Ignite Procurement AS

SOC 2 REPORT

FOR

Ignite System

A TYPE 1 INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS RELEVANT TO SECURITY

August 26, 2021

Attestation and Compliance Services
by Prescient Assurance LLC.

Table of Contents

SECTION 1

Management's Assertion

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Ignite's system as of August 26, 2021, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report. The description is intended to provide report users with information about Ignite's system that may be useful when assessing the risks arising from interactions with Ignite's system, particularly information about system controls that Ignite 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 set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Ignite uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Ignite, to achieve Ignite's service commitments and system requirements based on the applicable trust services criteria. The description presents Ignite's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Ignite's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Ignite, to achieve Ignite's service commitments and system requirements based on the applicable trust services criteria. The description presents Ignite's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Ignite's controls.

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

a. the description presents Ignite's system that was designed and implemented as of August 26, 2021, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of August 26, 2021, to provide reasonable assurance that Ignite'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, and if the subservice organization and user entities applied the complementary controls assumed in the design of Ignite Procurement AS's controls as of that date.

DocuSigned by:
Iuliia Thuen
C54165A8ABB4454...

Iuliia Thuen
Chief Operating Officer
Ignite Procurement AS
September 3, 2021

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Ignite Procurement AS

Scope

We have examined Ignite Procurement AS's ("Ignite") accompanying description of its system as of August 26, 2021, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, and the suitability of the design of controls stated in the description as of August 26, 2021, to provide reasonable assurance that Ignite's service commitments and system requirements were achieved based on the trust services criteria relevant to security set forth in TSP 100, 2017 Trust Services Criteria for Security.

Ignite Procurement AS uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Ignite, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents Ignite's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Ignite's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or Implementation and Design Effectiveness of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Ignite, to achieve Ignite's service commitments and system requirements based on the applicable trust services criteria. The description presents Ignite's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Ignite's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or Implementation and Design Effectiveness of such controls.

Service Organization's Responsibilities

Ignite 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 Ignite's service commitments and system requirements were achieved. In Section 1, Ignite has provided the accompanying assertion titled "Management's Assertion" (assertion) about the description and the suitability of design of controls stated therein. Ignite 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 AICPA. 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:

- 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.

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 Matters

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 Ignite's system that was designed and implemented as of August 26, 2021, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of August 26, 2021, to provide reasonable assurance that Ignite'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 and if the subservice organization and user entities applied the complementary controls assumed in the design of Ignite's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Ignite, user entities of Ignite's system as of August 26, 2021, business partners of Ignite subject to risks arising from interactions with the system, 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, and other parties.
- Internal control and its limitations.
- Complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- 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.

Prescient Assurance LLC

DocuSigned by:
John D Wallace
F5ADFA3569EA450...

John D. Wallace, CPA
September 3, 2021
Signal Mountain, TN

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Overview and Background

Ignite Procurement is a Norwegian SaaS company facilitating data-driven, smarter, and sustainable procurement decisions through its best-of-breed spend management solution. With the ever-increasing importance of technology and data in all aspects of business decision making, Ignite Procurement aims to become the number one player within strategic procurement. The company was founded by Sigbjørn Nome and Børge Langedal in 2016.

Overview of Products and Services

Ignite Procurement is a Norwegian SaaS company facilitating data-driven, smarter, and sustainable procurement decisions through its best-of-breed spend management solution.

The application covers:

- Data Management – import, consolidate, transform, classify, clean and enrich spend data.
- Procurement Analytics – transform your data into actionable insights.
- Category Management – harness the potential of digital category management.
- Contract Management – unlock the full value from every contract.
- Supplier Management – manage your suppliers and empower the collaboration with your suppliers.
- Initiative and Tasks – keep track of procurement activities across your team

Users can access our web application from anywhere to get insight and work with their strategic procurement processes in a data-driven and smarter way.

Principal Service Commitments and System Requirements

Security commitments to user entities are documented and communicated in our Terms and Conditions and its appendixes and other customer agreements. The agreements define how we shall handle client data and our security obligations. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design within the application
- How Ignite Procurement are handling of client data
- The Ignite Procurement application is 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 both at rest and in transit.

Ignite Procurement establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Ignite Procurement policies and procedures, and in contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, 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 Ignite Procurement application.

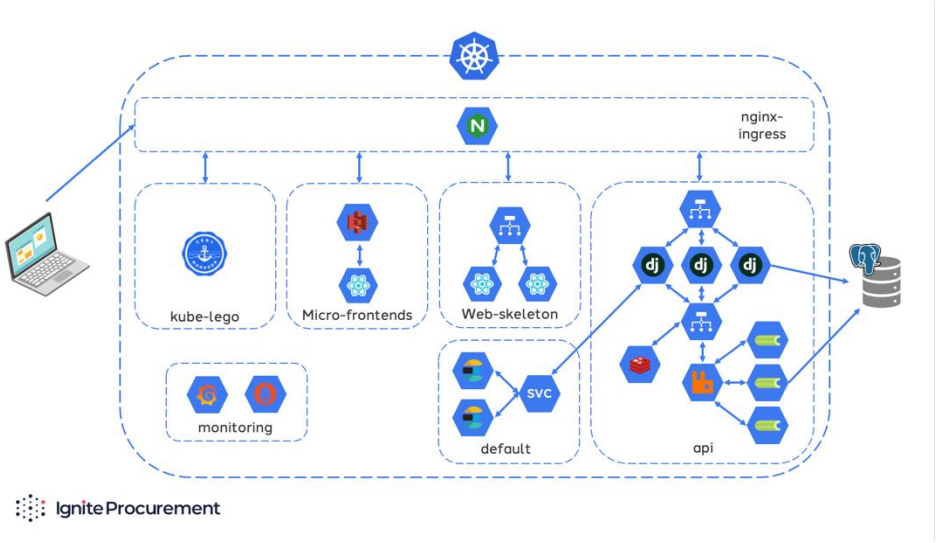
Components of the System Used to Provide the Services Infrastructure

System Infrastructure

Primary infrastructure used to provide Ignite's Services system includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
GCP	Hosted Kubernetes	Kubernetes, also known as K8s, is an open-source system for automating deployment, scaling, and management of containerized applications.
GCP	Cloud SQL	Fully managed relational database service for MySQL, PostgreSQL, and SQL Server.
GCP	Cloud Storage	Static File Storage
Github	Github Actions	CI / CD system to produce containers from source code and buildpacks, perform unit and integration tests on built containers, and deploy containers to staging and production environments
AWS	s3	Static File Storage

Software



Primary software used to provide Ignite Procurement's Services system includes the following:

Primary Software		
Software	Operating System	Purpose
Django/ Django Rest framework	Linux	Primary ORM framework and server application for all Ignite Procurement's internal and external api.
React Typescript		Web application framework used to power the Ignite Procurement's web application.
PostgreSQL	Linux	Transactional database for Ignite Procurement's data
RabbitMQ	Linux	Used to maintain the Ignite Procurement's job queue for async tasks.
Celery	Linux	Running async task jobs for Ignite Procurement's main server.
Redis	Linux	Cache engine for task results and api requests.
Elasticsearch	Linux	Document database of customer data for rapid search and data analysis.

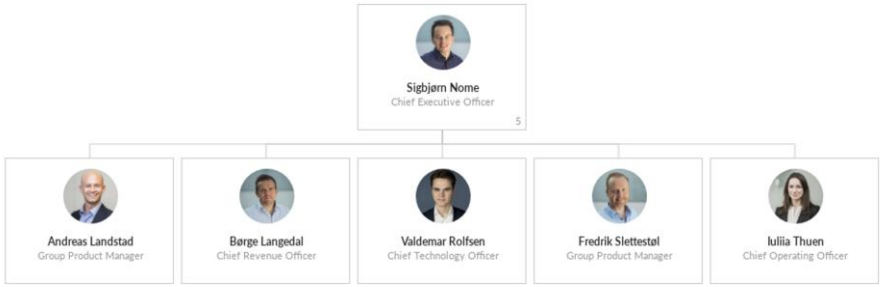
In addition to the mentioned technologies used for providing Ignite Procurement's services, we utilize subcontractors such as Sentry (used for error-monitoring), Intercom (used for customer support chat and communication) and Prometheus (used for server monitoring)

People

Ignite Procurement has a staff of approximately 46 employees organized in the following functional areas:

- Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.
- Product: Product Managers, Product Designers, Tech Leads, QA Leads, Data Scientist and Software Engineers who design and maintain the Ignite product offering, including the web interface, the API's, the job queuing infrastructure, and all debugging tools. This team designs and implements new functionality, assesses, and remediates any issues or bugs found in the product, and architects and deploys the underlying cloud infrastructure on which Ignite runs. Members of the product team are responsible for peer reviews of code and infrastructure designed and authored within the team. The product team is also monitoring and maintaining the product, which involves proactively designing and deploying monitoring software and tools to help identify errors or bugs in the Ignite product offering. The team is also ensuring the Ignite is using the correct cloud infrastructure and scale to maintain high sync performance. Finally, the product org is responsible for responding to any potential security issues with Ignite and notifying affected customers if applicable.
- Commercial: Individuals with commercial roles work to market, sell, and support our users. They are usually the primary point of contact to Ignite customers. They help identify how we can make impact and create value for our prospective customers, and existing once. In the marketing role, Ignite employees identify best practices and educate the market to ensure that prospects get more mature with how the work with strategic procurement via webinars, blog posts, white papers, SOME and other channels. Finally, the customer success team ensures that our customers can use the product effectively and help them with configuration and setup. By assisting customers with onboarding into the product, helping identify useful

data sources, analysis, and proper training.



Data

There are four major types of data used by Ignite Procurement:

- Configuration data: Data used to configure the use of Ignite Procurement's services.
- Global Data: Data fetched from Ignite Procurement's supplier sources and aggregated data created by Ignite Procurement. These sources may include both free/public and proprietary/paid suppliers. The global data is used to provide valuable information to Ignite Procurement's customers.
- Customer Data: Data owned by Ignite Procurement's customers that they upload to Ignite Procurement's services either manually or by integrating with their data warehouses. It also includes data manually created within Ignite Procurement's services by the customer.
- Log Data: Logs, traces, and samples produced by the Ignite Procurement's services while performing operations, either on behalf of the customer or while doing sync tasks with Ignite Procurement's subcontractors.

Configuration Data

Configuration data is mostly stored in Ignite Procurement's primary PostgreSQL databases and includes:

- Ignite Procurement's customers' email addresses, names, and company names
- Credentials for accessing customers data warehouses, including usernames, passwords, OAuth tokens, and certificates.
- The names of data tables and columns that the customer have configured for their customer data.
- Configuration objects that determine how, and how often, data should be fetched for customers that have integrated data connection.
- Configuration objects that build queries for the data the customer sees on their dashboards

Configuration Data is treated as sensitive by Ignite Procurement. Access controls limit configuration data access to each customer's Ignite Procurement organization. Customers can invite other people in their company to access their Ignite Procurement organization and read and write configuration data. Ignite Procurement operators may access configuration data to troubleshoot customer issues or to gather feedback for improving the Ignite Procurement 's product.

Global Data

Global data is treated as sensitive by Ignite Procurement. Not all customers have access to all the different global data, depending on the access to the source of the global data in question.

Customer Data

Customer data is the most sensitive data in the Ignite Procurement system. Ignite Procurement takes several safety precautions to ensure that customer data is kept confidential, as our customers trust us to do.

Log Data

Log data is produced by Ignite Procurement's services to make it easier for Ignite Procurement's operators to monitor the health of the system and track down any issues. Log data is a trace of the actions performed by the system before the log is sent. Log data will include snapshots of the request the system received, so operators can see what the system was attempting to do. Log data also includes stack traces and samples of running code. Due to the nature of logging frameworks, there is a small possibility that log data can also include some **Customer Data** captured by automatic tracers. Log data may be stored by vendors that Ignite Procurement has entrusted for purposes like indexing, monitoring, and trending. Regardless of whether log data is stored within Ignite Procurement's own databases or by vendors, it is given a limited lifetime and automatically removed.

Data Protection

All communication should be encrypted, not only for server-to-client communication but also from server-to-server inside a data center. Therefore, for all relevant services, TLS connections are enforced with certificates generated from Let's Encrypt [1].

The platform database is hosted on the Google Cloud Platform (GCP) using Cloud Storage. Cloud Storage manages server-side encryption keys on the Platform's behalf using the same hardened key management systems that Google uses for their own encrypted data, including strict key access controls and auditing. Cloud Storage encrypts user data at rest using AES-256.

Today the platform uses a multitenant system architecture which means that the software runs on a single instance server that serves multiple tenants. The security of the data for all customers of the Platform is safeguarded through a robust relational database structure that combined with appropriate practices for code reviews ensures the safety of the data.

