

Who is CSG?

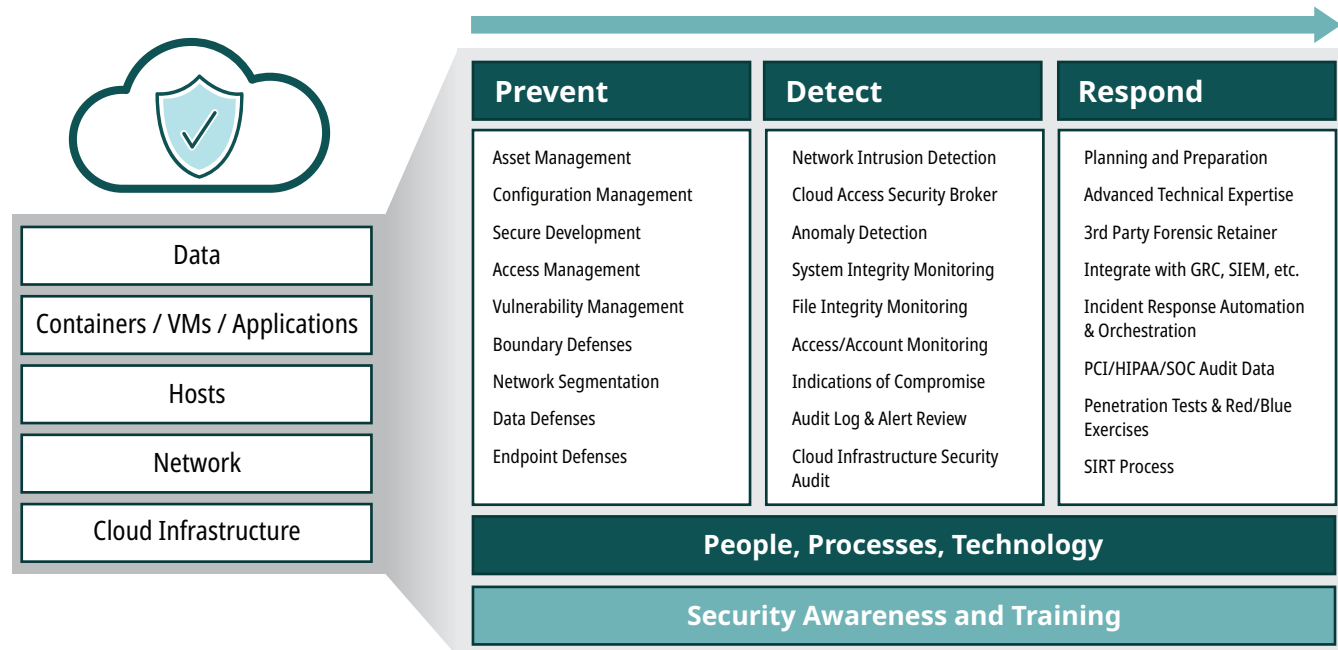
CSG is a purpose-driven, high-growth SaaS platform company helping some of the world’s most recognizable brands solve their toughest business challenges. We’re a trusted partner to global companies that want to evolve to meet the demands of today’s digital economy, with future-ready solutions that drive exceptional customer experiences.

We help connect billions of customers around the world and process hundreds of millions of payments every year. As such, we take data privacy and security seriously to ensure that our customers’ data—and their end customers’ data—is secure.

What Is Our Approach to Data Privacy and Security?

Our business goal is to ensure cyber safety for our customers and employees. CSG delivers this goal through a combination of people, processes, technology, and partnerships to prevent, detect, and respond to threats in an efficient, effective, and scalable manner.

Cybersecurity Principles and Best Practices



Validated Assurance

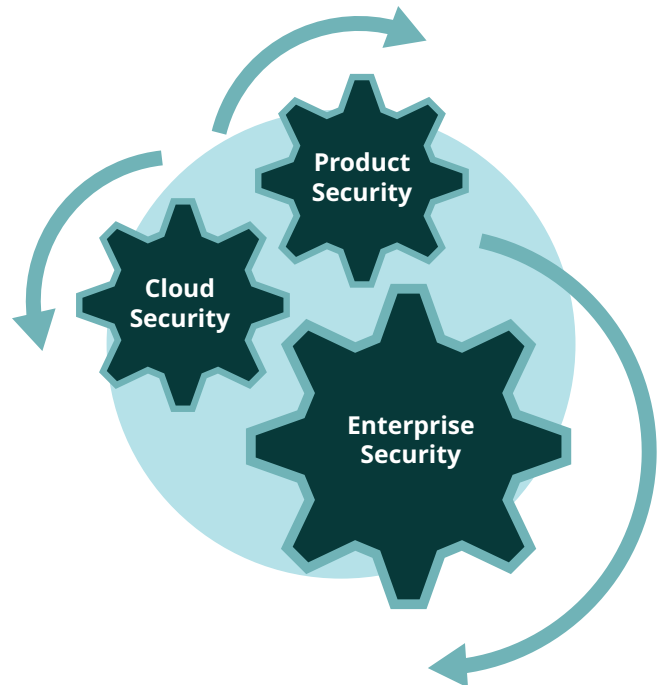


What Best Practices and Processes Do We Use?

