System and Organization Controls (SOC) 2 Type I
Report on Management's Description of its

Service and Asset Management Platform

And the Suitability of Design of Controls Relevant to the Trust Services Criteria for Security, Availability, and Confidentiality

As of July 25, 2022

Together with
Independent Service Auditors' Report

Table of Contents

I. Independent Service Auditors' Report

Independent Service Auditors' Report

To the Management of InvGate

Scope

We have examined InvGate's accompanying description of its Service and Asset Management Platform titled "Description of InvGate's Service and Asset Management Platform" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design of controls stated in the description as of July 25, 2022, to provide reasonable assurance that InvGate's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

InvGate is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that InvGate's service commitments and system requirements were achieved. InvGate has provided the accompanying assertion titled "Assertion of InvGate Management" (assertion) about the description and the suitability of the design of controls stated therein. InvGate is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

a. The description presents InvGate's Service and Asset Management Platform that was designed and implemented as of July 25, 2022, in accordance with the description criteria.
b. The controls stated in the description were suitably designed as of July 25, 2022, to provide reasonable assurance that InvGate service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date.

Restricted Use

This report is intended solely for the information and use of InvGate, user entities of InvGate's Service and Asset Management Platform as of July 25, 2022, business partners of InvGate subject to risks arising from interactions with the Service and Asset Management Platform, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

San Jose, California
September 6, 2022

II. Assertion of InvGate Management

Assertion of InvGate Management

We have prepared the accompanying description of InvGate's Service and Asset Management Platform system titled *"Description of InvGate's Service and Asset Management Platform*" as of July 25, 2022, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the Service and Asset Management Platform system that may be useful when assessing the risks arising from interactions with InvGate's system, particularly information about system controls that InvGate has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

We confirm, to the best of our knowledge and belief, that:

a. The description presents InvGate's Service and Asset Management Platform system that was designed and implemented as of July 25, 2022, in accordance with the description criteria.

b. The controls stated in the description were suitably designed as of July 25, 2022, to provide reasonable assurance that InvGate's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date.

Signed by InvGate Management

September 6, 2022

III. Description of InvGate's Service and Asset Management Platform

Description of InvGate's Service and Asset Management Platform

Company Background

InvGate was founded in 2009 to develop innovative IT Management solutions for organizations all over the world. The company was built on the belief that technology and usability improvements that were becoming widespread in the B2C space would greatly benefit B2B software offerings, replacing cumbersome and complicated products with newer offerings better suited for younger and more modern organizations.

Serving customers in over 50 countries, InvGate was founded in Buenos Aires, Argentina, and because of its global focus, currently operates subsidiaries in the US, Mexico and Spain.

InvGate's products are delivered either as SaaS or on-prem software offerings to customers in almost all industries, including Finance, Manufacturing, Retail, Oil & Gas, Healthcare, Education, Government, Military, Aerospace and many others.

Services Provided

InvGate develops two distinct software product lines that are regularly sold together as a bundle.

InvGate Service Desk, offered both as SaaS or on-prem software, is a service management system that allows organizations to optimize their service delivery to their employees or customers.

The product offers a web based self-service portal where customers or employees can enter requests (for example, an IT support request) that is then routed to appropriate teams for its treatment. The tool then allows for:

- collaboration between different parties for the purpose of dealing with the request
- automation of business workflows and actions
- enhanced visibility over the workload and performance of teams providing service using the tool
- enhanced visibility over customer satisfaction and quality of services

InvGate Insight and InvGate Assets, offered both as SaaS or on-prem software, is an IT asset management platform that allows IT teams to centrally manage their IT infrastructure.

The products offer a web-based management platform where administrators can gain visibility over IT devices and manage them from a single interface. The tools allow for:

- automated discovery and inventory of IT devices in a company's network
- automated tracking of changes in configuration
- searching and reporting on IT devices, their configuration and status
- monitoring compliance requirements over these IT devices

Principal Service Commitments and System Requirements

InvGate designs its processes and procedures related to its products to meet its objectives as an innovative IT Management solution. These processes and procedures are implemented taking into consideration the laws and regulations that govern the provision of InvGate services, and the financial, operational, and compliance requirements that InvGate has established for the services.

