CSG Systems Sustainability Accounting Standards Board Index

2025

Table of Contents

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 approximately 6,000 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 some of the best brands 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, 2023) unless otherwise noted. For more information on CSG’s ESG program, please visit: **https://ir.csgi.com/investors/ESG/default.aspx**

Energy Management

Energy Use by Source

(1) Total energy consumed, (2) percentage grid electricity and (3) percentage renewable.

(1) Total energy consumed, (2) percentage grid electricity and (3) percentage renewable

Total amount of energy consumed as an aggregate figure, in gigajoules (GJ)	68,153
Percentage of energy consumed that was supplied from grid electricity (%)	94%
Percentage of energy consumed that was renewable energy (%)	31%
Trailing 12-month (TTM) weighted average power usage effectiveness (PUE) for data centres	

Reduction due to Workplace Management's increased focus to close unused office space to reduce costs as well as to reduce carbon footprint. In 2023, 3 sites were terminated: Fort Worth OSC (Stratum Drive address), Allen Storage and Austin OSC.

Water Use and Sources - Energy Management

(1) Total water withdrawn, (2) total water consumed, percentage of each in regions with High or Extremely High Baseline Water Stress.

(1) Total water withdrawn, (2) total water consumed

Total water withdrawn from all sources, in thousands of cubic metres (m³)	11,584
Total water consumed in operations, in thousands of cubic metres (m³)	11,584

Disclose portions of water supply by source

Water Source	Percentage of total use (%)
Rivers, Aquifers and Surface water	100%

Identify activities that withdraw and consume water in areas with High or Extremely High Baseline Water Stress

The Fort Worth Design and Delivery Center is in a high baseline water stress area. The consumption at that site is from normal daily facility and operations use and irrigation. Invoices for water usage for the entire property are managed by the landlord/property manager.

Percentage of each in regions with High or Extremely High Baseline Water Stress

Percentage of total water that is withdrawn in areas with High or Extremely High Baseline Water Stress (%)	33%
Percentage of total water consumed in areas with High or Extremely High Baseline Water Stress (%)	33%

Environmental Discussion

Discussion of the integration of environmental considerations into strategic planning for data centre needs.

Discussion Section

Describe the integration of environmental considerations, including energy and water use, into strategic planning for data centres

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 in order to ensure alignment of results to our original strategic plan.

Customer Privacy

Advertising and Privacy Discussion

Description of policies and practices relating to behavioural advertising and user privacy.

Discussion Section

Describe the nature, scope, and implementation of policies and practices related to user privacy, with a focus on how you address the collection, usage, and retention of user information

CSG maintains a comprehensive global privacy program designed to meet applicable privacy and data protection requirements in the jurisdictions where we operate, including major frameworks such as the GDPR, CCPA/CPRA and other applicable privacy laws.

The program is implemented through internal privacy and security policies and procedures that are embedded in CSG's Code of Conduct and related standards, is supported by enterprise-wide training, including mandatory annual privacy and security awareness training for all employees and completion within 90 days for new hires.

CSG collects, uses and retains customer and user information in accordance with applicable law, the terms of its customer agreements and its internal policies and processes. Our practices are designed to limit collection to what is necessary for defined business purposes, use personal information only for those purposes (or as otherwise permitted by law or contract), and retain it only for as long as needed to fulfill those purposes and related legal or regulatory obligations. Personal information is retained and deleted securely in accordance with CSG’s Data Retention and Destruction Policy and Schedules.

Describe the information "lifecycle" and how information-handling practices at each stage may affect individual's privacy

CSG has a comprehensive approach to information handling and to prevent the compromise or misuse of CSG's information, applications, networks and computer systems. In line with CSG’s Information Handling Standard, we categorize information by type and sensitivity and define required protections, commensurate with its business value and impact. Across the customer lifecycle, once CSG receives approval from a customer to process personal information to provide products and services, we apply a defined protection sequence: (1) classifying the information, (2) handling and storing it in line with its classification, (3) retaining it only for that information for appropriate periods and (4) securely deleting or destroying it when no longer needed.

These requirements apply to all entities or individuals with access to information controlled or processed by CSG, including CSG entities, employees, contingent workers, contractors and as external parties, such as business partners, vendors, suppliers, and outsourced service providers. Information owners are responsible for determining the appropriate information classification and ensuring that information custodians protect the information accordingly. All information is protected in line with its classification as it is created, used, stored, transmitted, and reproduced within CSG, and no and CSG-owned system or network may connect to the internet without the appropriate procedures consistent with the applicable classification. High-impact information is not retained in any public zone and protected health information, credit card numbers, or other account numbers are not stored on internet-facing servers 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.