CSG integrates security at every level of our business practices to secure our business and our customers' businesses alike. This is a 360-degree, comprehensive security practice covering all facets and disciplines of modern security management.

Enterprise Security

- **Relentless Improvement:** At CSG, we understand that “good enough” today is not enough for tomorrow. We maintain a hyper-focused, intentional approach to continuous improvement, risk management, and regulatory compliance.
- **People Are Our Power:** Everyone at CSG has a role in delivering our best-in-class cloud platforms and security. Everyone is properly equipped with the tools to support all cloud and security needs. Continuous training, education, testing, monitoring and feedback enable our rapidly innovating organization to deliver a modern and mature Enterprise Security program. CSG’s world-class security program is led by our Chief Information Security Officer and executed by highly credentialed security professionals organized by function at a global scale.



Cloud Security

- CSG’s Cloud Usage Framework defines fail-safe guardrails to enable agile innovation while ensuring the utmost security of our solutions. CSG maintains tiered cloud proficiency training tied to roles, enforced cloud build and configuration standards, and governance for all cloud infrastructure configuration.

Product Security

- CSG’s Product Security function enables the visibility, standardization and assurance required to ensure quality outcomes of the system development lifecycle. They establish policy, governance, and oversight of secure coding practices that promote confidentiality, integrity and availability across CSG’s product portfolios.

How Does Each Step of Our Approach Work?

Enterprise Security

Ensuring cyber safety for our customers and employees is the cornerstone of CSG's Enterprise Security Management System.

Holistic Security Program

GOVERNANCE, RISK AND COMPLIANCE

The global risk and regulatory landscape is complex, and non-compliance is a significant business risk. CSG is a trusted partner in managing risk, policy, continuous monitoring, and oversight of IT controls, including those of third parties, to deliver security assurance and sustainment of legal and regulatory requirements that promote and align to your business objectives.

IDENTITY AND ACCESS MANAGEMENT

Users require the right access to the right data at the right time for the right reasons so your business can run smoothly. CSG's Identity and Access Management function ensures appropriate access to data and resources to reduce risk, meet compliance requirements and enable agility to support your business objectives.

DATA PRIVACY OPERATIONS

CSG's data practices offer a chance for brands to take the lead and own a strategic space focused on data transparency and access. CSG's Data Privacy function maintains controls aligned to Privacy objectives to identify, inventory, classify, protect and monitor data throughout the data management lifecycle. A robust program and capabilities enable CSG to meet regulatory privacy obligations including Data Subject Requests.

PHYSICAL AND ENVIRONMENTAL SECURITY

CSG maintains an effective suite of controls and requirements to protect data and information, hardware, and human resource assets. Whether our solution is being delivered from CSG's cloud or public cloud, our infrastructure and resources are protected from inappropriate physical access, theft, and sabotage in addition to accidental, intentional, or natural events.

PRODUCT SECURITY

CSG provides visibility, standardization, and assurance for development practices, with established policy, governance, and oversight of secure coding practices that promote confidentiality, integrity, and availability across CSG's product portfolios.

SECURITY TESTING AND AUTOMATION

CSG provides routine vulnerability management and ongoing penetration testing services to ensure security hardening of CSG platforms and applications, and builds internal Development Security Operations (DevSecOps) services and automations that deliver efficiency, scale, and pervasiveness of security controls.

SECURITY OPERATIONS

CSG manages a comprehensive Security Incident Response process, and implements and monitors comprehensive security alerting and preventative technical controls across all technology platforms and at several levels and abstractions of our technology stack. This is integral in maintaining CSG's reputation as a secure and trusted partner to our customers, and allows us to provide the utmost confidence in our service.

NETWORK OPERATIONS

CSG ensures that no matter where in the world CSG's customers or employees are, our platform and products will be reliable, available, and performant for our customers and their clients. CSG is skilled in the design, build, and maintenance of global connectivity for every CSG employee, facility, data center, application, and customer. Our deep skill and experience guarantees first-in-class service experiences and sustained customer satisfaction.