Security commitments are documented and communicated through several documents referenced in InvGate products which include, but not limited to, “Cloud Security Practices”, “InvGate Cloud Services Privacy Policy” and “Terms and Conditions”. Particular commitments can be agreed and documented during the purchase process. InvGate defines operational requirements and good practices that support the achievement of security commitments, relevant laws and regulations, and other system requirements.

Security commitments are standardized and include, but are not limited to, the following:
Security principles within the design and functionalities of the InvGate products that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
Use of encryption technologies to protect customer data at rest and in transit.

Information security policies define an organization-wide framework to how systems and data are protected. These include internal policies around how the service is designed, developed and tested, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the InvGate platform.

Components of the System

Infrastructure

The production environment is hosted on Amazon Web Services (AWS). The production servers are run on a dedicated Virtual Private Cloud in a dedicated AWS account hosted in the US-West zone within Amazon Elastic Compute Cloud (EC2) and backed up in Amazon Simple Storage Service (S3).

Primary Infrastructure		
Hardware	Type	Purpose
AWS VPC	*Virtual Networking*	Cloud computing service that provides a virtual private cloud, where InvGate cloud product are deployed
AWS S3	*Storage*	Maintains customer files as well as database backups.

Primary Infrastructure		
Hardware	Type	Purpose
AWS Elastic IP		Is a static IPv4 address designed for dynamic cloud computing
AWS RDS	Database	Operates relational databases engines (MySQL & PostgreSQL) in the cloud
AWS EC2	Computing Instances	Provides secure, resizable compute capacity in the cloud
AWS ElasticCache	Cache	In-memory data store and cache service that improves the performance by retrieving information from managed in-memory caches
AWS	CloudSearch	Used for free text searches along the products served
AWS Classic Load Balancer	Balancer	Provides load balancing across multiple Amazon EC2 instances and operates at both the request level and connection level
AWS IAM	Identity and Access Management	Assists management of access to AWS services and resources.

Software

Primary software used to provide InvGate's system includes the following:

Primary Software		
Software	Operating System	Purpose
Jenkins	Linux	Automates the parts of software development related to building, testing, and deploying, facilitating continuous integration and continuous delivery.
Zabbix	Linux	Monitors IT infrastructure such as networks, servers, virtual machines, and cloud services by collecting data and displaying metrics
VictorOps	VictorOps	Integrated with Zabbix triggers alerts to on call people

Primary Software		
Software	Operating System	Purpose
Terraform		Infrastructure as code software tool
Google Workspace	Google	Collaborative tools and IAM of other tools by using Google as authentication method
Mercurial		Hosting for software development and version control.
Github		Hosting for software development and version control.
Instances-list	Linux	Internally developed tool used as repository of cloud instances information
InvGate Service Desk		Assist customers with their needs
InvGate Insight		IT assets repository
Slack	Chat	Messaging application
Open Project	Issue tracking system	Used as issue tracker for InvGate Insight
RedMine	Issue tracking system	Used as issue tracker for InvGate Service Desk

People

InvGate has a staff of about 200 people organized under an organizational structure that includes management leads, teams and job titles. The personnel supporting the Platform and assisting in delivering services include the following areas:

- Engineering, engineering staff and Product. This includes the teams in charge of designing, developing, testing, deploying, monitoring and overviewing the whole development process for our products and services:
    - Assets team
    - Service Desk team
    - Insight team
    - Infrastructure team
    - Integrations team

  - Internal tools team
  - Product team
  - Operations team
- Customer facing areas. This includes the teams that string along with customers through all the customer journey
  - Implementations team
  - Technical Support team
  - Customer Success team
- Sales areas. This includes the teams that go along with prospects during the sales and renewal processes:
  - Sales Development team
  - Business Development team
  - Sales LATAM team
  - Sales US team
  - Renewals team
- Marketing areas.
  - Design
  - Growth Marketing
  - Product Marketing
  - Content
  - Corporate Marketing
- HR areas. These teams are in charge of recruiting, maintaining and developing talent across InvGate
  - Talent Acquisition team
  - Talent Management team
- Finance & administration

Data

Data, as defined by InvGate, constitutes the following:

- Data stored in databases

- Files and attachments
- Error logs
- System files and logs
- Testing plans and their results
- Security events data

InvGate classifies data into three categories to ensure sensitive and confidential data is properly classified, protected, retained and disposed. These three designated classifications are Confidential, Restricted and Public.

Confidential

Highly sensitive data requires the highest levels of protection; access is restricted to specific employees or departments, and these records can only be passed to others with approval from the data owner, or a company executive. Customer data is considered Confidential data and is encrypted at rest.