Further server permissions for the Platform are managed through IAM solutions to ensure that the right people have the right level of access to the different resources used in the platform. The access rights are delegated based on the principle of least privilege which states that every module must be able to access only the information and resources that are necessary for its legitimate purpose. Furthermore, IAM-access keys are only stored encrypted with strict access and are updated on a regular, recommended basis.

Business Processes and Procedures

Formal IT and Non-IT Business Processes and procedures exist that describe how service commitments are met.
They are described below:

Customer success

- All customers follow a thorough on-boarding process of 6-10 weeks: establishing way of working, validating data, and set mutual success plan

- Monthly status meeting after on-boarding to ensure mutual success plan is reached and to ensure effective operations
- Scheduled weekly checkups in periods to solve immediate issues and/or to expand to new modules
- Live chat functions during office hours for immediate support and Help center articles for support after hours

Product Teams
- Bugs that are reported are assigned a priority in relation to the company SLA
- Errors in the platform are logged and developers are alerted about these errors

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

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. Integrity and ethical values are essential elements of Ignite Procurement's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Ignite Procurement'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.

The code of conduct outlines the company's expectations measured against the highest possible standards of ethical business conduct. Committing to the highest standards helps Ignite Procurement hire great people, build great products, and attract loyal customers.

The code of conduct covers
- Respectful workplace
- Safe workspace
- Workspace visitors
- Equal opportunity employment
- Professionalism
- Conflict of interest
- Internet and social media
- Enforcement

Commitment to Competence

Ignite Procurement 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 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 levels for jobs and translated required skills and knowledge levels into written position requirements.
- Training and coaching are provided to maintain the skill level of all personnel.
- Onboarding program is established to ensure a common understand of our business, processes and routines for all new employees.

Management's Philosophy and Operating Style

Ignite Procurement management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative towards of the highly-sensitive data and workflows our customers entrust to us.

The management team meets every quarter to be briefed on technology changes that impact the way Ignite Procurement can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Ignite Procurement to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

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

- Management, including CTO, that is also chief security officer, is periodically briefed on regulatory 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.
- The topics are periodically discussed in the Board of Directors meetings.

Organizational Structure and Assignment of Authority and Responsibility

Ignite Procurement is currently organized in a simple, relatively flat structure with five employees reporting directly to the CEO/CPO: CTO, CRO, COO and two Group Product Managers. The next level of the organization comprises of 3 VPs (Sales, Customer Success and Marketing) and the rest of organization is reporting either to C level, VPs or Group Product Managers level without further hierarchy. As the team grows, management will elect to build an organizational structure that ensures that employees clearly understand their role in the organization, how they and their team are responsible for furthering company-wide initiatives, and channels for reporting upward and downward in the organizational hierarchy.

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 on the intranet.

Human Resource Policies and Practices

Ignite Procurement's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Ignite Procurement's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and termination.

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

- New employees are required to accept Ignite's Code of Conduct policy and a confidentiality agreement as a part of the signing contract.
- Written performance evaluations for each employee are performed on an annual basis while typically performance chat is conducted on a 6 month basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist in our HR system.

Security Management

Ignite Procurement has a dedicated information security team consisting of a security officer and tech leads responsible for management of information security throughout the organization. They hold positions on the Security Steering Committee and maintain security credentials and are required to annually sign and acknowledge their review of the information security policies. They are responsible for developing, maintaining, and enforcing Ignite's information security policies. The information security policy is reviewed annually by the security officer, CTO, and COO, and it is approved by the Security Steering Committee.

As the information security team maintains security, it monitors known incidents and patches as well as results from recent vulnerability assessments and addresses necessary changes to the policies and procedures. Such changes can include a reclassification of data, a reassessment of risk, changes in incident response plans, and a verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during weekly IT maintenance meetings or through system alerts.

During annual security training and awareness programs, management ensures communication of the latest security policies as well as written job descriptions for security management.

Additionally, management is responsible for ensuring business associate agreements are current for third parties and for updating the annual IT risk assessment.

Security Policies

The following security policies and related processes are in place:

- Acceptable Use Policy
- Access Control and Termination Policy
- Business Continuity and Disaster Recovery Plan
- Change management Policy
- Code of Conduct
- Configuration and Asset Management Policy
- Data Retention and Disposal Policy
- Encryption and Key Management Policy
- Information Security Policy
- Internal Control Policy
- Network Security Policy
- Performance Review Policy
- Physical Security Policy
- Risk Assessment and Treatment Policy
- Secure Development Policy
- Security Incident Response Plan
- Vendor Management Policy
- Vulnerability and Patch Management Policy

Personnel Security

All Ignite Procurement personnel will undergo a required reference check. An authorized member of Ignite Procurement must contact a reference either from a previous employer or from the university to confirm the person's identity. Prior to accessing sensitive information, personnel are required to sign an industry-standard confidentiality agreement protecting Ignite Procurement confidential information. Ignite Procurement has a security awareness training program in place to promote the understanding of security policies and procedures. All personnel

are required to undergo training following initial employment and annually thereafter. Completion of the training program is logged by Ignite Procurement. All employees, clients and partners are asked to report any incident or security risk to the incident help desk.

Physical Security and Environmental Controls

Ignite Procurement personnel are required to ensure that all sensitive information in hardcopy or electronic form is secure in their work area when it is unattended. Hardcopies of sensitive information shall be removed from desks and lock the information in a drawer when desks are unoccupied and at the end of the workday. Keys used to access sensitive information must not be left at an unattended desk.

Employees and contractors must be aware of their surroundings at all times and ensure that no unauthorized individuals have access to see or hear sensitive information. All mobile and desktop devices must be locked when unoccupied. Session time-outs and lockouts are enforced through technical controls for all systems containing covered information. All devices containing sensitive information, including mobile devices, shall be configured to automatically lock after a period of inactivity (e.g. screen saver).

Any Ignite Procurement issued devices used to access company applications, systems, infrastructure, or data must be used only by the authorized employee or contractor of such device. Employees or contractors accessing the Ignite Procurement network or other cloud-based networks or tools are required to use HTTPS/TLS 1.1+ at a minimum to protect data-in-transit. In a public space, employees must ensure your sight lines are blocked and do not have customer conversations or other confidential conversations. If someone is close to you, assume they can see and hear everything. Connecting directly to a public wireless network that doesn't employ, at minimum, WPA-2 or an equivalent wireless protocol is prohibited. While working at home, employees and applicable contractors should be mindful when visitors (e.g. maintenance personnel) are at their residences, as visitors could become privy to sensitive information left up on computer screens.

The Physical Security Policy specifies the requirements for physically protecting assets and their data via physical controls and safeguards. Physical security is the first line of defense in information security - without physical protections, virtual protections offer minimal security for assets and data. Ignite Procurement maintains reasonable steps to ensure that its facilities, information systems, and data are accessed only by authorized personnel or authorized third party visitors to prevent unauthorized access, damage, theft, and interference. All physical security requirements are applicable to both remote and in-office work. Key aspects of physical security include: perimeter and border security, entry controls, visitor management, restricted areas, equipment protection and maintenance, awareness and training, and risk management.

Change Management

All change requests must be documented end-to-end via the Ignite Procurement change management and ticketing tools.

Change management should be conducted according to the following procedure:

(1) Product Roadmap
The Ignite Procurement product management team evaluates which change requests and features will be implemented based on their alignment with the business plan and the overall level of effort required. All change requests should be prioritized in terms of benefits, urgency, effort required, security impacts, and other potential impacts on the organization’s operations.

A ticket should be created to track a change request at the onset. If the change is part of an existing ticket the original ticket may be used and modified appropriately.

(2) Planning and Evaluation
Plan and evaluate the change. This may include design, scheduling, and implementation of a communications plan, testing plan, and roll-back plan. During planning, wire-frames, mockups, and functional requirements may be created and reviewed among the applicable team members. The team may set priority levels of the service and may determine any risk that the proposed change introduces to the system.

The scope and impact of the change should be determined during this phase. If possible, specific use cases should also be determined.

(3) Build, Test, and Document
In this step Ignite Procurement sprints may be defined and the overall software design and development happens.

UI/UX and other optimizations should occur to enhance the performance and security of the change across all platforms.

The changes must be tested in the Ignite Procurement staging environment before release to production. Test setups and scenarios are built for operational, performance, and security testing. Automated test scripts should be developed, used, and updated as changes occur.

The appropriate teams work to create documentation such as release notes, help articles, and blog posts applicable to the changes. Existing documentation is updated to ensure that team members and customers have the most up-to-date and accurate information. Customer-facing documentation should be provided to Ignite Procurement customers as applicable.

(4) Code Review
Ignite Procurement uses code reviews to maintain the quality of Ignite Procurement code and products.

Secure Coding
Secure coding practices are incorporated into the development lifecycle and security architecture of Ignite Procurement. Engineers at Ignite Procurement are responsible for defining security requirements early in the software development life cycle and then evaluating for compliance with those requirements.

All engineers at Ignite Procurement are responsible for reviewing the OWASP top 10 web application security risks.

(5) Approval and Implementation
Once the new release is ready and the appropriate documentation is in place, the new release may be pushed to the production environment after the appropriate review and approval by the appropriate product owner. Automation test suites should be used across all production environments.

Access to push changes to production at Ignite Procurement must be restricted to a limited set of authorized team members and the engineer responsible for coding the change should not also be responsible for pushing the change to production, unless approved by management.

(6) Communication
Implemented changes should be communicated to all applicable team members and externally as appropriate.

(7) Post-Change Review
Ignite Procurement continuously measures the success of new releases and identifies areas that can be enhanced further in the future.
The appropriate team may conduct a post-implementation review to determine how the change is impacting Ignite Procurement and our customers, either positively or negatively. Discuss and document any lessons learned with product management and other appropriate team members.

System Monitoring

Ignite Procurement collects & monitors audit logs and alerts on key events stemming from production systems, applications, databases, servers, message queues, load balancers, and critical services, as well as IAM user and admin activities. Ignite Procurement manages logging solution(s) and/or SIEM tool(s) to collect event information of the aforementioned systems and activities. Ignite Procurement implements filters, parameters, and alarms to trigger alerts on logging events that deviate from established system and activity baselines. Logs are securely stored and archived for a minimum of 1 year to assist with potential forensic efforts.

Logs are made available to relevant team members for troubleshooting, auditing, and capacity planning activities. System and user activity logs may be utilized to assess the causes of incidents and problems. Ignite Procurement utilizes access control to prevent unauthorized access, deletion, or tampering of logging facilities and log information.

When various logging and alerting solutions and mechanisms give rise to events and alerts, Ignite Procurement correlates those events and alerts across all log sources to identify root causes and formally declare incidents, as necessary, in accordance with the Security Incident Response Policy and Change Management Policy.

Additionally, Ignite Procurement utilizes threat detection solution(s) to actively monitor and alert on network and application-based threats.

Incident Management

The Security Incident Response Plan provides a systematic incident response process for all Information Security Incident(s) (defined below) that affect any of Ignite Procurement's information technology systems, network, or data, including Ignite Procurement data held or services provided by third-party vendors or other service providers. From time to time, Ignite Procurement may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations.

This plan applies to all Ignite Procurement assets utilized by personnel acting on behalf of Ignite Procurement or accessing its applications, infrastructure, systems or data. All personnel are required to read, accept and follow all Ignite Procurement policies and plans.

The process outlined below should be followed by the appropriate Staff at Ignite Procurement in the event of an Information Security Incident. Ignite Procurement shall assign resources and adopt procedures to timely assess automated detection results, screen internal and external

reports, and identify actual information security events. Ignite Procurement shall document each identified Information Security Incident.

Detection and Reporting

Automated Detection
Ignite Procurement may utilize automated detection means and other technical safeguards to automatically alert the Ignite Procurement of incidents or potential incidents.
Report from Ignite Procurement Personnel
All Ignite Procurement personnel must report potential security incidents.

Report from External Source
External sources, including our customers, who claim to have information regarding an actual or alleged information security incident should be directed to security@ignite.no.

Response Procedures

Responding to a data breach typically involves the following stages:

- verification
- assessment
- containment and mitigation
- post-breach response

All of the steps must be documented in an incident log and/or corrective action plan.

The data breach response is not purely linear, as these stages and the activities associated with these stages frequently overlap. Ignite Procurement may keep a record of any actions the organization takes in responding to the incident and preserve any evidence that may be relevant to any potential regulatory investigation or litigation including through use of an incident log, corrective action plan or other applicable documentation.

(1) Verification
The SRT will work with Ignite Procurement employees and contractors to identify the affected systems or hardware (such as a lost laptop or USB drive) and determine the nature of the data maintained in those systems or on the hardware.