Information owners are responsible for creating information repositories and data transfer procedures, which protect information in the manner appropriate to its classification. Appropriate information is backed up, with backups tested periodically and handled with the same security precautions as the source data. When systems are disposed of, or repurposed, data is securely deleted, or media is destroyed in accordance with industry best practices, the Information Handling Standard, and CSG’s Data Retention and Destruction Policy and associated Schedules.

CSG maintains a data subject request portal that enables individuals to inquire about and request access to, correction of, deletion of or other actions on their personal information. Data subject requests are handled in accordance with applicable law and CSG's internal policies and processes.

Discuss the degree to which policies and practices address similar issues in M-03-22, including use of PIAs

N/A

Discuss policies and practices related to children's privacy, including relations to COPPA

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.

Discuss how behavioural advertising is addressed, using the Self-Regulatory Principles for Online Behavioural Advertising

CSG addresses behavioural advertising on its public website, csgi.com, through it's website privacy notice (including our cookie policy) that is designed to comply with applicable privacy and data protection requirements in the jurisdictions where we operate, including major frameworks such as the GDPR, CCPA/CPRA and other applicable privacy laws, and to reflect the core concepts of the Self-Regulatory Principles for Online Behavioural Advertising, such as transparency, notice, and user control.

CSG and certain third parties may place advertising cookies or similar technologies on a user's device to enable third party ad networks to recognize a unique cookie or device identifier, understand user interests based on browsing activity, and deliver targeted advertisements on our website and third-party sites.

These activities are disclosed in our website privacy notice (available at csgi.com/privacy), which explains the types and purposes of cookies used and provides users with mechanisms to manage their preferences, including the ability to disable or withdraw consent for advertising cookies through cookie settings and browser-level controls. Where a cookie lifespan is not otherwise specified in the cookie settings, CSG applies a default life span of thirteen months or a shorter period where required by law.

User Information Use

Number of users whose information is used for secondary purposes.

Number of unique users whose information is used for secondary purposes

Number of unique users whose information is used for secondary purposes	0

User Privacy Legal Losses

Total amount of monetary losses as a result of legal proceedings associated with user privacy.

Total amount of monetary losses as a result of legal proceedings associated with user privacy

Total monetary losses	0
Monetary losses from adjudicative proceedings	0
Monetary liabilities to opposing parties or others	0

Discussion Section

Briefly describe the nature and context of all monetary losses as a result of legal proceedings
N/A
Describe any corrective actions implemented as a result of the legal proceedings
N/A

Comments

CSG has not been involved in any proceeding related to customer privacy resulting in monetary damages during the reporting period.

Requests for User Information

(1) Number of law enforcement requests for user information, (2) number of users whose information was requested, (3) percentage resulting in disclosure.

Requests for User Information from Government or Law Enforcement Agencies

Unique requests for user information	0
Unique users whose information was requested	0
Percentage of requests that resulted in disclosure to the requesting party (%)	0%

Requests for User Information by Region or Country

Region or Country	Unique requests for user information	Unique users whose information was requested	Percentage of requests that resulted in disclosure to the requesting party (%)
N/A	N/A	N/A	N/A

Discussion Section

Discuss whether these characteristics apply to a portion of your data releases if this discussion would provide necessary context for interpretation of your company's disclosure

N/A

Discuss policy for determining compliance with requests for user data

As a general principle, CSG will not disclose personal data in response to a request received from a law enforcement authority or state security policy (together the "**Requesting Authority**") to disclose personal information processed by CSG (“**Data Disclosure Request**”) unless either:

- it is under a compelling legal obligation to make such disclosure; or
- taking into account the nature, context, purposes, scope and urgency of the Data Disclosure Request and the privacy rights and freedoms of any affected individuals, there is an imminent risk of serious harm that merits compliance with the Data Disclosure Requests in any event.

For that reason, unless it is legally prohibited from doing so or there is an imminent risk of serious harm, CSG will notify and cooperate with the competent data protection authorities (and, where it processes the requested personal data on behalf of a customer, the customer) in order to address the Data Disclosure Request.

If CSG receives a Data Disclosure Request, the recipient of the request must pass it to Chief Compliance Officer immediately upon receipt, indicating the date on which it was received together with any other information which may assist CSG's Chief Compliance Officer to deal with the request.