Cloud Security

CSG’s Cloud Security Framework provides clients with assurance and peace of mind for critical workloads and data being processed in the cloud. CSG’s Cloud Security standards provide CSG with simplified alignment to standards that ensure cloud security competencies at all levels. CSG provides clearly defined usage standards for the public cloud and trusted enablement so that CSG can safely innovate to solve our customer’s business challenges. Based on the CSG-developed cloud Usage Framework, all public cloud environments are measured against the standard, and remediation activities are orchestrated through notifications provided to users, security, and cloud teams with automated escalations.

With CSG's developed core engine, supporting tools and potential future tools, clients can rest assured their data is protected by CSG's world-class services.

Why Trust CSG’s Public Cloud Community of Practices and Framework?

Our practices are best-in-class, and cloud experts like AWS agree.

We invested 2+ years working with AWS experts to tune and perfect our practices. During our engagement they acknowledged and praised our practices.

Dozens of communication service providers (CSPs) trust CSG’s practices for their most important data— their financials.

Your balanced strategy, enablement, engine, and focus on operational excellence are impressive. Many of our other customers can learn from your example.

AWS

Trusted Provider
CSG operating SaaS for

25+

years for the world’s leading telecom and entertainment companies

\$300 million
CSG Revenue

Annually from solutions in the public cloud as of July 2022

Business
CSG solutions hosted in public cloud are

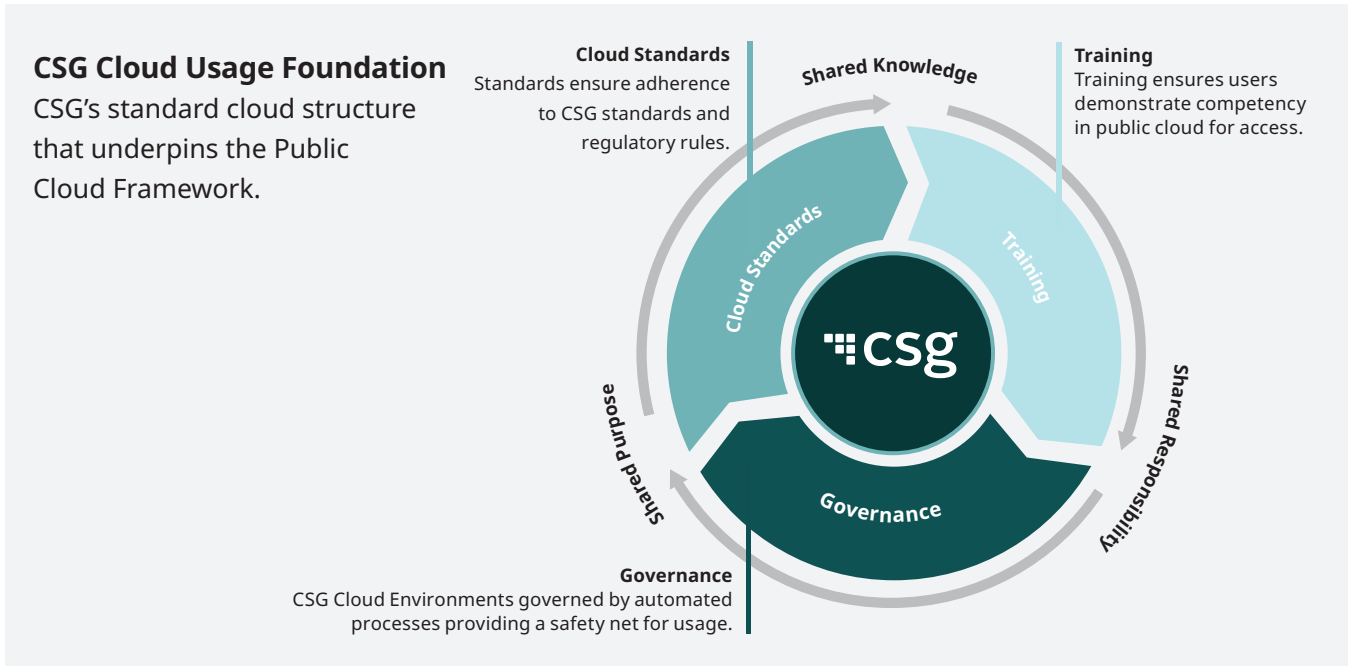
28%

of our total business and continues to grow

Product Security

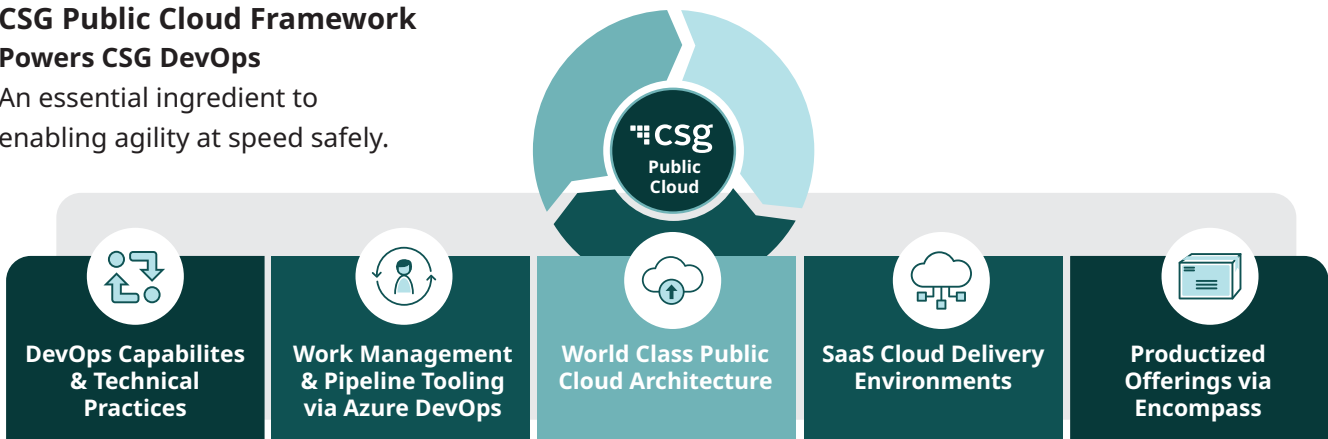
CSG DEVSECOPS

CSG has established automation standards and frameworks, and provides automation services to enable DevSecOps functions and self-service capabilities to the entire enterprise. CSG has successfully automated critical security mechanisms to ensure that CSG products are hardened, secured, and available.