Restricted

InvGate proprietary information requiring thorough protection; access is restricted to employees with a "need-to-know" based on business requirements. This data can only be distributed outside the company with approval. This is default for all company information unless stated otherwise.

Public

Documents intended for public consumption which can be freely distributed outside InvGate.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the InvGate policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any InvGate team member.

Physical Security

All data is hosted by Amazon Web Services (AWS). AWS data centers do not allow InvGate employees physical access.

Logical Access

InvGate uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources.

Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists.

InvGate uses AWS IAM as identity access management to access cloud management tool provided by Amazon.

Employees are required to use Google Workspace for Single Sign-On (SSO), with a required second factor authentication (2FA) in their account. Users are also required to separately sign on to any systems or applications that do not implement Google SSO using passwords that conform to InvGate's security policies.

On an annual basis, access rules for each role are reviewed by executive management.

Computer Operations – Backups

Customer data is backed up according to a policy that is signed by every employee and it's the responsibility of the infrastructure team to guarantee its continuity. In the event of an exception a monitoring alarm is triggered, and personnel must perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS, with physical access restricted according to applicable AWS policies. All backups are encrypted with access restricted to key personnel via AWS IAM permissions.

Computer Operations – Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

InvGate monitors the utilization computing infrastructure for customers to ensure that service delivery matches service level expectations. InvGate has defined a standard level of usage of the cloud infrastructure and offers dedicated hosting if requested.

Cloud infrastructure capacity monitoring includes, but is not limited to, disk storage and memory consumption for all the applications needed to run the product and services provided by the InvGate system.

InvGate has implemented a patch management process to ensure contracted customer and cloud infrastructure systems are patched in accordance with the latest operating system patches.

The Security Officer, CTO and Infrastructure Manager are responsible for determining the urgency with which patches need to be applied, taking into account risk and service availability.

Change Control

InvGate has an ISO 9001 certified Design and Development Procedure which is part of the whole Systems Development Life Cycle (SDLC). Policies and procedures guide personnel in documenting and implementing application and infrastructure changes.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes.

Development policies and standards are documented so every developer is aware. Every change goes through a peer review process in which another developer reviews the written code. After that, the change is put through a set of automated tests that is constantly growing. The change is submitted to testing once all the automated tests passed correctly. Quality assurance testing is documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment.

Every piece of code implemented in InvGate's products goes through the whole process.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers

Data Communications

InvGate's products can be configured, and is highly recommended, so that data submitted through them travels encrypted.

Those requests are filtered by an AWS Web application firewall (WAF) that filters unauthorized inbound network traffic from the Internet. Access to the WAF configuration is only possible through AWS web application which access is limited to the members of the infrastructure team. If requested by the customer, InvGate can configure IP access restriction to incoming traffic.

InvGate cloud infrastructure is hosted in a virtual private cloud which access is restricted to a limited group of employees that need to use a VPN with a nominal private key.

Accesses always follow the principle of least privilege, that ensures that every employee must be able to access only the information and resources that are necessary for its legitimate purpose.

Penetration testing is conducted at least annually by a third party to measure the security posture of the products provided by InvGate. The third-party vendor uses an accepted industry standard penetration testing methodology. The third-party vendors run a bunch of tests in an environment separate from the production one. Once vulnerabilities are identified and categorized by severity, they are submitted to InvGate, and a retest date is agreed. Vulnerabilities include, but are not limited to, network and code

findings. During the retest a new version of the product is deployed and the third-party proceeds to determine if the vulnerabilities were fixed. Proper documentation of this process is delivered by the third party to InvGate

Boundaries of the System

The scope of this report includes the Services performed by InvGate. This report does not include the data center hosting services provided by AWS.

The applicable trust services criteria and the related controls

Common Criteria (Security)
Security refers to the protection of information during its collection or creation, use, processing, transmission, and storage and systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability
Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality
Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Good faith, integrity and ethical values are essential elements of InvGate's control environment and culture.

Integrity and ethical behavior are the product of InvGate's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Documented organizational policy statements, codes of conduct, organizational values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees with access to sensitive data

Commitment to Competence

InvGate's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence for every role
- Management has translated those competences into skills and knowledge levels required for open positions
- Training is provided to develop skills needed to perform required tasks
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

InvGate's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to working culture, that embraces an open dialogue among employees and management team focusing on the best way the organization can achieve its own and its customers' aims. The management philosophy emphasizes solving problems with accountability rather than guiltiness to reach this open dialogue.

