 100-point</p>	Employee Engagement Percentage (%):	79												
Employee Engagement Percentage (%):	79															

		<p>scale, with 0 as the lowest and 100 as the highest. This is how engagement score is calculated.</p> <p>If results are limited to a subset of employees, include the percentage of employees included in the study or survey, and the representativeness of the sample: Results are for all of CSG with a 92% response rate</p> <p>Additional Comments: In 2021, CSG launched a DEI Meet-Up series that featured internal and external speakers who delivered thought leadership and engaging discussion around a range of topics including Black History Month, International Women's Day, Asian American Pacific Islander Heritage, and Hispanic Heritage Month.</p> <p>Our newly formed Employee Belonging Groups began in 2021 and were formalized in early 2022. These employee-led groups with executive sponsorship offer community, courageous conversation, and awareness activities. They include WE LEaD (supporting women), Pride@CSG (supporting LGBTQ+), and Aspiring Allies (allies supporting underrepresented groups).</p> <p>We are focused on global inclusion with local relevance for over 5,200 employees representing over 20 countries. In 2022 we are launching new DEI training for all employees, a quarterly Inclusion Lab in each of our regions, and dynamic virtual and micro-learning opportunities. In 2021, we hosted our first Inclusive Leadership training for leaders and have expanded that program through 2022 as a DEI Forum that meets quarterly.</p>																																								
TC-SI-330a.3	Percentage of gender representation for (1) management, (2) technical staff, and (3) all other employees.	<p>Additional Comments: Gender in the context of this tool is defined as a binary male or female, or in some jurisdictions known as 'legal sex', other data collection is planned regarding gender identity.</p>																																								
<table><tr><th>US Employees</th><th>Total Employees</th><th>Male</th><th>Female</th><th>Not Disclosed/Available:</th></tr><tr><td>Management:</td><td>563</td><td>64%</td><td>36%</td><td>0</td></tr><tr><td>Technical Staff:</td><td>1019</td><td>69%</td><td>31%</td><td>0</td></tr><tr><td>All Other Employees:</td><td>742</td><td>49%</td><td>51%</td><td></td></tr><tr><th>Non-US Employees</th><th>Total Employees</th><th>Male</th><th>Female</th><th>Not Disclosed/Available:</th></tr><tr><td>Management:</td><td>531</td><td>77%</td><td>23%</td><td></td></tr><tr><td>Technical Staff:</td><td>2063</td><td>66%</td><td>34%</td><td></td></tr><tr><td>All Other Employees:</td><td>316</td><td>51%</td><td>49%</td><td></td></tr></table>			US Employees	Total Employees	Male	Female	Not Disclosed/Available:	Management:	563	64%	36%	0	Technical Staff:	1019	69%	31%	0	All Other Employees:	742	49%	51%		Non-US Employees	Total Employees	Male	Female	Not Disclosed/Available:	Management:	531	77%	23%		Technical Staff:	2063	66%	34%		All Other Employees:	316	51%	49%	
US Employees	Total Employees	Male	Female	Not Disclosed/Available:																																						
Management:	563	64%	36%	0																																						
Technical Staff:	1019	69%	31%	0																																						
All Other Employees:	742	49%	51%																																							
Non-US Employees	Total Employees	Male	Female	Not Disclosed/Available:																																						
Management:	531	77%	23%																																							
Technical Staff:	2063	66%	34%																																							
All Other Employees:	316	51%	49%																																							
TC-SI-330a.3	Percentage of racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees.	<p>Additional Comments: At the moment, race/ethnicity is reported at a domestic (U.S.) level only. We are currently reviewing future plans regarding how we will articulate the narrative of global representational ethnicity by location.</p>																																								

US Employees	Total Employees	Asian	Black or African American	Hispanic or Latino	White	Other	Not Disclosed/Available:
Management	563	9%	4%	5%	79%	1%	2%
Technical Staff	1019	16%	4%	5%	70%	1%	4%
All Other Employees	742	6%	12%	11%	62%	2%	6%
Non-US Employees	Total						
Management	531						
Technical Staff	2063						
All Other Employees	316						

Leadership & Governance

Business Ethics & Competitive Behavior

TC-SI-520a.1	Total amount of monetary losses as a result of legal proceedings associated with anti-competitive behavior regulations.	CSG provides required annual training for all of its employees in a number of areas pertaining to labor and employment issues which includes but is not limited to anti-harassment training. For the settled litigation related to a breach of confidential information, CSG legal department provides proactive training to employees in departments which can better position CSG should such claims arise in the future. CSG has been granted the majority of state-issued almost all MTLs and implemented will provide training as appropriate to ensure employees in areas supporting the business comply with applicable laws and regulations.
--------------	---	--