(2) Assessment
Following verification of an Information Security Incident, the SRT will determine the level of response required based on the incident's characteristics, including affected systems and data, and potential risks and impact to Ignite Procurement and its customers, employees, or others.
Such assessment may include what employees or contractors were affected, what customers were affected, and what data was potentially exfiltrated, modified, deleted or compromised.

The SRT will work together to assess a priority with respect to the incident based on factors such as whether:

- the incident exposed or is reasonably likely to have exposed data; or
- personally identifiable information was affected and the data elements possibly at risk, such as name or date of birth.

In addition, the SRT will consider whether the disclosure was:

- internal or external;
- caused by a company insider or outside actor; and/or
- the result of a malicious attack or an accident.

Lastly, if an information security breach has occurred, federal/country-wide law enforcement and local law enforcement should be contacted and informed of the breach. Law enforcement should be contacted in alignment with applicable breach notification laws. External general counsel should lead law enforcement communication efforts (in collaboration with SRT). If general counsel is not available, SRT should lead law enforcement communication efforts.

(3) Containment and Mitigation
As soon as Ignite Procurement has verified and assessed the breach, the SRT may take all necessary steps to contain the incident and return the Ignite Procurement systems back to their original state and limit further data loss or intrusion.

(4) Post-Breach Response
Any post-breach response including external and internal communications, notifications, and further inquiries will depend on the assessment and priority of the data breach.

As part of the final response, Ignite Procurement will review applicable access controls, policies and procedures and determine whether to take any actions to strengthen the organization's information security program.

As soon as possible, Ignite Procurement senior management should meet with the SRT and other relevant team members of the Ignite Procurement for a post-mortem to better understand the disaster event that took place and how it and others may be prevented in the future.

The retrospective should be documented and key learnings from the retrospective should be presented to all appropriate team members in a timely manner.

Data Backup and Recovery

Ignite Procurement maintains a plan for continuous business operations if facilities, infrastructure or systems fail. The plan is tested, reviewed and updated at least annually. Backups are performed according to the appropriate backup schedules to ensure critical systems, records, and configurations can be recovered in the event of a disaster or media failure.

Ignite Procurement maintains requirements and controls for the separation of development and production environments.

System Account Management

Ignite Procurement adheres to the principle of least privilege, specifying that team members will be given access to only the information and resources necessary to perform their job functions as determined by management or a designee. Requests for escalation of or changes to privilege and access are documented and require approval by an authorized manager. System access is revoked upon termination or resignation. Audits of access and privileges to sensitive Ignite Procurement applications, infrastructure, systems, and data are performed and reviewed by authorized personnel.

Unique accounts and passwords are required for all users. Passwords must be kept confidential

and not shared with multiple users. Where possible, all user and system accounts must have a minimum of eight characters including alpha (upper and lower case), one numeric and one non-alphanumeric character. All accounts must use unique passwords not used elsewhere. Passwords must only be stored using a Ignite Procurement approved password manager. Ignite Procurement does not hard code passwords or embed credentials in static code. If a password is suspected to be compromised, the password should be rotated immediately and the security team should be immediately notified.

Risk Management Program

Data Classification

Public Data

Public data is information that may be disclosed to any person regardless of their affiliation with Ignite Procurement. The Public classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to data that does not require any level of protection from disclosure. While it may be necessary to protect original (source) documents from unauthorized modification, public data may be shared with a broad audience both within and outside Ignite Procurement and no steps need be taken to prevent its distribution. Public data can be retained for an indefinite period of time.

Internal Data

Internal data is information that is potentially sensitive and is not intended to be shared with the public. Internal data should be classified as such when the unauthorized disclosure, alteration, or destruction of that data would result in moderate risk to Ignite Procurement, its customers, or its partners. Internal data generally should not be disclosed outside of Ignite Procurement without the permission of the person or group that created the data. It is the responsibility of the data owner to designate information as Internal where appropriate.. Internal data can be retained for an indefinite period of time.

Confidential Data

Confidential data is information that, if made available to unauthorized parties, may adversely affect individuals or Ignite Procurement. This classification also includes data that Ignite Procurement may be required to keep confidential, either by law or under a confidentiality agreement with a third party, such as a vendor. This information should be protected against unauthorized disclosure or modification. Confidential data should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or transported. Confidential data should be retained for only as long as it is needed to conduct internal/external business operations. Customer deletion requests and contractual deletion obligations should be the main source of authority for storing/deleting Confidential data, as applicable.

Restricted Data

Restricted data includes any information that Ignite Procurement has a legal or regulatory obligation to safeguard in the most stringent manner. Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to Ignite Procurement, its customers, or its partners. The highest level of security controls should be applied to Restricted data.

Restricted data should be used only when no alternative exists and must be carefully protected. Regulatory data retention requirements should be the main source of authority for storing/deleting restricted data, as applicable, unless stricter organizational requirements have been enacted.

Risk Management Responsibilities

All covered personnel that are included in IT risk assessment activities are responsible for adhering to this policy and with any local Risk Assessment requirements.

ROLE	DEFINITION
Management	Management is responsible for the sponsorship and support of the Risk Management Plan and process, participating on the Risk Management Council, the review and approval of risk assessments and control recommendations and reporting to the BOD what mitigationactions have been taken.
Security Liaison	Security Liaisons are responsible for conducting the risk assessments, analyzing the risk and recommending controls, presenting risks for approval, documenting the process and managing and facilitating the implementation of controls.
System-Owner/ Administration	System Owners/Administrators are responsible for participating in the identification and analysis process, participating on the Risk Management Council and for the implementation of technical controls
Solution Managers	Managers in the functional areas are responsible for participating in the risk identification and analysis process, providing some participation on the Risk Management Council, and for the implementation of administrative controls.
Board of Directors	The BOD is responsible for general oversight. The BOD approves this policy and reviews all identified risks, approves the planned course of action, and ensures risks identified that require action have been followed through to remediation. The BOD also sets risk appetite.

Risk Management Policy

This Risk Assessment Policy guides Ignite Procurement in performing risk assessments to account for threats, vulnerabilities, likelihood, and impact to Ignite Procurement assets, team members, customers, vendors, suppliers, and partners based upon the Ignite Procurement services considering security, availability, and confidentiality needs.

Ignite Procurement conducts assessments of risk, which include the likelihood and impact of harm from the unauthorized access, use, disclosure, disruption, modification and/or destruction of Ignite Procurement systems, applications, infrastructure, and the data processed, stored or transmitted by such.

The risk assessment process is coordinated by collaboration between CTO and COO, identification of threats and vulnerabilities is performed by asset owners, and assessment of consequences and

likelihood is performed by the risk owner.

A risk assessment may include a review of:

- internal controls including policies, procedures, and implemented security safeguards
- human resource practices related to hiring, termination, and discipline procedures
- facility controls
- systems and applications used to collect, store, process or transmit confidential data

For each risk, a risk owner has to be identified – the person or organizational unit responsible for each risk. This person may or may not be the same as the asset owner. Once risk owners have been identified, it is necessary to assess consequences for each combination of threats and vulnerabilities for an individual asset if such a risk materializes.

Risk Management Program Activities

The Risk Assessment Policy guides Ignite Procurement in performing risk assessments to account for threats, vulnerabilities, likelihood, and impact to Ignite Procurement assets, team members, customers, vendors, suppliers, and partners based upon the Ignite Procurement services considering security, availability, and confidentiality needs.

This policy applies to all Ignite Procurement assets utilized by personnel acting on behalf of Ignite Procurement or accessing its applications, infrastructure, systems, or data. All personnel are required to read, accept, and follow all Ignite Procurement policies and plans.

Ignite risk management program consist of

- risk assessment framework
- risk assessment process
- exceptions
- enforcement
- responsibility, review and audit.

The risk assessment process includes the following activities

- Scoping assets
- Identifying threats and vulnerabilities
- Analyze risks
- Risk treatment including risk migration, risk transfer and risk acceptance
- Calculated residual risk
- Reporting

Risk Assessment

Ignite Procurement conducts assessments of risk, which include the likelihood and impact of harm from the unauthorized access, use, disclosure, disruption, modification and/or destruction of Ignite Procurement systems, applications, infrastructure, and the data processed, stored or transmitted by such. The risk assessment process is coordinated by COO and CTO, identification of threats and vulnerabilities is performed by asset owners, and assessment of consequences and likelihood is performed by the risk owner.

A risk assessment may include a review of:

- internal controls including policies, procedures, and implemented security safeguards
- human resource practices related to hiring, termination, and discipline procedures
- facility controls
- systems and applications used to collect, store, process or transmit confidential data Risk Assessment Process at Ignite Procurement should align with the following steps:

In order to begin the risk assessment process, the assessor should determine the scope of what needs to be covered in the assessment. An effective assessment should be limited in its scope to the applicable assets.

Such scope may include:

- Review inventory of critical system assets (hardware, software, facilities, etc.)
- Identification of data owners (electronic and non-electronic data)
- Identification of workforce members with access to stored data by hardware/software
- Mapping data flow through Ignite Procurement and vendor systems
- Conducting an inventory of data storage (including non-electronic data)
- System characterization (e.g. essential, non-essential)

Vulnerabilities and threats, both internal and external, to Ignite Procurement operations (including, but not limited to, its mission, functions, image, or reputation), assets, information, and individuals may be identified and documented as part of the Ignite Procurement risk assessment.

A threat is any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, or other organizations, through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. [SP 800-30 Rev.1]

A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. [SP 800-30 Rev.1]

Such identification steps may include:

- Security control analysis
- Identification of relevant patterns, practices, or specific activities that indicate possible identity theft

Risk Analysis

For each risk, a risk owner has to be identified – the person or organizational unit responsible for each risk. This person may or may not be the same as the asset owner. Once risk owners have been identified, it is necessary to assess consequences for each combination of threats and vulnerabilities for an individual asset if such a risk materializes:

Initial (or Inherent) Risk Likelihood Determination

How likely will an identified threat or vulnerability impact the organization given existing security controls?

The likelihood of occurrence is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities).

Description	Likelihood Level	Likelihood Score
A threat that is highly likely to occur without adequate and effective security controls.	Very High	5
A threat that is likely to occur with little to no security controls and a high level of probability.	High	4
A threat that could occur but has been protected against with minimal security controls or the probability of risk is moderate without such controls.	Moderate	3
A threat that may occur but is unlikely given the low probability of the risk or security controls taken.	Low	2
A threat that is highly unlikely to occur given the very low probability of the risk or security controls taken.	Very Low	1

Initial (or Inherent) Risk Impact Analysis

What is the cost if an identified threat or vulnerability impacts the organization given existing security controls?

The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Description	Impact Level	Impact Score
Any loss due to this threat will have an immediate and material effect on the organization's legal, regulatory or contractual obligations or its operations, cash flow or reputation.	Very High	5
Any loss due to this threat may have an immediate and significant effect on the organization's legal, regulatory or contractual obligations or its operations, cash flow or reputation.	High	4
Any loss due to this threat may have a moderate effect on the organization's legal, regulatory or contractual obligations or its operations, cash flow or reputation.	Moderate	3
Any loss due to this threat may have a non-material effect on the organization's legal, regulatory or contractual obligations or its operations, cash flow or reputation.	Low	2
Any loss due to this threat will not affect legal, regulatory or contractual obligations or its operations, cash flow or reputation.	Very Low	1

Initial (or Inherent) Risk Score

After the likelihood and impact analysis, a risk determination should be made. Risk is a function of the likelihood of a threat event's occurrence and potential adverse impact should the event occur. In order to determine risk score, Ignite Procurement multiplies impact * likelihood. The higher number equating to higher potential risk.

Risk Response

For any critical or high threats and vulnerabilities identified during the risk assessment process, Ignite Procurement will immediately determine the associated risks and develop action plans to mitigate those risks including, but not limited to patching of vulnerable systems and/or applying other control activities. Risk responses shall consider industry or organizational laws, regulations or standards, or other priorities, cultural fit, IT policy and strategies, risk strategies, cost-effectiveness, type of protection, threats covered, risk levels, existing alternatives and additional benefits derived from the treatment.

There are three possible responses to risk:

- Risk mitigation is the implementation of safeguards and countermeasures to reduce or eliminate vulnerabilities or threats.
- Risk transfer is the placement of the cost of loss a risk represents onto another entity. This is accomplished by purchasing insurance and/or outsourcing.
- Risk Acceptance of risk is the valuation by Ignite Procurement that the cost/benefit analysis of a possible safeguard and the determination that the cost of the countermeasure

greatly outweighs the possible cost of loss due to a risk. Values under 15 are acceptable risks, while values 15+ are unacceptable risks. Unacceptable risks must be treated. On behalf of the risk owners, Senior Management will accept all residual risks.