It's the core responsibility of the management team analyzing, reviewing, taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is up to date on regulatory, trends and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole
- Meeting with middle management are held to discuss about the impact of this regulatory changes, trends and major initiatives

Organizational Structure and Assignment of Authority and Responsibility

InvGate's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. InvGate's structure is explained to every employee during its onboarding process. It is also properly documented in an org chart that can be inquired every time needed.

InvGate's assignment of authority and responsibilities comes with guidelines, process and key performance indicators that key personnel use to be aware of its own performance.

Escalations paths are established and documented so that employees are prepared to escalate an issue if they consider it is not handled the proper priority

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.
- A "Who is who" document is communicated and updated as needed

Human Resource Policies and Practices

InvGate's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. InvGate human resources policies and practices relate to employee hiring, onboarding, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- The candidates are carefully assessed at the hiring process, taking into consideration not only the skills to perform the role but also how they will match with the company culture, mission and values.
- New employees are required to sign acknowledgement policies and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on a biannual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.
- HR periodically performs assessments to improve internal equality and external competitiveness regarding Compensation and Benefits.

Risk Assessment Process

InvGate's risk assessment process identifies and manages risks that could potentially affect InvGate's ability to provide reliable services to user organizations.

This ongoing process is the responsibility of an independent organizational business unit by discussing with each team leader and identifying significant risks in their areas of responsibility that might affect the quality or reliability of the product or services provided to by InvGate. Then InvGate identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

Risks identified in this process are prioritized taking parameters which include, but are not limited to likelihood, business impact and control factors.

Periodic reports will be made to the senior leadership of InvGate to ensure risks are being mitigated appropriately, and in accordance with business priorities and objectives.

This process has identified risks resulting from the nature of the services provided by InvGate, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk – changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance – legal and regulatory changes

InvGate has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities

in the rapidly changing market environment. InvGate attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of InvGate's system; as well as the nature of the components of the system result in risks that the criteria will not be met. InvGate addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address those risks.

Information and Communications Systems

Information and communication is an integral component of InvGate's internal control system. People, processes, procedures and information systems work together and coordinate to run the operations of the company. Is crucial in that dynamic gathering data from the operations that will be converted into information.

At InvGate communications systems run a central role in the coordination of the operations. They are designed so that the information of the operation goes upwards from the daily operations to middle management and from middle management to upper management. At the same time, there are in place communications systems that pass on and coordinate InvGate's business needs, objectives and goals, from upper management to daily operations.

There is a fortnightly meeting held with the whole company where relevant cross teams' information is broadcasted to every employee. Those meetings are recorded and are available. Weekly meetings are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization.

There is a mandatory Slack channel used for general updates to entity-wide security policies and procedures which afterwards need to be signed by every employee.

Monitoring Controls

InvGate has defined several key performance indicators that have a strong relationship with business objectives and operational goals. These indicators have been discussed with the people that work with them. They are public and can be consulted when needed.

Management has set meetings in which responsibilities of the operations report on a regular basis the status of their duties, firstly with hard indicators, accompanied with qualitative analysis of those indicators and the operations itself. As output of those meetings is expected to reach conclusions regarding good

practices that need to be continued and deviations and action plans to redirect the operation towards the goals. If an external factor arises and operational goals need to be modified, an action plan is triggered.

Any taken measure has a responsibility and an ETA by when the task has to be completed. Different tracking resources are used to track these tasks, depending on various factor, including but not limited to, difficulty, complexity and amount of involved people.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to InvGate's Service and Asset Management Platform.

Subservice Organizations

InvGate's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to InvGate's services to be solely achieved by InvGate's control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of InvGate.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met.

Subservice Organization – AWS		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.

Subservice Organization – AWS		
Category	Criteria	Control
		Closed circuit television camera (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
		Access to server locations is managed by electronic access control devices.
Availability	A1.2	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment.
		AWS maintains a formal risk management program to identify, analyze, treat and continuously monitor and report risks that affect AWS' business objectives and regulatory requirements. The program identifies risks, documents them in a register as appropriate, and reports results to leadership at least semi-annually.
		AWS has a process in place to review environmental and geo-political risks before launching a new region.
		Access to server locations is managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
		Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers and third-party colocation sites where Amazon maintains the UPS units.