The request does not have to be made in writing, made under a Court order, or mention data protection law to qualify as a Data Disclosure Request. Any Data Disclosure Request, howsoever made, must be notified to Chief Compliance Officer for review.

CSG's Chief Compliance Officer will carefully review every Data Disclosure Request on a case-by-case basis. CSG's Chief Compliance Officer will liaise with the legal department as appropriate to deal with the request to determine the nature, context, purposes, scope and urgency of the Data Disclosure Request, as well as its validity under applicable laws, in order to identify whether action may be needed to challenge the Data Disclosure Request.

Describe the policy for notifying users about such requests, including the timing of notification

If CSG receives a Data Disclosure Request for personal data processed on behalf of a customer, after assessing the nature, context, purposes, scope and urgency of the Data Disclosure Request, CSG will Immediately notify and provide such customer with the details of the Data Disclosure Request prior to disclosing any of such customer's personal data, unless legally prohibited or where an imminent risk of serious harm exists that prohibits prior notification.

Further, some customer agreements require disclosure about Data Disclosure Requests. We have a contractual obligation to provide customers in the EU, UK and Switzerland with notice of Data Disclosure Requests under clause 15 of the Standard Contractual Clauses, which include the obligations of the data importer if there is a Data Disclosure Request.

Government Oversight of Products

List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring.

Discussion Section

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.

Describe the extent of monitoring, blocking, content filtering, or censorship across product or service lines

N/A

Discuss implications of blocking or censorship

N/A

For products and services that have been modified in a manner material to their functionality, identify the product or service affected and discuss the nature of the modification

N/A

Discuss policies and practices related to freedom of expression
N/A

Comments

Data Privacy & Security - CSG (csgi.com)

Data Security

Data Breaches

(1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of users affected.

(1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of users affected

Total number of data breaches	N/A
Percentage of data breaches involving personally identifiable information (%)	N/A
Total number of unique users affected by data breaches, including those whose personal data was compromised	N/A

Discussion Section

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 provides an Incident Report that is communicated through this team detailing timelines, business and customer impact, risk, solution/remediation efforts, and security recommendations.
Disclose policy for disclosing data breaches to affected users in a timely manner
CSG’s Chief Information Security Officer (CISO) oversees a comprehensive security program designed to manage data security risks, including the use of recognized third-party cybersecurity standards. CSG treats security as a top priority and aims to be as transparent as possible with customers and consumers. At a minimum, CSG complies with all contractual, legal, and regulatory breach-notification requirements, and strives to exceed those requirements whenever feasible.

Comments

CSG’s Security Program is independently audited at least annually against ISO/IEC 27001:2022 and supports enterprise-wide certifications and attestations, including SOC 2 Type II and CSA STAR for Enterprise Cloud and PCI DSS v4.0 Level 1 Service Provider status.

Data Security Discussion

Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards.

Discussion Section

Describe your approach to identifying information system vulnerabilities that may pose a data security risk

CSG uses independent third parties and industry-leading discovery tools to identify vulnerabilities across software/applications, platforms, network, infrastructure, and logged traffic, with the goal of preventing, detecting, and responding to potential threats.

CSG’s network security capabilities include 24/7 infrastructure monitoring, leveraging enterprise-grade firewalls, intrusion detection and prevention systems (IDS/IPS), content-filtering solutions, and application firewalls in a Demilitarized Zone (DMZ) configuration. These controls are designed to protect both public and private data and continuously monitor all traversing network communications.

Centralized log-monitoring capabilities are used to detect anomalies and security events. Events are sourced from multiple layers, including network infrastructure (IDS/IPS, firewalls, routers, switches), operating systems, and applications.

CSG employs enterprise anti-malware solutions to protect systems and prevent the spread of malicious code. Protection and monitoring include remotely deployed updates to each system and consolidated malware/software reporting for analysis. CSG-owned servers, workstations, and email systems are protected by these controls.

CSG also performs application code scanning and vulnerability testing for both product and service offerings, covering development and post-development stages for customer-facing applications and services. These activities are governed by CSG’s Vulnerability Management Program.

Describe your approach to managing identified data security risks and vulnerabilities

CSG’s Security Incident Response Team (SIRT) is responsible for managing security incidents. SIRT works with technical teams to assess incidents, perform forensic analysis, and plan and execute remediation. All significant actions are reviewed and approved by the Chief Information Security Officer (CISO).

SIRT produces formal incident reports following a defined MSIRT process, with executive oversight and review by CSG’s Audit Committee as appropriate. These reports include timelines, business and customer impact, risk assessment, remediation efforts, and security recommendations.