CSG Public Cloud Framework Powers CSG DevOps

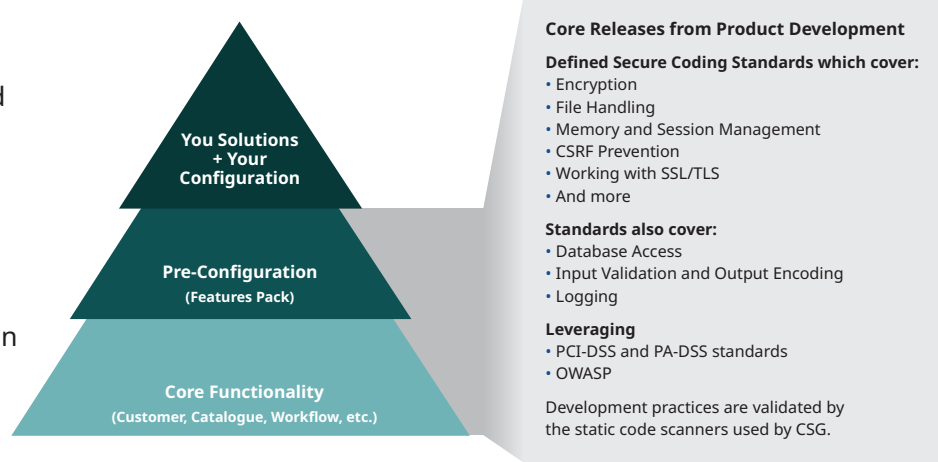
An essential ingredient to enabling agility at speed safely.



CSG’s Cloud standards and framework are the cornerstone of all applications from the cloud environment to cloud principles.

APPLICATION-LEVEL SECURITY PRINCIPLES

All CSG applications follow a defined and extensive application development process.



All CSG Applications Provide:

Secure by Design (SbD)	SbD is a security assurance approach that formalizes design, security controls, and auditing.
Secure Development Training	Each developer is required to complete modules specific to the area of application development they are performing.
Secure Development Environments	Development environments are hardened, secured, and monitored with the same standards and controls as production environments.
Static Application Security Testing	Static Application Security Testing provides coverage of common flaws in source code, including but not limited to the OWASP Top 10.
Dynamic Application Security Testing	More than 95 categories of attacks and vulnerabilities, including but not limited to OWASP top 10 are tested.
Open-Source Software Composition Analysis	CSG uses of variety testing suites for Software Composition Analysis, to identify and reduce open-source risk and manage license compliance.
API Testing	CSG uses a variety of testing suites and custom generated playbooks to identify common API vulnerabilities such as OWASP API Top 10 and CWE, and logic vulnerabilities, such as Role Based Access Controls.

CSG provides data privacy and security at every level of our business. As a trusted partner supporting billions of customers world-wide, CSG delivers future-ready security best practices to prevent, detect and respond to all potential risks ensuring cyber safety for all employees and customers.