Subservice Organization – AWS		
Category	Criteria	Control
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units (unless maintained by Amazon), and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.
		AWS contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. The AWS contingency plan is tested on at least an annual basis.
		AWS maintains a capacity planning model to assess infrastructure usage and demands at least monthly, and usually more frequently (e.g., weekly). In addition, the AWS capacity planning model supports the planning of future demands to acquire and implement additional resources based upon current resources and forecasted requirements.

InvGate management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, InvGate performs monitoring of the subservice organization controls, including the following procedures

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

Complementary User Entity Controls

InvGate's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the SOC 2 Criteria related to InvGate's services to be solely achieved by InvGate's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of InvGate's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the SOC 2 Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to InvGate.
2. User entities are responsible for notifying InvGate of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of InvGate services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize InvGate services.
6. User entities are responsible for providing InvGate with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying InvGate of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

IV. Description of Design of Controls and Results Thereof

Description of Design of Controls and Results Thereof

Relevant trust services criteria and InvGate related controls are an integral part of management's system description and are included in this section. Sensiba San Filippo LLP performed testing to determine if InvGate controls were suitably designed to achieve the specified criteria for the Security, Availability, and Confidentiality set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria)*, as of July 25, 2022.

Criteria Number	Description of Company Controls	Result
CC1.0 - Control Environment		
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.		
CC1.1.1	The company has established a Code of Conduct and requires all employees to agree to it. Management monitors employees' acceptance of the code.	Control is suitably designed
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
CC1.2.1	The company demonstrates a commitment to integrity and ethical values by completing an annual review of ethical management and hiring practices.	Control is suitably designed
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
CC1.3.1	Company management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication and escalation. The organizational charts are made available to employees through the company's HR Information System to facilitate communication in their role with the company.	Control is suitably designed
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
CC1.4.1	All positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by the company.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
CC1.4.2	Background checks are performed on new hires, as permitted by local laws. The results are reviewed by HR and appropriate action is taken if deemed necessary.	Control is suitably designed
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
CC1.5.1	The company has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with the company's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete these trainings annually.	Control is suitably designed
CC1.5.2	Management has approved the company's security policies, and all employees agree to these procedures. Management also ensures that security policies are accessible to all employees and contractors.	Control is suitably designed
CC2.0 - Communication and Information		
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
CC2.1.1	The company uses a SOC 2 compliance platform called Vanta which objectively and continuously monitors the company's control environment and alerts management when internal control and security issues arise.	Control is suitably designed
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
CC2.2.1	The company has policies and procedures in place to establish access control of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must agree to the Access Control Policy on hire.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.		
CC2.3.1	The company maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	Control is suitably designed
CC2.3.2	The company maintains a Terms of Service that is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems. Where the Terms of Service may not apply, the company has Client Agreements or Master Service Agreements in place.	Control is suitably designed
CC3.0 - Risk Assessment		
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
CC3.1.1	The company's Risk Management Policy describes the processes the company has in place to identify new business and technical risks and how frequently those risks are mitigated.	Control is suitably designed
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
CC3.2.1	The company maintains a risk register that continuously documents risks facing the company and in-progress remediation programs to address those risks.	Control is suitably designed
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
CC3.3.1	The company identifies and performs forensics regarding potential fraud activity (e.g., fraudulent reporting, loss of assets, unauthorized acquisitions, etc.).	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.		
CC3.4.1	The company uses a SOC 2 compliance platform called Vanta which objectively and continuously monitors the company's control environment and alerts management when internal control and security issues arise.	Control is suitably designed
CC4.0 - Monitoring Activities		
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
CC4.1.1	Monitoring software is used to identify and evaluate ongoing system performance, changing resource utilization needs, and unusual system activity.	Control is suitably designed
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		
CC4.2.1	The company has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Control is suitably designed
CC4.2.2	The company provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	Control is suitably designed
CC5.0 - Control Activities		
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
CC5.1.1	A list of the company's system components is maintained for management's use in order to protect inventory from security events, maintain data confidentiality, and ensure system availability.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.		
CC5.2.1	The company has implemented a vulnerability management program to detect and remediate system vulnerabilities in software packages used in company infrastructure.	Control is suitably designed