Based on risk treatment decisions, plans, and net new compensating controls to be implemented, recalculate new residual risks, reassessing risk likelihoods and impacts.

COO or a designee is responsible for creating the risk assessment and treatment report and delivering results to senior management and other applicable team members including risk responses and documentation of risks that will be accepted by the organization such as threats or vulnerabilities that will likely impact the organization and with a low impact cost. All risk assessment reports must be documented and retained for a minimum of three years.

Unacceptable risks should be appropriately remediated in accordance with the Change Management Policy and Vulnerability Management Policy.

Ignite Procurement business needs, local situations, laws and regulations may occasionally call for an exception to this policy or any other Ignite Procurement policy. If an exception is needed, Ignite Procurement management will determine an acceptable alternative approach.

Any violation of this policy or any other Ignite Procurement policy or procedure may result in disciplinary action, up to and including termination of employment. Ignite Procurement reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Ignite Procurement does not consider conduct in violation of this policy to be within an employee's or contractor's course and scope of work.

Any personnel who are requested to undertake an activity that he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager or any other manager of Ignite Procurement as soon as possible.

The disciplinary process should also be used as a deterrent to prevent employees and contractors in violating organizational security policies and procedures, and any other security breaches.

COO or a designee is responsible for overseeing the successful completion of the risk assessment. Such risk assessments must be conducted at least annually or whenever there are significant changes to Ignite Procurement, its systems, or other conditions that may impact the security of Ignite Procurement such as the failure of a mission critical vendor or a security breach.

Ignite Procurement reviews and updates its security policies and plans to maintain organizational security objectives and meet regulatory requirements at least annually. The results are shared with appropriate parties internally and findings are tracked to resolution. Any changes are communicated across the organization.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Ignite Procurement's system; as well as the nature of the components of the system result in risks that the criteria will not be met. Ignite Procurement 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 the risks will be unique. As part of the design and operation of the system, Ignite Procurement's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Email and other messaging tools are intended to be used as a business tool to facilitate communications and the exchange of information needed by team members to perform their assigned duties. All messages and/or attachments that contain confidential information are required to be encrypted to protect the privacy and integrity of the information.

- Communication tool passwords should not be shared with another individual. They are intended for the authorized team member only.
- Team members who transmit confidential information outside the organization should comply with applicable regulatory and customer requirements and Ignite Procurement policies regarding the disclosure of confidential information to third parties.
- Communications may be monitored and tracked without advanced notice to or consent by the team member.
- Retention and disposal of electronic communications should be in accordance with all other Ignite Procurement data protection and privacy policies.
- Dissemination of confidential information (i.e., trade secrets, team member personal information or financial data), except for approved business purposes.
- Attempting to gain access to another team member's account, without permission.
- Misrepresenting, obscuring, suppressing, or replacing a team member's identity.
- Sending confidential information over an open network (the Internet) without proper encryption.
- Transmitting, retrieving, or storing of any communications of a defamatory, discriminatory, or harassing nature or materials that are obscene.
- Transmission of messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference.

Data Communication

Ignite Procurement manages, controls, and secures its networks, the connected systems and applications, and data-in-transit to safeguard against internal and external threats.

Ignite Procurement utilizes network and/or web application firewalls to safeguard networks and core applications from threats. Ignite Procurement configures appropriate firewall alerts and alarms for timely response and investigation.

Ignite Procurement ensures available networking ports and protocols are restricted based on the principle of least functionality. Firewall configurations and rulesets are maintained. Firewall rules are implemented to minimize exposure to external threats. As an additional layer of defense, Ignite Procurement utilizes monitoring solutions to detect and alert on network-based threats.

Ignite Procurement establishes, documents, and reviews access control policy based on business and security requirements, which also encompasses network access control. Reference the Access Control and Termination Policy for more information.

Ignite Procurement segregates networks based on the required groups of information services, users, and systems.

Ignite Procurement utilizes firewall configurations to restrict connections between untrusted networks and trusted networks. Additionally, Ignite Procurement may utilize security groups and network access control lists (NACLs) to improve network security for individual virtual machines.

Ignite Procurement implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

Ignite Procurement is required to use a defense-in-depth (DiD) architecture to protect the Confidentiality, Integrity, and Availability of information systems and data, i.e. placing information systems that contain sensitive data in an internal network zone, segregated from the DMZ and other untrusted networks.

Ignite Procurement synchronizes clocks of all applicable information systems to the same time protocol to enforce consistent and accurate timestamping.

Access to Production Code

Ignite Procurement adheres to the principle of least privilege, specifying that team members will be given access to only the information and resources necessary to perform their job functions as determined by management or a designee. Requests for escalation of or changes to privilege and access are documented and require approval by an authorized manager. System access is revoked upon termination or resignation.

Our PaaS provider also automates the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on underlying hardware.

Monitoring Controls

Ignite Procurement collects & monitors audit logs and alerts on key events stemming from production systems, applications, databases, servers, message queues, load balancers, and critical services, as well as IAM user and admin activities. Ignite Procurement manages logging solution(s) and/or SIEM tool(s) to collect event information of the aforementioned systems and activities. Ignite Procurement implements filters, parameters, and alarms to trigger alerts on logging events that deviate from established system and activity baselines. Logs are securely stored and archived for a minimum of 1 year to assist with potential forensic efforts.

Logs are made available to relevant team members for troubleshooting, auditing, and capacity planning activities. System and user activity logs may be utilized to assess the causes of incidents and problems. Ignite Procurement utilizes access control to prevent unauthorized access, deletion, or tampering of logging facilities and log information.

When various logging and alerting solutions and mechanisms give rise to events and alerts, Ignite Procurement correlates those events and alerts across all log sources to identify root causes and formally declare incidents, as necessary, in accordance with the Security Incident Response Policy and Change Management Policy.

Additionally, Ignite Procurement utilizes threat detection solution(s) to actively monitor and alert on network and application-based threats.

Boundaries of the System

The scope of this report includes the Services performed by Ignite Procurement.

The applicable trust services criteria and the related controls

Security

Material Changes: Changes to the System in the Last 12 Months

We have implemented several features and feature improvements the last 12 months that have enhanced the capabilities of and the experience of using Ignite Procurement's services.

We have implemented a multitenant system architecture which means that the software runs on a single instance server that serves multiple tenants. This change has increased the information security on our server.

During the last 12 months we have implemented support for logging in to our SaaS platform through the use of AD single-sign-on. This process eases the user creation and log in for our customers with AD.

There are also additional features and improvements, that should not affect the users understanding of how the system is used to provide the service.

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.

Complementary User Entity Controls (CUECs)

As outlined in the terms and conditions customers must agree on:

"The Customer shall not use the Service in a way that violates any laws, infringes on anyone's rights, is offensive, or interferes with the Service or any features on the Service, and undertakes to ensure that all Users respect the Terms and this provision in particular. Customer is responsible for any and all activities that occur under User's account.

The Customer shall ensure that User identities, passwords, and equivalent obtained by the Customer in conjunction with registration are stored and used in a secure manner and cannot be accessed and used by third parties. Customer agrees to notify Ignite immediately of any unauthorized use of User's account or any other breach of security.

Ignite has no obligation to monitor the Services to assure compliance with the Terms. Ignite reserves the right at all times to edit, refuse to post or to remove and delete any information or materials, in whole or in part, if Ignite reasonably suspects it to be comprised by the prohibition above"

Further, from the data processing agreement Ignite Procurement rely on the customer to be "responsible for ensuring that the processing of personal data complies with the requirements set out in Norwegian data protection legislation and the GDPR, hereunder ensuring that the processing of personal data, which the Processor is instructed to perform, has a legal basis. "

Subservice Organizations and Complementary Subservice Organization Controls (CSOCS)

Ignite Procurement uses Google Cloud Platform (GCP) as a subservice organization for data center colocation services. Ignite Procurement's controls related to their system cover only a portion of the overall internal control for each user entity of the System. The description does not extend to the services provided by the subservice organization that provides colocation services for IT infrastructure. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of the Company and exclude the related controls of GCP.

Although the subservice organization has been carved out for the purposes of this report, certain Trust Services Criteria are intended to be met by controls at the subservice organization. Complementary Subservice Organization Controls (CSOCs) are expected to be in place at GCP related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. GCP physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities. Management of Ignite Procurement receives and reviews the GCP SOC 2 report annually. In addition, through its operational activities, Ignite Procurement management monitors the services performed by GCP to determine whether operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also has communication with the subservice organization to monitor compliance with the service agreement, stay abreast of changes planned at the hosting facility, and relay any issues or concerns to GCP management.

It is not feasible for the criteria related to the System to be achieved solely by Ignite Procurement. Therefore, each user entity's internal control must be evaluated in conjunction with Ignite Procurement's controls and related tests and results described in Section 4 of this report, considering the related CSOCs expected to be implemented at the subservice organization as described below.

Criteria	Complementary Subservice Organization Controls
CC6.4	GCP is responsible for restricting data center access to authorized personnel.
CC6.4	GCP is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC7.2 A1.2	GCP is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
CC7.2 A1.2	GCP is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
CC7.2 A1.2	GCP is responsible for overseeing the regular maintenance of environmental protections at data centers.

Report Use

The description does not omit or distort information relevant to the system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider it important to his or her own particular needs.

SECTION 4

TESTING MATRICES

TESTS OF DESIGN and IMPLEMENTATION EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the IGNITE system provided by Ignite Procurement AS. The scope of the testing was restricted to the IGNITE System, and its boundaries as defined in Section 3.

Prescient Assurance LLC conducted the examination testing as of August 26th, 2021

The tests applied to test the Implementation and Design Effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that all applicable trust services criteria were achieved during the review date. In selecting the tests of controls, Prescient Assurance LLC considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates.
- The control risk mitigated by the control.
- The effectiveness of entity-level controls, especially controls that monitor other controls.
- The degree to which the control relies on the effectiveness of other controls.
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations, and settings or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Prescient Assurance utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, to determine the number of items to be selected in a sample for a particular test. Prescient Assurance, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices. Any phrase other than the, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the Implementation and Design Effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

CONTROL MATRIX and TEST RESULTS

Category	Trust ID	Points of Focus	Trust Criteria	Established Internal Controls	Test Performed	Results of Testing
Control Environment	CC1.1		COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
Control Environment	CC1.1	1	Sets the Tone at the Top—The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.	Ignite Procurement has documented a code of conduct published to the organization that outlines ethical and behavioral standards.	Ignite Procurement requires all employees to read and electronicall y acknowledge the Code of Conduct policy.	No Exceptions Noted
Control Environment	CC1.1	2	Establishes Standards of Conduct—The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the entity and by outsourced service providers and business partners.	Ignite Procurement has documented a code of conduct published to the organization that outlines ethical and behavioral standards.	Ignite Procurement requires all employees to read and electronicall y acknowledge the Code of Conduct policy.	No Exceptions Noted
Control Environment	CC1.1	3	Evaluates Adherence to Standards of Conduct—Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.	Ignite Procurement evaluates the performance of its personnel through formal, annual evaluations.	Ignite Procurement' s management documents a formal evaluation for each team member to provide feedback on performance at least annually.	No Exceptions Noted