Describe your use of third-party cybersecurity risk management standards

CSG requires third-party vendors to adhere to practices and standards that support CSG’s regulatory obligations and internal security requirements. This applies both during vendor onboarding and throughout the vendor’s lifecycle as regulatory expectations and industry practices evolve.

CSG’s Vendor Management Program applies a tiered risk-based approach that evaluates vendors according to the type and sensitivity of Personally Identifiable Information (PII) they access or process.

Discuss observed trends in type, frequency and origination of attacks on data security and information systems
In recent years, attack patterns have shifted from primarily exploiting perimeter-level vulnerabilities to more targeted manipulation of users through phishing, social engineering, and ransomware. Threat actors increasingly focus on exploiting human behavior to gain authorized or otherwise undetected access to systems. Once access is gained, they may collect and exfiltrate data over extended periods to correlate information and refine their approach to compromising data.

Comments

All employees, contractors, and contingent workers are required to complete annual Security Awareness training, along with additional security-focused training tailored to their job responsibilities and relevant global events.

CSG applies a Three Lines of Defense model. Control activities are performed by operational teams (first line), regularly evaluated by security and governance functions (second line), and, where appropriate, reviewed by independent auditors (third line). Penetration testing is conducted on critical systems after each release to validate the effectiveness of internal and external vulnerability scanning and remediation processes.

CSG's Governance and Internal Audit teams perform quarterly and ongoing monitoring of critical controls to maintain a consistent security posture and reinforce the organization's security knowledge base.

Each year, external auditors assess the design and operating effectiveness of critical controls for PCI DSS v4.0, ISO/IEC 27001:2022, SOC 2 Type II and CSA STAR for Enterprise Cloud Services, and SOX reporting.

Employee Engagement & Inclusion

Foreign Employees

Percentage of employees that are (1) foreign nationals and (2) located offshore.

Percentage of employees that are foreign nationals

Disclose the percentage of employees that are foreign nationals (%)	4.5%

Percentage of employees that are located offshore from the entity's country of domicile, by region

Region	Percentage of Employees Located Offshore (%)
APAC	46%
CALA	8%
EMEA	10%
North America	2%
Total	66%

Discussion Section

Describe potential risks from recruiting foreign nationals and/or offshore employees
N/A
Describe management's approach to addressing the risks it has identified related to recruiting foreign nationals
N/A
Describe management's approach to addressing the additional risks identified related to conducting offshore business activities
N/A

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 INCLUSION & IMPACT strategy to develop and nurture approaches to channel the power of all and mature our INCLUSION & IMPACT program. To further our INCLUSION & IMPACT 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.

Employee Engagement

Employee engagement as a percentage.

Employee Engagement Percentage (%)

Employee Engagement Percentage (%)	86%

Discussion Section

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.

The two questions that make up eSat (Employee Satisfaction Score)+ are:

1. I would recommend CSG as a great place to work

2. How happy are you working at CSG?

What is an Engagement score?

Engagement score is calculated by computing the average score for eSat (Employee Satisfaction) and recommend.

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.

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 scale, with 0 as the lowest and 100 as the highest. This is how engagement score is calculated.

When the survey methodology has changed compared to previous reporting years, indicate results based on both the old and new methods for the year in which the change is made
N/A
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 an 86% response rate
Disclose results of other survey findings
N/A

Comments

Employee Representation - Gender

Percentage of gender representation for (1) management, (2) technical staff, and (3) all other employees.

Percentage of gender representation for (1) management, (2) technical staff, and (3) all other employees

Employee Categories	Total Employees	Male (%)	Female	Not Disclosed/Available (%)
Management	867	71%	29%	
Technical Staff	3,741	65%	35%	
All Other Employees	1,262	51%	49%	

Workforce by Region

Region	Total Employees	Male	Female	Other
APAC	2,701	62%	38%	
CALA	460	73%	27%	
EMEA	582	73%	27%	
North America	2,127	59%	41%	