CC5.2.2	A penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.	Control is suitably designed
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
CC5.3.1	Management has approved the company's security policies, and all employees agree to these procedures. Management also ensures that security policies are accessible to all employees and contractors.	Control is suitably designed
CC6.0 - Logical and Physical Access Controls		
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
CC6.1.1	Access to corporate network, production machines, network devices, and support tools requires a unique ID.	Control is suitably designed
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
CC6.2.1	Access to infrastructure and code review tools is granted to new employees subsequent to the initial request.	Control is suitably designed
CC6.2.2	Access to infrastructure and code review tools is removed as a component of the termination process.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
CC6.3.1	Access is restricted to authorized personnel. Access approval and modification to access list are logged. Access is removed when appropriate.	Control is suitably designed
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
CC6.4.1	The company relies on AWS's physical and environmental controls, as defined and tested within AWS SOC 2 efforts.	The Criterion is carved out and the responsibility of the subservice organization.
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.		
CC6.5.1	Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.	Control is suitably designed
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
CC6.6.1	Access to sensitive systems and applications requires two factor authentication in the form of user ID, password, OTP and/or certificate.	Control is suitably designed
CC6.6.2	The company implements firewalls and configures them to protect against threats from sources outside its system boundaries.	Control is suitably designed
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
CC6.7.1	Company management ensures that all company-issued laptop hard drives are encrypted using full disk encryption.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
CC6.7.2	Customer data stored in databases is encrypted at rest.	Control is suitably designed
CC6.7.3	Encryption is used to protect user authentication and administrator sessions of the internal admin tool transmitted over the Internet.	Control is suitably designed
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
CC6.8.1	The company deploys malware detection software on all workstations that can access the production environment and has configured malware detection software to perform daily scans with immediate notification if malware is detected.	Control is suitably designed
CC7.0 - System Operations		
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
CC7.1.1	The company has implemented a vulnerability management program to detect and remediate system vulnerabilities in software packages used in company infrastructure.	Control is suitably designed
CC7.1.2	A penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.	Control is suitably designed
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
CC7.2.1	The company uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system administrator.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		
CC7.3.1	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Control is suitably designed
CC7.3.2	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Control is suitably designed
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
CC7.4.1	The company has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Control is suitably designed
CC7.4.2	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Control is suitably designed
CC7.4.3	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Control is suitably designed
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.		
CC7.5.1	The company has created a Disaster Recovery Plan to define the organization’s procedures to recover information technology (IT) infrastructure and IT services within set deadlines in the case of a disaster or other disruptive incident.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC8.0 - Change Management		
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
CC8.1.1	The company uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system administrator.	Control is suitably designed
CC8.1.2	System changes must be approved by an independent technical resource prior to deployment to production.	Control is suitably designed
CC9.0 - Risk Mitigation		
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
CC9.1.1	The company's Risk Management Policy describes the processes the company has in place to identify new business and technical risks and how frequently those risks are mitigated.	Control is suitably designed
CC9.1.2	The company has created a Business Continuity Plan to define the criteria for continuing business operations for the organization in the event of a disruption.	Control is suitably designed
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.		
CC9.2.1	The company's team collects and reviews the SOC reports of its sub-service organizations on an annual basis.	Control is suitably designed
CC9.2.2	The company has implemented a Vendor Risk Management program with a framework for managing the lifecycle of vendor relationships.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
A1.0 - Additional Criteria for Availability		
A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.		
A1.1.1	Processing capacity and usage is monitored and expanded as necessary to provide for the continued availability of the system in accordance with system commitments and requirements.	Control is suitably designed
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.		
A1.2.1	The company relies on AWS's physical and environmental controls, as defined and tested within AWS SOC 2 efforts.	The Criterion is carved out and the responsibility of the subservice organization.
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
A1.3.1	Backups are performed daily and retained in accordance with a pre-defined schedule in the Backup Policy.	Control is suitably designed
A1.3.2	The entity has documented a disaster recovery plan that is tested annually to ensure that recovery procedures are complete and accurate.	Control is suitably designed
C1.0 - Additional Criteria for Confidentiality		
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
C1.1.1	Management has approved the company's security policies, and all employees agree to these procedures. Management also ensures that security policies are accessible to all employees and contractors.	Control is suitably designed
C1.1.2	Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
C1.2.1	Procedures are in place to erase or otherwise destroy confidential information that has been identified for destruction.	Control is suitably designed