Control Environment	CC1.1	4	Addresses Deviations in a Timely Manner—Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.	Violations of Ignite Procurement policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	Ignite Procurement's policies contain a discipline statement that is clearly documented and available. Complete	No Exceptions Noted
Control Environment	CC1.1	5	Considers Contractors and Vendor Employees in Demonstrating Its Commitment—Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.	Ignite Procurement has documented a code of conduct published to the organization that outlines ethical and behavioral standards.	Ignite Procurement requires all employees to read and electronicall y acknowledge the Code of Conduct policy.	No Exceptions Noted
Control Environment	CC1.2		COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
Control Environment	CC1.2	1	Establishes Oversight Responsibilities—The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.	The Board of Directors is governed by the Ignite Procurement bylaws to ensure its independence from management.	The board of directors is governed by Ignite Procurement's bylaws.	No Exceptions Noted
Control Environment	CC1.2	2	Applies Relevant Expertise—The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take	Ignite Procurement has a Board of Directors in place that includes senior management and external advisors with sufficient expertise and independence to perform their duties advising management.	Ignite Procurement has a board of directors in place that meets at least quarterly.	No Exceptions Noted

			commensurate action.			
Control Environment	CC1.2	3	Operates Independently—The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.	The Board of Directors is governed by the Ignite Procurement bylaws to ensure its independence from management.	The board of directors is governed by Ignite Procurement's bylaws.	No Exceptions Noted
Control Environment	CC1.2	4	*Supplements Board Expertise—The board of directors supplements its expertise relevant to security, availability, processing integrity, confidentiality, and privacy, as needed, using a subcommittee or consultants.*	The Board of Directors and Ignite Procurement management meet at least quarterly to review business goals, KPIs, objectives, needs, and risk management activities and maintains formal meeting minutes for each such meeting.	Ignite Procurement's board of directors maintains formal meeting minutes that address concerns of security, availability, and confidentiality, as applicable.	No Exceptions Noted
Control Environment	CC1.3		COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
Control Environment	CC1.3	1	Considers All Structures of the Entity—Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.	The Board of Directors and Ignite Procurement management meet at least quarterly to review business goals, KPIs, objectives, needs, and risk management activities and maintains formal meeting minutes for each such meeting.	Ignite Procurement's board of directors maintains formal meeting minutes that address concerns of security, availability, and confidentiality, as applicable.	No Exceptions Noted
Control Environment	CC1.3	2	Establishes Reporting Lines—Management designs and evaluates lines of reporting for each entity structure to enable execution of	Ignite Procurement maintains an organizational chart with identified positions of authority and clear reporting	Ignite Procurement has an organization chart with identified	No Exceptions Noted

			authorities and responsibilities and flow of information to manage the activities of the entity.	lines. Such information is communicated to personnel and freely made available.	positions of authority and reporting lines. The organization chart is available to the Ignite Procurement team.	
Control Environment	CC1.3	3	Defines, Assigns, and Limits Authorities and Responsibilities—Management and the board of directors' delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization.	All positions at Ignite Procurement have detailed job descriptions that define roles and responsibilities and are freely available to personnel.	Ignite Procurement has job descriptions that are available and reviewed at least once per year.	No Exceptions Noted
Control Environment	CC1.3	4	*Addresses Specific Requirements When Defining Authorities and Responsibilities—Management and the board of directors consider requirements relevant to security, availability, processing integrity, confidentiality, and privacy when defining authorities and responsibilities.*	New personnel are required to sign an industry standard confidentiality agreement protecting company confidential information.	Ignite Procurement requires all employees and full-time contractors to sign an industry standard confidentialit y agreement.	No Exceptions Noted
Control Environment	CC1.3	5	*Considers Interactions with External Parties When Establishing Structures, Reporting Lines, Authorities, and Responsibilities—Management and the board of directors consider the need for the entity to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities.*	Ignite Procurement maintains an organizational chart with identified positions of authority and clear reporting lines. Such information is communicated to personnel and freely made available.	Ignite Procurement has an organization chart with identified positions of authority and reporting lines. The organization chart is available to the Ignite Procurement team.	No Exceptions Noted

Control Environment	CC1.4		COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
Control Environment	CC1.4	1	Establishes Policies and Practices—Policies and practices reflect expectations of competence necessary to support the achievement of objectives.	Ignite Procurement evaluates the performance of its personnel through formal, annual evaluations.	Ignite Procurement's management documents a formal evaluation for each team member to provide feedback on performance at least annually.	No Exceptions Noted
Control Environment	CC1.4	2	Evaluates Competence and Addresses Shortcomings—The board of directors and management evaluate competence across the entity and in outsourced service providers in relation to established policies and practices and act as necessary to address shortcomings.	Ignite Procurement evaluates the performance of its personnel through formal, annual evaluations.	Ignite Procurement's management documents a formal evaluation for each team member to provide feedback on performance at least annually.	No Exceptions Noted
Control Environment	CC1.4	3	Attracts, Develops, and Retains Individuals— The entity provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced service providers to support the achievement of objectives.	Ignite Procurement has a security awareness training program in place to promote the team's awareness of their obligations with respect to maintaining information security, privacy and understanding of internal policies. Such program is logged and completed by all applicable new hires.	Ignite Procurement has a security awareness training program in-place for all applicable personnel. All applicable personnel complete the training and completion of such training is logged.	No Exceptions Noted

Control Environment	CC1.4	4	Plans and Prepares for Succession—Senior management and the board of directors develop contingency plans for assignments of responsibility important for internal control.	The Board of Directors and Ignite Procurement management meet at least quarterly to review business goals, KPIs, objectives, needs, and risk management activities and maintains formal meeting minutes for each such meeting.	Ignite Procurement's board of directors maintains formal meeting minutes that address concerns of security, availability, and confidentiality, as applicable.	No Exceptions Noted
Control Environment	CC1.4	5	*Considers the Background of Individuals—The entity considers the background of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.*	Background checks are in place to qualify new personnel. Such screening is reviewed prior to a new employee first day, in accordance with local laws.	Ignite Procurement completes background checks for all new hires in accordance with local laws.	No Exceptions Noted
Control Environment	CC1.4	6	*Considers the Technical Competency of Individuals—The entity considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.*	Ignite Procurement evaluates the performance of its personnel through formal, annual evaluations.	Ignite Procurement's management documents a formal evaluation for each team member to provide feedback on performance at least annually.	No Exceptions Noted
Control Environment	CC1.4	7	*Provides Training to Maintain Technical Competencies— The entity provides training programs, including continuing education, and training, to ensure skill sets and technical competency of existing personnel, contractors, and vendor employees are developed and maintained.*	Ignite Procurement has a security awareness training program in place to promote the team's awareness of their obligations with respect to maintaining information security, privacy and understanding of internal policies. Such program is logged and completed by all applicable new hires.	Ignite Procurement has a security awareness training program in-place for all applicable personnel. All applicable personnel complete the training and	No Exceptions Noted

					completion of such training is logged.	
Control Environment	CC1.5		COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
Control Environment	CC1.5	1	Enforces Accountability Through Structures, Authorities, and Responsibilities—Management and the board of directors establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the entity and implement corrective action as necessary.	Ignite Procurement evaluates the performance of its personnel through formal, annual evaluations.	Ignite Procurement's management documents a formal evaluation for each team member to provide feedback on performance at least annually.	No Exceptions Noted
Control Environment	CC1.5	2	Establishes Performance Measures, Incentives, and Rewards—Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives.	Ignite Procurement evaluates the performance of its personnel through formal, annual evaluations.	Ignite Procurement's management documents a formal evaluation for each team member to provide feedback on performance at least annually.	No Exceptions Noted
Control Environment	CC1.5	3	Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance—Management and the board of directors align incentives and rewards with the fulfillment of internal control responsibilities in the achievement of	Ignite Procurement evaluates the performance of its personnel through formal, annual evaluations.	Ignite Procurement's management documents a formal evaluation for each team member to provide	No Exceptions Noted

			objectives.		feedback on performance at least annually.	
Control Environment	CC1.5	4	Considers Excessive Pressures—Management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.	Ignite Procurement evaluates the performance of its personnel through formal, annual evaluations.	Ignite Procurement's management documents a formal evaluation for each team member to provide feedback on performance at least annually.	No Exceptions Noted
Control Environment	CC1.5	5	Evaluates Performance and Rewards or Disciplines Individuals—Management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, and provide rewards or exercise disciplinary action, as appropriate.	Ignite Procurement evaluates the performance of its personnel through formal, annual evaluations.	Ignite Procurement's management documents a formal evaluation for each team member to provide feedback on performance at least annually.	No Exceptions Noted
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.			
Communication and Information	CC2.1	1	Identifies Information Requirements—A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity's objectives.	All positions at Ignite Procurement have detailed job descriptions that define roles and responsibilities and are freely available to personnel.	Ignite Procurement has job descriptions that are available and reviewed at least once per year.	No Exceptions Noted
Communication and Information	CC2.1	2	Captures Internal and External Sources of Data—Information systems capture	Ignite Procurement uses tools to log security events, user activity, application	Ignite Procurement has implemented	No Exceptions Noted

			internal and external sources of data.	states and system performance from its cloud infrastructure. Such logs are reviewed to identify and report unusual or malicious activities.	tools to capture information about IP traffic going to and from network interfaces in their virtual private cloud.	
Communication and Information	CC2.1	3	Processes Relevant Data into Information—Information systems process and transform relevant data into information.	Ignite Procurement has a Change Management Policy governing the system development lifecycle (infrastructure, data, software, and procedures), including procedures for tracking, testing, approving, and validating changes.	Ignite Procurement patches its systems in accordance with its Change Management Policy to protect from new risks.	No Exceptions Noted
Communication and Information	CC2.1	4	Maintains Quality Throughout Processing—Information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to assess its relevance in supporting the internal control components.	Ignite Procurement has a Change Management Policy governing the system development lifecycle (infrastructure, data, software, and procedures), including procedures for tracking, testing, approving, and validating changes.	Ignite Procurement patches its systems in accordance with its Change Management Policy to protect from new risks	No Exceptions Noted
Communication and Information	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.			
Communication and Information	CC2.2	1	Communicates Internal Control Information—A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.	All positions at Ignite Procurement have detailed job descriptions that define roles and responsibilities and are freely available to personnel.	Ignite Procurement has job descriptions that are available and reviewed at least once per year.	No Exceptions Noted

Communication and Information	CC2.2	2	Communicates With the Board of Directors—Communication exists between management and the board of directors so that both have information needed to fulfill their roles with respect to the entity's objectives.	The Board of Directors and Ignite Procurement management meet at least quarterly to review business goals, KPIs, objectives, needs, and risk management activities and maintains formal meeting minutes for each such meeting.	Ignite Procurement has a board of directors in place that meets at least quarterly.	No Exceptions Noted
Communication and Information	CC2.2	3	Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.	Communication lines are in place to provide an anonymous / confidential way for internal personnel, customers and other third parties to report security failures, incidents, vulnerabilities, system failures etc.	Ignite Procurement has an email available to receive disclosures of incidents or system failures. The email is publicly listed on the company's security page.	No Exceptions Noted
Communication and Information	CC2.2	4	Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the information.	The organization communicates using telephone, video conferencing tools, messaging tools, email, physical mail, and in person.	Inspected the Business Continuity and Disaster recovery Plan to determine that there were communicati on methods established.	No Exceptions Noted
Communication and Information	CC2.2	5	*Communicates Responsibilities—Entity personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and have the information necessary to carry out those responsibilities.*	All positions at Ignite Procurement have detailed job descriptions that define roles and responsibilities and are freely available to personnel.	Ignite Procurement has job descriptions that are available and reviewed at least once per year.	No Exceptions Noted

Communication and Information	CC2.2	6	*Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters—Entity personnel are provided with information on how to report systems failures, incidents, concerns, and other complaints to personnel.*	Communication lines are in place to provide an anonymous / confidential way for internal personnel, customers and other third parties to report security failures, incidents, vulnerabilities, system failures etc.	Ignite Procurement has an email available to receive disclosures of incidents or system failures. The email is publicly listed on the company's security page.	No Exceptions Noted
Communication and Information	CC2.2	7	*Communicates Objectives and Changes to Objectives—The entity communicates its objectives and changes to those objectives to personnel in a timely manner.*	The organization communicates using telephone, video conferencing tools, messaging tools, email, physical mail, and in person.	Inspected the Business Continuity and Disaster recovery Plan to determine that there were communicati on methods established.	No Exceptions Noted
Communication and Information	CC2.2	8	*Communicates Information to Improve Security Knowledge and Awareness—The entity communicates information to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program.*	Ignite Procurement has a security awareness training program in place to promote the team's awareness of their obligations with respect to maintaining information security, privacy and understanding of internal policies.	Ignite Procurement has a security awareness training program in-place for all applicable personnel. All applicable personnel complete the training and completion of such training is logged.	No Exceptions Noted
Communication and Information	CC2.2	9	*Communicates Information About System Operation and Boundaries—The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized personnel to enable them to*	All positions at Ignite Procurement have detailed job descriptions that define roles and responsibilities and are freely available to personnel.	Ignite Procurement has job descriptions that are available and reviewed at least once per year.	No Exceptions Noted

			understand their role in the system and the results of system operation.			
Communication and Information	CC2.2	10	*Communicates System Objectives—The entity communicates its objectives to personnel to enable them to carry out their responsibilities.*	All positions at Ignite Procurement have detailed job descriptions that define roles and responsibilities and are freely available to personnel.	Ignite Procurement has job descriptions that are available and reviewed at least once per year.	No Exceptions Noted
Communication and Information	CC2.2	11	*Communicates System Changes—System changes that affect responsibilities or the achievement of the entity's objectives are communicated in a timely manner.*	All positions at Ignite Procurement have detailed job descriptions that define roles and responsibilities and are freely available to personnel.	Ignite Procurement has job descriptions that are available and reviewed at least once per year.	No Exceptions Noted
Communication and Information	CC2.3		COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
Communication and Information	CC2.3	1	Communicates to External Parties—Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties.	The organization communicates using telephone, video conferencing tools, messaging tools, email, physical mail, and in person.	Inspected the Business Continuity and Disaster recovery Plan to determine that there were communication methods established.	No Exceptions Noted
Communication and Information	CC2.3	2	Enables Inbound Communications—Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant information.	The organization communicates using telephone, video conferencing tools, messaging tools, email, physical mail, and in person	Inspected the Business Continuity and Disaster recovery Plan to determine that there were communication methods established.	No Exceptions Noted