Discussion Section

Discuss factors that significantly influence gender group representation, such as the country or region where employees are located
At CSG, our dedication to continuous learning and development took center stage in 2023, with our 15- on-15 series on INCLUSION & IMPACT topics emerging as a consistent favorite. Co-hosts from around the world, spanning India, Colombia, Australia, the UK and the US, shared best practices on inclusive hiring, accessibility, leadership keystones, microaggressions and inclusive practices for international teams. We continued our commitment to INCLUSION & IMPACT with the deployment of our continued e-training on workplace inclusion, receiving strong positive reviews and completion globally. Employees embraced foundational concepts that paved the way for deeper and more meaningful discussions on topics around psychological safety, allyship and accountability within teams.
Describe your policies and programs for fostering equitable employee representation across your global operations
At CSG, our dedication to continuous learning is part of our purpose driven culture. Co-hosts from around the world, spanning India, Colombia, Australia, the UK and the US, shared best practices on inclusive hiring, accessibility, leadership keystones, microaggressions and inclusive practices for international teams. We continued our commitment to INCLUSION & IMPACT with the deployment of our continued e-training on workplace inclusion, receiving strong positive reviews and completion globally. Employees embraced foundational concepts that paved the way for deeper and more meaningful discussions on topics around psychological safety, allyship and accountability within teams.

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.

Employee Representation - Race/Ethnicity

Percentage of racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees.

Percentage of racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees

US Employees	Total Employees	Asian (%)	Black or African American (%)	Hispanic or Latino (%)	White (%)	Other (%)	Not Disclosed/Available (%)
Management	366	12%	4%	5%	73%	2%	4%
Technical Staff	797	17%	4%	6%	64%	3%	6%
All Other Employees	846	7%	10%	11%	64%	2%	6%

Workforce breakout by region

Region	Total Employees	Supplemental Disclosures

Discussion Section

Discuss factors that significantly influence racial/ethnic group representation
N/A

Business Ethics & Competitive Behaviour

Anti-Competitive Behaviour Litigation

Total amount of monetary losses as a result of legal proceedings associated with anti-competitive behaviour regulations.

Total amount of monetary losses as a result of legal proceedings associated with anti-competitive behaviour regulations

Total monetary losses	0

Discussion Section

Briefly describe the nature and context of all monetary losses as a result of legal proceedings
N/A

Describe any corrective actions implemented as a result of the legal proceedings
N/A

Comments

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. CSG has been granted a majority of state-issued MTLs and will provide training as appropriate to ensure employees in areas supporting the business comply with applicable laws and regulations.

Systemic Risk Management

Technology Disruptions

Number of (1) performance issues and (2) service disruptions; (3) total customer downtime.

Number of (1) performance issues and (2) service disruptions; (3) total customer downtime

Total number of performance issues	0
Total number of service disruptions	0
Total customer downtime related to performance issues and service disruptions	0

Discussion Section

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”. CSG has not experienced a recent performance incident or downtime issue that had a material impact on our business that required regulatory reporting to authorities or incurred material financial penalties.

Comments

Number of performance issues:

Total customer downtime related to performance issues and service disruptions:

At CSG, operational excellence and reliability are supported by a structured continuous improvement approach, focusing on critical improvement priorities, driving measurable year-over-year performance improvement and embedding accountability and transparency. Management of this program is integrated into CSG’s broader risk and governance structure.

Technology Disruptions Discussion

Description of business continuity risks related to disruptions of operations.

Discussion Section

Describe potential business continuity risks associated with technology disruptions 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 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.

Discuss measures to address business continuity risks

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:

(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 organizations ability to provide critical functional processes or services.

(4) A planned or unplanned event where an organizations management invokes their disaster recovery plans.

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. CSG has not experienced a recent performance incident or downtime issue that had significant impact on the business.

Identify which critical business operations support cloud-based services, and further note whether those operations are owned or outsourced
Deliver an Exceptional Customer Experience: We believe we deliver more business value by having developed a long track record of doing what we say and being easy to do business with. We do this by putting the customer at the heart of our decision-making which is always directed at improving our agility, delivery capabilities, operational excellence, efficiency, and reliability to enable our customers' success.
Discuss the estimated amount of potential loss, probability of that loss, and the associated timeframe

Identify which critical business operations support cloud-based services, and shall further note whether those operations are owned or outsourced:

Activity Metrics

Data Storage

TC-SI-000.A (1) Number of licenses or subscriptions, (2) percentage cloudbased.

TC-SI-000.B (1) Data processing capacity, (2) percentage outsourced.

TC-SI-000.C (1) Amount of data storage, (2) percentage outsourced.

(1) Number of licenses or subscriptions, (2) percentage cloudbased

Number of Licenses or Subscriptions	N/A
Percentage Cloudbased (%)	N/A

(1) Data processing capacity, (2) percentage outsourced

Unit of Measure	N/A
Data Processing Capacity	N/A
Percentage Outsourced (%)	N/A

(1) Amount of data storage, (2) percentage outsourced

Amount of Data Storage	N/A
Percentage Outsourced (%)	N/A

Comments