Systemic Risk Management

TC-SI-550a.1	Number of (1) performance issues and (2) service disruptions; (3) total customer downtime.	Provide details of significant service disruptions: CSG maintains focus on the reduction of customer impacting events defined in CSG's "four disciplines of execution" operational improvement program in order to continually improve customer satisfaction through measured "Impact Minutes". Additionally, in 2021, CSG did not experience a performance incident or downtime issue that had a material impact on our business that required regulatory reporting to authorities or incurred material financial penalties.
TC-SI-550a.2	Description of business continuity risks related to disruptions of operations.	Discuss business continuity risks affecting operations: CSG operates in rapidly changing and evolving markets throughout the world addressing the complex needs of communication service providers, financial institutions, and many others, and as a result, new risk factors will likely emerge and currently identified risk factors will likely evolve in their scope. Further, as we enter new market sectors as well as new geographic markets, we could be subject to new regulatory requirements that increase the risk of non-compliance and the potential for economic harm to us and our customers. CSG is committed to promoting its business continuity management so the company can fulfill its responsibilities to our customers with products and services even when risks actualize

		<p>in the form of earthquakes, typhoons and other natural disasters; global pandemics; wars or other forms. CSG's goal is to provide resiliency of our products and services while testing recoverability to build confidence in those processes. Accordingly, CSG maintains Business Continuity, Disaster Recovery, and Information/Cyber Security programs with frameworks and methodologies designed to effectively manage business continuity risk. These frameworks include but are not limited to ISO 22301, NIST 800-53 and Information Technology Infrastructure Library (ITIL) processes. Our programs are designed to create a resilient operating environment with preestablished response and recovery strategies in the event of business disruption.</p> <p>Discuss measures to address business continuity risks, such as technology or processes that reduce impacts from disruptions, enhance the resilience of systems, insure against loss, or provide redundancies to critical business operations:</p> <p>CSG's Business Continuity program identifies all products and services that are critical to maintaining business operations, and correspondingly builds BCP plans for each. These are reviewed and updated twice annually, exercised annually at a minimum, and includes management of risks for products and services outages, staff loss or unavailability. Business Continuity risks are defined as:</p> <ol style="list-style-type: none"> (1) A sudden, unplanned catastrophic event causing unacceptable damage or loss. (2) Potential disaster events that are considered in our DR plans, including physical events (fire, flood, etc.), cyberattacks, terrorism or sabotage, loss of electric power or human resource availability. (3) An event that compromises an organization's ability to provide critical functional processes or services. (4) A planned or unplanned event where an organizations management invokes their disaster recovery plans. <p>Improved data center architecture provides product and service resiliency across data centers while leading protection solutions provide proven recoverability. Cloud built products and services follow frameworks and methodologies designed to provide resiliency and recoverability while mitigating risks. Use of an architecture review board ensures applications are designed and constructed in compliance with CSG standards. A central incident command process provides immediate response to incidents and disasters. With advancements in CSG's technology and a committed focus on improving our resiliency posture to meet client, regulatory, and stakeholder expectations; CSG continues to reduce "Impact Minutes" year over year in accordance with CSG's "4DX" operational improvement program. In FY21 CSG did not experience a performance incident or downtime issue that had significant impact on the business.</p> <p>References: 10-K Annual Documents Page 9</p>
--	--	--



Cautionary Statement Regarding Forward-Looking Statements & Disclaimers

This document may contain forward-looking statements within the meaning of the Private Securities Litigation Reform Act of 1995. In this context, forward-looking statements often address expected future business and financial performance and financial condition, and often contain words such as “expect,” “anticipate,” “intend,” “plan,” “believe,” “seek,” “see,” “will,” “would,” “may,” “target,” and similar expressions and variations or negatives of these words. These forward-looking statements may include, among other things, statements with respect to our strategies and priorities, future growth prospects and opportunities, uses of cash, and other measures that may impact our financial performance; expectations regarding our share repurchase program; anticipated impacts of the COVID-19 pandemic; the strength of our balance sheet and tenor of our third-party debt; and other information and statements that are not historical fact. These forward-looking statements involve certain risks and uncertainties that could cause actual results to differ materially from those expressed or implied by these statements. These risks and uncertainties include events that are outside of our control, such as general economic, legislative, political and regulatory factors, and the impact of weather conditions, natural disasters, or any epidemic, pandemic or disease outbreak (including COVID-19); other factors detailed from time to time in our filings with the U.S. Securities and Exchange Commission; and management’s response to any of the aforementioned factors. For additional information on identifying factors that may cause actual results to vary materially from those stated in forward-looking statements, please see our filings with the U.S. Securities and Exchange Commission, including our most recently filed Form 10-Q and/or Form 10-K. These forward-looking statements speak only as of the date of this release. We expressly disclaim any obligation or undertaking to disseminate any updates or revisions to any forward-looking statement contained herein to reflect any change in our expectations with regard thereto or any change in events, conditions or circumstances on which any such statement is based.