Communication and Information	CC2.3	3	Communicates With the Board of Directors—Relevant information resulting from assessments conducted by external parties is communicated to the board of directors.	Ignite Procurement has a Board of Directors in place that includes senior management and external advisors with sufficient expertise and independence to perform their duties advising management. The Board of Directors and Ignite Procurement management meet at least quarterly to review business goals, KPIs, objectives, needs, and risk management activities and maintains formal meeting minutes for each such meeting.	Ignite Procurement's board of directors maintains formal meeting minutes that address concerns of security, availability, and confidentiality, as applicable.	No Exceptions Noted
Communication and Information	CC2.3	4	Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.	Communication lines are in place to provide an anonymous / confidential way for internal personnel, customers and other third parties to report security failures, incidents, vulnerabilities, system failures etc. Such communication is monitored by management and any issues identified are resolved in accordance with the company Security Incident Response Plan.	Ignite Procurement has an email available to receive disclosures of incidents or system failures. The email is publicly listed on the company's security page.	No Exceptions Noted
Communication and Information	CC2.3	5	Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.	The organization communicates using telephone, video conferencing tools, messaging tools, email, physical mail, and in person.	Inspected the Business Continuity and Disaster recovery Plan to determine that there were communication methods established.	No Exceptions Noted
Communication	CC2.3	6	*Communicates*	The organization	Inspected the	No

and Information			*Objectives Related to Confidentiality and Changes to Objectives— The entity communicates, to external users, vendors, business partners and others whose products and services are part of the system, objectives and changes to objectives related to confidentiality.*	communicates using telephone, video conferencing tools, messaging tools, email, physical mail, and in person.	Business Continuity and Disaster recovery Plan to determine that there were communicati on methods established.	Exceptions Noted
Communication and Information	CC2.3	7	*Communicates Objectives Related to Privacy and Changes to Objectives—The entity communicates, to external users, vendors, business partners and others whose products and services are part of the system, objectives related to privacy and changes to those objectives.*	The organization communicates using telephone, video conferencing tools, messaging tools, email, physical mail, and in person.	Inspected the Business Continuity and Disaster recovery Plan to determine that there were communicati on methods established.	No Exceptions Noted
Communication and Information	CC2.3	8	*Communicates Information About System Operation and Boundaries—The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized external users to permit users to understand their role in the system and the results of system operation.*	All positions at Ignite Procurement have detailed job descriptions that define roles and responsibilities and are freely available to personnel.	Ignite Procurement has job descriptions that are available and reviewed at least once per year.	No Exceptions Noted
Communication and Information	CC2.3	9	*Communicates System Objectives—The entity communicates its system objectives to appropriate external users.*	Ignite Procurement has a vendor management program in place for evaluating vendor performance and compliance with contractual obligations.	Ignite Procurement uses Secureframe to manage its vendor management program and has a Vendor Management Policy in place.	No Exceptions Noted

Communication and Information	CC2.3	10	*Communicates System Responsibilities—External users with responsibility for designing, developing, implementing, operating, maintaining, and monitoring system controls receive communications about their responsibilities and have the information necessary to carry out those responsibilities.*	All positions at Ignite Procurement have detailed job descriptions that define roles and responsibilities and are freely available to personnel.	Ignite Procurement has job descriptions that are available and reviewed at least once per year.	No Exceptions Noted
Communication and Information	CC2.3	11	*Communicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters—External users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate personnel.*	Communication lines are in place to provide an anonymous / confidential way for internal personnel, customers and other third parties to report security failures, incidents, vulnerabilities, system failures etc.	Ignite Procurement has an email available to receive disclosures of incidents or system failures. The email is publicly listed on the company's security page.	No Exceptions Noted
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.			
Risk Assessment	CC3.1	1	Reflects Management's Choices—Operations objectives reflect management's choices about structure, industry considerations, and performance of the entity.	The Board of Directors and Ignite Procurement management meet at least quarterly to review business goals, KPIs, objectives, needs, and risk management activities and maintains formal meeting minutes for each such meeting.	Ignite Procurement's board of directors maintains formal meeting minutes that address concerns of security, availability, and confidentiality, as applicable.	No Exceptions Noted
Risk Assessment	CC3.1	2	Considers Tolerances for Risk—Management	Ignite Procurement implemented a	Ignite Procurement	No Exceptions

			considers the acceptable levels of variation relative to the achievement of operations objectives.	documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks. The risk assessment process determines how to respond and manage risk, including whether to accept, avoid, reduce, or share the risk.	has a risk assessment policy in place to guide it during its risk Assessments.	Noted
Risk Assessment	CC3.1	3	Includes Operations and Financial Performance Goals—The organization reflects the desired level of operations and financial performance for the entity within operations objectives.	Ignite Procurement implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks.	Ignite Procurement has a risk assessment policy in place to guide it during its risk Assessments.	No Exceptions Noted
Risk Assessment	CC3.1	4	Forms a Basis for Committing of Resources—Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.	Formal risk assessments are performed annually and as needed in accordance with the risk assessment policy.	A formal Risk Assessment is completed at least annually and upon implementation of any new critical infrastructure.	No Exceptions Noted
Risk Assessment	CC3.1	5	Complies With Applicable Accounting Standards—Financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are	Ignite Procurement implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated	Ignite Procurement has a risk assessment policy in place to guide it during its risk Assessments.	No Exceptions Noted

			appropriate in the circumstances.	with the identified threats, including fraud and mitigation strategies for those risks.		
Risk Assessment	CC3.1	6	Considers Materiality—Management considers materiality in financial statement presentation.	Ignite Procurement implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks. The risk assessment process determines how to respond and manage risk, including whether to accept, avoid, reduce, or share the risk.	Ignite Procurement has a risk assessment policy in place to guide it during its risk Assessments.	No Exceptions Noted
Risk Assessment	CC3.1	7	Reflects Entity Activities—External reporting reflects the underlying transactions and events to show qualitative characteristics and assertions.	Ignite Procurement implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks.	Ignite Procurement has a risk assessment policy in place to guide it during its risk Assessments.	No Exceptions Noted
Risk Assessment	CC3.1	8	Complies With Externally Established Frameworks—Management establishes objectives consistent with laws and regulations or standards and frameworks of recognized external organizations.	Ignite Procurement has documented and communicated security policies that define information security, availability and confidentiality requirements for its systems and service commitments.	Ignite Procurement has an information security management system in place with all relevant security policies.	No Exceptions Noted
Risk Assessment	CC3.1	9	Considers the Required Level of Precision—Management reflects	Ignite Procurement has a vendor management program	Ignite Procurement uses	No Exceptions Noted

			the required level of precision and accuracy suitable for user needs and based on criteria established by third parties in nonfinancial reporting.	in place for evaluating vendor performance and compliance with contractual obligations.	Secureframe to manage its vendor management program and has a Vendor Management Policy in place.	
Risk Assessment	CC3.1	10	Reflects Entity Activities—External reporting reflects the underlying transactions and events within a range of acceptable limits.	Formal risk assessments are performed annually and as needed in accordance with the risk assessment policy.	A formal Risk Assessment is completed at least annually and upon implementation of any new critical infrastructure.	No Exceptions Noted
Risk Assessment	CC3.1	11	Reflects Management's Choices—Internal reporting provides management with accurate and complete information regarding management's choices and information needed in managing the entity.	The Board of Directors and Ignite Procurement management meet at least quarterly to review business goals, KPIs, objectives, needs, and risk management activities and maintains formal meeting minutes for each such meeting.	Ignite Procurement has a board of directors in place that meets at least quarterly.	No Exceptions Noted
Risk Assessment	CC3.1	12	Considers the Required Level of Precision—Management reflects the required level of precision and accuracy suitable for user needs in nonfinancial reporting objectives and materiality within financial reporting objectives.	The Board of Directors and Ignite Procurement management meet at least quarterly to review business goals, KPIs, objectives, needs, and risk management activities and maintains formal meeting minutes for each such meeting.	Ignite Procurement's board of directors maintains formal meeting minutes that address concerns of security, availability, and confidentiality, as applicable.	No Exceptions Noted
Risk Assessment	CC3.1	13	Reflects Entity Activities—Internal reporting reflects the underlying transactions and events within a range of acceptable limits.	Ignite Procurement implemented a documented risk management program that includes guidance on the identification of potential threats,	Ignite Procurement has a risk assessment policy in place to guide it	No Exceptions Noted

				rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks.	during its risk assessments.	
Risk Assessment	CC3.1	14	Reflects External Laws and Regulations—Laws and regulations establish minimum standards of conduct, which the entity integrates into compliance objectives.	Ignite Procurement has documented a code of conduct published to the organization that outlines ethical and behavioral standards.	Ignite Procurement requires all employees to read and electronically acknowledge the Code of Conduct policy.	No Exceptions Noted
Risk Assessment	CC3.1	15	Considers Tolerances for Risk—Management considers the acceptable levels of variation relative to the achievement of operations objectives.	Ignite Procurement implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks. The risk assessment process determines how to respond and manage risk, including whether to accept, avoid, reduce, or share the risk.	Ignite Procurement has a risk assessment policy in place to guide it during its risk assessments.	No Exceptions Noted
Risk Assessment	CC3.1	16	*Establishes Sub-objectives to Support Objectives—Management identifies sub-objectives related to security, availability, processing integrity, confidentiality, and privacy to support the achievement of the entity's objectives related to reporting, operations, and compliance.*	The Board of Directors and Ignite Procurement management meet at least quarterly to review business goals, KPIs, objectives, needs, and risk management activities and maintains formal meeting minutes for each such meeting.	Ignite Procurement's board of directors maintains formal meeting minutes that address concerns of security, availability, and confidentiality, as applicable.	No Exceptions Noted

Risk Assessment	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.			
Risk Assessment	CC3.2	1	Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels—The entity identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.	Ignite Procurement implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks.	ignite Procurement has a risk assessment policy in place to guide it during its risk assessments.	No Exceptions Noted
Risk Assessment	CC3.2	2	Analyzes Internal and External Factors—Risk identification considers both internal and external factors and their impact on the achievement of objectives.	Ignite Procurement implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks. The risk assessment process determines how to respond and manage risk, including whether to accept, avoid, reduce, or share the risk.	ignite Procurement has a risk assessment policy in place to guide it during its risk assessments.	No Exceptions Noted
Risk Assessment	CC3.2	3	Involves Appropriate Levels of Management—The entity puts into place effective risk assessment mechanisms that involve appropriate levels of management.	Ignite Procurement implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated	Ignite Procurement has a risk assessment policy in place to guide it during its risk assessments.	No Exceptions Noted

				with the identified threats, including fraud and mitigation strategies for those risks.		
Risk Assessment	CC3.2	4	Estimates Significance of Risks Identified—Identified risks are analyzed through a process that includes estimating the potential significance of the risk.	The risk assessment process determines how to respond and manage risk, including whether to accept, avoid, reduce, or share the risk.	Ignite Procurement has a risk assessment policy in place to guide it during its risk assessments.	No Exceptions Noted
Risk Assessment	CC3.2	5	Determines How to Respond to Risks—Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.	The risk assessment process determines how to respond and manage risk, including whether to accept, avoid, reduce, or share the risk.	Ignite Procurement has a risk assessment policy in place to guide it during its risk assessments.	No Exceptions Noted
Risk Assessment	CC3.2	6	*Identifies and Assesses Criticality of Information Assets and Identifies Threats and Vulnerabilities—The entity's risk identification and assessment process includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets.*	Ignite Procurement has a policy for vulnerability and patch management to guide it in the detection and remediation of vulnerabilities.	Ignite Procurement has a Vulnerability Management Policy in place to govern the detection and remediation of vulnerabilities.	No Exceptions Noted
Risk Assessment	CC3.2	7	*Analyzes Threats and Vulnerabilities from Vendors, Business Partners, and Other Parties—The entity's*	Ignite Procurement has a vendor management program in place for evaluating	Inspected the Information Security Policy to determine	No Exceptions Noted

			risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information systems.	vendor performance and compliance with contractual obligations.	that Ignite Procurement requires vendor security assessment before third party products or services are used confirming the provider can maintain appropriate security and privacy controls.	
Risk Assessment	CC3.2	8	*Considers the Significance of the Risk—The entity's consideration of the potential significance of the identified risks includes (1) determining the criticality of identified assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; and (4) determining the risk associated with assets based on asset criticality, threat impact, and likelihood.*	Ignite Procurement implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks. The risk assessment process determines how to respond and manage risk, including whether to accept, avoid, reduce, or share the risk.	Ignite Procurement has a risk assessment policy in place to guide it during its risk assessments.	No Exceptions Noted
Risk Assessment	CC3.3		COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives			
Risk Assessment	CC3.3	1	Considers Various Types of Fraud—The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.	Ignite Procurement implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated	Ignite Procurement has a risk assessment policy in place to guide it during its risk assessments.	No Exceptions Noted

				with the identified threats, including fraud and mitigation strategies for those risks.		
Risk Assessment	CC3.3	2	Assesses Incentives and Pressures—The assessment of fraud risks considers incentives and pressures.	Ignite Procurement implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks.	Ignite Procurement has a risk assessment policy in place to guide it during its risk assessments.	No Exceptions Noted
Risk Assessment	CC3.3	3	Assesses Opportunities—The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering the entity's reporting records, or committing other inappropriate acts.	Ignite Procurement implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks.	Ignite Procurement has a risk assessment policy in place to guide it during its risk assessments.	No Exceptions Noted
Risk Assessment	CC3.3	4	Assesses Attitudes and Rationalizations—The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions.	Ignite Procurement implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks.	Ignite Procurement has a risk assessment policy in place to guide it during its risk assessments.	No Exceptions Noted
Risk Assessment	CC3.3	5	*Considers the Risks Related to the Use of IT and Access to Information—The assessment of fraud risks includes consideration of*	Ignite Procurement has a policy for vulnerability and patch management to guide it in the detection and remediation of	Ignite Procurement has a Vulnerability Management Policy in place to	No Exceptions Noted

			threats and vulnerabilities that arise specifically from the use of IT and access to information.	vulnerabilities.	govern the detection and remediation of vulnerabilities.	
Risk Assessment	CC3.4		COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
Risk Assessment	CC3.4	1	Assesses Changes in the External Environment—The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.	A Business Continuity and Disaster Recovery Plan is in place and tested annually.	Ignite Procurement has a Business Continuity and Disaster Recovery Plan in place to handle backups, and the steps necessary to recover from potential disasters.	
Risk Assessment	CC3.4	2	Assesses Changes in the Business Model—The entity considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.	A Business Continuity and Disaster Recovery Plan is in place and tested annually.	Ignite Procurement has a Business Continuity and Disaster Recovery Plan in place to handle backups, and the steps necessary to recover from potential disasters.	No Exceptions Noted
Risk Assessment	CC3.4	3	Assesses Changes in Leadership—The entity considers changes in management and respective attitudes and philosophies on the system of internal control.	Ignite Procurement continuously assesses internal controls used to maintain the security, availability and confidentiality of its systems and service commitments. Any non-conformities are addressed by senior management in accordance with the company's Change	Ignite Procurement uses Secureframe, an internal control platform that helps Ignite Procurement management continuously maintain and review internal	No Exceptions Noted

				Management and Risk Assessment and Risk Treatment Policy.	controls.	
Risk Assessment	CC3.4	4	*Assess Changes in Systems and Technology—The risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment.*	To manage, authorize, design, develop, and document changes, a version control system manages source code, documentation, release labeling, and other change management tasks. Only system administrators can provide access.	Ignite Procurement utilizes a version control system for version control management.	No Exceptions Noted
Risk Assessment	CC3.4	5	*Assess Changes in Vendor and Business Partner Relationships—The risk identification process considers changes in vendor and business partner relationships.*	Ignite Procurement has a vendor management program in place for evaluating vendor performance and compliance with contractual obligations.	Inspected the Information Security Policy to determine that agreements will be updated and amended as necessary when business, laws, and regulatory requirements change.	No Exceptions Noted
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.			
Monitoring Activities	CC4.1	1	Considers a Mix of Ongoing and Separate Evaluations—Management includes a balance of ongoing and separate evaluations.	Formal risk assessments are performed annually and as needed in accordance with the risk assessment policy.	A formal Risk Assessment is completed at least annually and upon implementation of any new critical infrastructure.	No Exceptions Noted
Monitoring Activities	CC4.1	2	Considers Rate of Change—Management	A Business Continuity and Disaster Recovery	Ignite Procurement	No Exceptions

			considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations.	Plan is in place and tested annually.	has a Business Continuity and Disaster Recovery Plan in place to handle backups, and the steps necessary to recover from potential disasters.	Noted
Monitoring Activities	CC4.1	3	Establishes Baseline Understanding—The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations.	Ignite Procurement continuously assesses internal controls used to maintain the security, availability and confidentiality of its systems and service commitments.	Ignite Procurement uses Secureframe, an internal control platform that helps Ignite Procurement management continuously maintain and review internal controls.	No Exceptions Noted
Monitoring Activities	CC4.1	4	Uses Knowledgeable Personnel—Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated.	All positions at Ignite Procurement have detailed job descriptions that define roles and responsibilities and are freely available to personnel.	Ignite Procurement has job descriptions that are available and reviewed at least once per year.	No Exceptions Noted
Monitoring Activities	CC4.1	5	Integrates With Business Processes—Ongoing evaluations are built into the business processes and adjust to changing conditions.	Formal risk assessments are performed annually and as needed in accordance with the risk assessment policy.	A formal Risk Assessment is completed at least annually and upon implementation of any new critical infrastructure.	No Exceptions Noted
Monitoring Activities	CC4.1	6	Adjusts Scope and Frequency—Management varies the scope and frequency of separate evaluations depending on risk.	Ignite Procurement implemented a documented risk management program that includes guidance on the identification of potential threats,	Ignite Procurement has a risk assessment policy in place to guide it	No Exceptions Noted

				rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks. The risk assessment process determines how to respond and manage risk, including whether to accept, avoid, reduce, or share the risk.	during its risk assessments.	
Monitoring Activities	CC4.1	7	Objectively Evaluates—Separate evaluations are performed periodically to provide objective feedback.	Formal risk assessments are performed annually and as needed in accordance with the risk assessment policy.	A formal Risk Assessment is completed at least annually and upon implementation of any new critical infrastructure.	No Exceptions Noted
Monitoring Activities	CC4.1	8	*Considers Different Types of Ongoing and Separate Evaluations—Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certification made against established specifications (for example, ISO certifications), and internal audit assessments.*	Ignite Procurement implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks. The risk assessment process determines how to respond and manage risk, including whether to accept, avoid, reduce, or share the risk.	Ignite Procurement has a risk assessment policy in place to guide it during its risk assessments.	No Exceptions Noted
Monitoring Activities	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.			
Monitoring Activities	CC4.2	1	Assesses Results—Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.	The Board of Directors and Ignite Procurement management meet at least quarterly to review business goals, KPIs, objectives, needs, and risk management activities and maintains formal meeting minutes for each such meeting.	Ignite Procurement's board of directors maintains formal meeting minutes that address concerns of security, availability, and confidentiality, as applicable.	No Exceptions Noted
Monitoring Activities	CC4.2	2	Communicates Deficiencies—Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.	Ignite Procurement performs vulnerability scans on production systems to identify potential vulnerabilities monthly. Results are assessed and high/critical findings are tracked through remediation.	Ignite Procurement performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation.	No Exceptions Noted
Monitoring Activities	CC4.2	3	Monitors Corrective Action—Management tracks whether deficiencies are remedied on a timely basis.	Ignite Procurement performs vulnerability scans on production systems to identify potential vulnerabilities monthly. Results are assessed and high/critical findings are tracked through remediation.	Ignite Procurement performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation.	No Exceptions Noted
Control	CC5.1		COSO Principle 10: The			

Activities			entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels			
Control Activities	CC5.1	1	Integrates With Risk Assessment—Control activities help ensure that risk responses that address and mitigate risks are carried out.	Ignite Procurement continuously assesses internal controls used to maintain the security, availability and confidentiality of its systems and service commitments. Any non-conformities are addressed by senior management in accordance with the company's Change Management and Risk Assessment and Risk Treatment Policy.	Ignite Procurement uses Secureframe, an internal control platform that helps Ignite Procurement management continuously maintain and review internal controls.	No Exceptions Noted
Control Activities	CC5.1	2	Considers Entity-Specific Factors—Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.	Ignite Procurement continuously assesses internal controls used to maintain the security, availability and confidentiality of its systems and service commitments. Any non-conformities are addressed by senior management in accordance with the company's Change Management and Risk Assessment and Risk Treatment Policy.	Ignite Procurement uses Secureframe, an internal control platform that helps Ignite Procurement management continuously maintain and review internal controls.	No Exceptions Noted
Control Activities	CC5.1	3	Determines Relevant Business Processes—Management determines which relevant business processes require control activities.	Ignite Procurement continuously assesses internal controls used to maintain the security, availability and confidentiality of its systems and service commitments.	Ignite Procurement uses Secureframe, an internal control platform that helps Ignite Procurement management continuously maintain and review	No Exceptions Noted

					internal controls.	
Control Activities	CC5.1	4	Evaluates a Mix of Control Activity Types—Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.	Any non-conformities are addressed by senior management in accordance with the company's Change Management and Risk Assessment and Risk Treatment Policy.	Ignite Procurement uses Secureframe, an internal control platform that helps Ignite Procurement management continuously maintain and review internal controls.	No Exceptions Noted
Control Activities	CC5.1	5	Considers at What Level Activities Are Applied—Management considers control activities at various levels in the entity.	The Board of Directors and Ignite Procurement management meet at least quarterly to review business goals, KPIs, objectives, needs, and risk management activities and maintains formal meeting minutes for each such meeting.	Ignite Procurement's board of directors maintains formal meeting minutes that address concerns of security, availability, and confidentiality, as applicable.	No Exceptions Noted
Control Activities	CC5.1	6	Addresses Segregation of Duties—Management segregates incompatible duties, and where such segregation is not practical, management selects and develops alternative control activities.	Ignite Procurement has an Access Control and Termination Policy that requires unique ids for access to email, cloud infrastructure, endpoint devices, version control and communication tools.	Inspected those changes to access are documented and evaluated based off of job role.	No Exceptions Noted
Control Activities	CC5.2		COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
Control Activities	CC5.2	1	Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls—Management	Ignite Procurement continuously assesses internal controls used to maintain the security, availability and	Ignite Procurement uses Secureframe, an internal control platform that	No Exceptions Noted

			understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls.	confidentiality of its systems and service commitments. Any non-conformities are addressed by senior management in accordance with the company's Change Management and Risk Assessment and Risk Treatment Policy.	helps Ignite Procurement management continuously maintain and review internal controls.	
Control Activities	CC5.2	2	Establishes Relevant Technology Infrastructure Control Activities—Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.	Ignite Procurement has a Change Management Policy governing the system development lifecycle (infrastructure, data, software, and procedures), including procedures for tracking, testing, approving, and validating changes.	Ignite Procurement patches its systems in accordance with its Change Management Policy to protect from new risks.	No Exceptions Noted
Control Activities	CC5.2	3	Establishes Relevant Security Management Process Controls Activities—Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.	Ignite Procurement has an Access Control and Termination Policy that requires unique ids for access to email, cloud infrastructure, endpoint devices, version control and communication tools.	Inspected those changes to access are documented and evaluated based off of job role.	No Exceptions Noted
Control Activities	CC5.2	4	Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities—Management selects and develops control activities over the acquisition, development, and maintenance of technology and its	Ignite Procurement has a Change Management Policy governing the system development lifecycle (infrastructure, data, software, and procedures), including procedures for tracking, testing, approving, and validating changes.	Ignite Procurement patches its systems in accordance with its Change Management Policy to protect from new risks.	No Exceptions Noted

			infrastructure to achieve management's objectives.			
Control Activities	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.			
Control Activities	CC5.3	1	Establishes Policies and Procedures to Support Deployment of Management 's Directives—Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.	Ignite Procurement has documented a code of conduct published to the organization that outlines ethical and behavioral standards. The code is required to be reviewed and electronically acknowledged by applicable personnel prior to accessing sensitive data.	Ignite Procurement requires all employees to read and electronicall y acknowledge the Code of Conduct policy.	No Exceptions Noted
Control Activities	CC5.3	2	Establishes Responsibility and Accountability for Executing Policies and Procedures—Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside.	All positions at Ignite Procurement have detailed job descriptions that define roles and responsibilities and are freely available to personnel.	Ignite Procurement has job descriptions that are available and reviewed at least once per year.	No Exceptions Noted
Control Activities	CC5.3	3	Performs in a Timely Manner—Responsible personnel perform control activities in a timely manner as defined by the policies and procedures.	Ignite Procurement has documented a code of conduct published to the organization that outlines ethical and behavioral standards. The code is required to be reviewed and electronically acknowledged by applicable personnel prior to accessing sensitive data.	Inspected the Code of Conduct.	No Exceptions Noted
Control Activities	CC5.3	4	Takes Corrective Action—Responsible	Violations of Ignite Procurement policies	Inspected that there	No Exceptions

			personnel investigate and act on matters identified because of executing control activities.	are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	are disciplinary action procedures in place.	Noted
Control Activities	CC5.3	5	Performs Using Competent Personnel—Competent personnel with sufficient authority perform control activities with diligence and continuing focus.	Ignite Procurement has assigned responsibility for the creation, implementation, and management of company policies and procedures.	Inspected that each policy is maintained.	No Exceptions Noted
Control Activities	CC5.3	6	Reassesses Policies and Procedures—Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.	All policies are reviewed at least annually and updated as necessary by Ignite Procurement management.	Inspected that each policy is maintained.	No Exceptions Noted
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			
Logical and Physical Access Controls	CC6.1	1	*Identifies and Manages the Inventory of Information Assets—The entity identifies, inventories, classifies, and manages information assets.*	Data Classification Policy is in place to govern the uses of sensitive data.	Inspected that there is a Data Classification Policy in place.	No Exceptions Noted
Logical and Physical Access Controls	CC6.1	2	*Restricts Logical Access—Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted using access control software and rule sets.*	A team manager reviews, audits, and documents user accounts and associated privileges of at least high-risk and critical vendors at least quarterly to ensure that access is restricted appropriately.	Inspected the Access Control and Termination Policy.	No Exceptions Noted

Logical and Physical Access Controls	CC6.1	3	*Identifies and Authenticates Users—Persons, infrastructure and software are identified and authenticated prior to accessing information assets, whether locally or remotely.*	Access to sensitive systems and applications must be approved and documented for all new hires and role changes.	Inspected the Access Control and Termination Policy.	No Exceptions Noted
Logical and Physical Access Controls	CC6.1	4	*Considers Network Segmentation—Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.*	Ignite Procurement management maintains a network and architecture diagram showing the components of production systems and data flow.	Inspected the Network Diagram.	No Exceptions Noted
Logical and Physical Access Controls	CC6.1	5	*Manages Points of Access—Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented, and managed.*	Anti-malware technology is installed and running on Ignite Procurement laptops and/or desktops to protect from malicious software.	Inspected the Information Security Policy.	No Exceptions Noted
Logical and Physical Access Controls	CC6.1	6	*Restricts Access to Information Assets—Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access control rules for information assets.*	Ignite Procurement has an Access Control and Termination Policy that requires unique ids for access to email, cloud infrastructure, endpoint devices, version control and communication tools.	Inspected the Access Control and termination Policy.	No Exceptions Noted
Logical and Physical Access Controls	CC6.1	7	*Manages Identification and Authentication—Identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure, and software.*	Ignite Procurement requires multi-factor authentication on critical systems and infrastructure, where available.	Inspected the Access Control and termination Policy.	No Exceptions Noted

Logical and Physical Access Controls	CC6.1	8	*Manages Credentials for Infrastructure and Software—New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required, or the infrastructure and software are no longer in use.*	Access to sensitive systems and applications must be approved and documented for all new hires and role changes	Inspected the onboarding and offboarding procedures.	No Exceptions Noted
Logical and Physical Access Controls	CC6.1	9	*Uses Encryption to Protect Data—The entity uses encryption to supplement other measures used to protect data-at-rest, when such protections are deemed appropriate based on assessed risk.*	Sensitive data stored in databases is encrypted at rest.	Inspected the Encryption and Key Management Policy.	No Exceptions Noted
Logical and Physical Access Controls	CC6.1	10	*Protects Encryption Keys—Processes are in place to protect encryption keys during generation, storage, use, and destruction.*	A policy is in place governing the management of cryptographic controls such as encryption of app secrets, SSL, and SSH.	Inspected the Encryption and Key Management Policy.	No Exceptions Noted
Logical and Physical Access Controls	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.			
Logical and Physical Access Controls	CC6.2	1	*Controls Access Credentials to Protected Assets—Information asset access credentials are*	Ignite Procurement has an Access Control and Termination Policy that requires	Inspected the Access Control and Termination Policy.	No Exceptions Noted

			created based on an authorization from the system's asset owner or authorized custodian.	unique ids for access to email, cloud infrastructure, endpoint devices, version control and communication tools.		
Logical and Physical Access Controls	CC6.2	2	*Removes Access to Protected Assets When Appropriate—Processes are in place to remove credential access when an individual no longer requires such access.*	Ignite Procurement has an Access Control and Termination Policy that requires unique ids for access to email, cloud infrastructure, endpoint devices, version control and communication tools.	Inspected the Access Control and Termination Policy.	No Exceptions Noted
Logical and Physical Access Controls	CC6.2	3	*Reviews Appropriateness of Access Credentials—The appropriateness of access credentials is reviewed on a periodic basis for unnecessary and inappropriate individuals with credentials.*	User access reviews for sensitive systems and applications are performed quarterly and documented.	Inspected the Access Control and Termination Policy.	No Exceptions Noted
Logical and Physical Access Controls	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, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
Logical and Physical Access Controls	CC6.3	1	*Creates or Modifies Access to Protected Information Assets—Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.*	Access to sensitive systems and applications must be approved and documented for all new hires and role changes.	Inspected the Onboarding Procedures.	No Exceptions Noted
Logical and Physical Access Controls	CC6.3	2	*Removes Access to Protected Information Assets—Processes are in place to remove access to protected information assets*	Ignite Procurement has an Access Control and Termination Policy that requires unique ids for access to email,	Inspected the Changes to Access Procedures.	No Exceptions Noted

			when an individual no longer requires access.	cloud infrastructure, endpoint devices, version control and communication tools.		
Logical and Physical Access Controls	CC6.3	3	*Uses Role-Based Access Controls—Role-based access control is utilized to support segregation of incompatible functions.*	Ignite Procurement has an Access Control and Termination Policy that requires unique ids for access to email, cloud infrastructure, endpoint devices, version control and communication tools.	Inspected those changes to access are documented and evaluated based off of job role.	No Exceptions Noted
Logical and Physical Access Controls	CC6.4		The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
Logical and Physical Access Controls	CC6.4	1	*Creates or Modifies Physical Access—Processes are in place to create or modify physical access to facilities such as data centers, office spaces, and work areas, based on authorization from the system's asset owner.*	The Access Control and Termination Policy defines requirements for access and removal of access to Ignite Procurement data, systems, facilities, and networks.	Inspected that access reviews are performed quarterly.	No Exceptions Noted
Logical and Physical Access Controls	CC6.4	2	*Removes Physical Access—Processes are in place to remove access to physical resources when an individual no longer requires access.*	The Access Control and Termination Policy defines requirements for access and removal of access to Ignite Procurement data, systems, facilities, and networks.	Inspected those changes to access are documented and evaluated based off of job role.	No Exceptions Noted
Logical and Physical Access Controls	CC6.4	3	*Reviews Physical Access—Processes are in place to periodically review physical access to ensure consistency with job responsibilities.*	The Access Control and Termination Policy defines requirements for access and removal of access to Ignite Procurement data, systems, facilities, and networks.	Inspected those changes to access are reviewed quarterly.	No Exceptions Noted

Logical and Physical Access Controls	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.			
Logical and Physical Access Controls	CC6.5	1	*Identifies Data and Software for Disposal—Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.*	Ignite Procurement retains and disposes of customer data based on agreed upon customer requirements or until a customer requests data deletion, if not specified.	Inspected that there are data disposal and retention processes in place.	No Exceptions Noted
Logical and Physical Access Controls	CC6.5	2	*Removes Data and Software from Entity Control—Procedures are in place to remove data and software stored on equipment to be removed from the physical control of the entity and to render such data and software unreadable.*	Ignite Procurement retains and disposes of customer data based on agreed upon customer requirements or until a customer requests data deletion, if not specified.	Inspected that there are data disposal and retention processes in place.	No Exceptions Noted
Logical and Physical Access Controls	CC6.6		The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
Logical and Physical Access Controls	CC6.6	1	*Restricts Access—The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.*	Sensitive data is encrypted when it is transmitted over public networks.	Inspected that TLS 1.1 or equivalent protocols are required when dealing with data transmission.	No Exceptions Noted
Logical and Physical Access Controls	CC6.6	2	*Protects Identification and Authentication Credentials—Identification and authentication credentials are protected during transmission outside its system boundaries.*	Sensitive data is encrypted when it is transmitted over public networks.	Inspected that TLS 1.1 or equivalent protocols are required when dealing with data transmission.	No Exceptions Noted
Logical and	CC6.6	3	*Requires Additional*	Ignite Procurement	Inspected	No

Physical Access Controls			*Authentication or Credentials—Additional authentication information or credentials are required when accessing the system from outside its boundaries.*	requires multi-factor authentication on critical systems and infrastructure, where available.	that multi factor authenticatio n is required whenever possible.	Exceptions Noted
Logical and Physical Access Controls	CC6.6	4	*Implements Boundary Protection Systems—Boundary protection systems (for example, firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts.*	Anti-malware technology is installed and running on Ignite Procurement laptops and/or desktops to protect from malicious software.	Inspected that there are device configuration standards.	No Exceptions Noted
Logical and Physical Access Controls	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.			
Logical and Physical Access Controls	CC6.7	1	*Restricts the Ability to Perform Transmission—Data loss prevention processes and technologies are used to restrict ability to authorize and execute transmission, movement, and removal of information.*	Ignite Procurement has documented and communicated security policies that define information security, availability and confidentiality requirements for its systems and service commitments.	Inspected that data is considered an asset and is protected accordingly.	No Exceptions Noted
Logical and Physical Access Controls	CC6.7	2	*Uses Encryption Technologies or Secure Communication Channels to Protect Data—Encryption technologies or secured communication channels are used to protect transmission of data and other*	A policy is in place governing the management of cryptographic controls such as encryption of app secrets, SSL, and SSH.	Inspected that TLS 1.1 or equivalent protocols are required when dealing with data transmission.	No Exceptions Noted

			communications beyond connectivity access points.			
Logical and Physical Access Controls	CC6.7	3	*Protects Removal Media—Encryption technologies and physical asset protections are used for removable media (such as USB drives and back-up tapes), as appropriate.*	Full-disk encryption is used on all Ignite Procurement laptops and/or desktops.	Inspected that there are minimum device configuration settings.	No Exceptions Noted
Logical and Physical Access Controls	CC6.7	4	*Protects Mobile Devices—Processes are in place to protect mobile devices (such as laptops, smart phones, and tablets) that serve as information assets.*	It is a part of the device configuration standards to have mobile devices have disk encryption and anti-virus software installed.	Inspected that there are minimum device configuration settings.	No Exceptions Noted
Logical and Physical Access Controls	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.			
Logical and Physical Access Controls	CC6.8	1	*Restricts Application and Software Installation—The ability to install applications and software is restricted to authorized individuals.*	If an asset must use a non-standardized configuration, approval of the use must be provided by Ignite Procurement management and such approval and request must be documented.	Inspected that there are non-standard device configuration procedures.	No Exceptions Noted
Logical and Physical Access Controls	CC6.8	2	*Detects Unauthorized Changes to Software and Configuration Parameters—Processes are in place to detect changes to software and configuration parameters that may be indicative of unauthorized or malicious software.*	Ignite Procurement has implemented tools for automated threat detection to the production network.	Inspected that there are threat detection and monitoring enabled on Ignite's network.	No Exceptions Noted
Logical and Physical Access Controls	CC6.8	3	*Uses a Defined Change Control Process—A management-defined change control process is used for the implementation of software.*	Ignite Procurement has a Change Management Policy governing the system development lifecycle (infrastructure, data, software, and procedures), including procedures for tracking, testing,	Inspected the procedures for the change management process.	No Exceptions Noted

				approving, and validating changes.		
Logical and Physical Access Controls	CC6.8	4	*Uses Antivirus and Anti-Malware Software—Antivirus and anti-malware software is implemented and maintained to provide for the interception or detection and remediation of malware.*	Anti-malware technology is installed and running on Ignite Procurement laptops and/or desktops to protect from malicious software	Inspected that there are minimum device configuration settings.	No Exceptions Noted
Logical and Physical Access Controls	CC6.8	5	*Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software—Procedures are in place to scan information assets that have been transferred or returned to the entity's custody for malware and other unauthorized software and to remove any items detected prior to its implementation on the network.*	Anti-malware technology is installed and running on Ignite Procurement laptops and/or desktops to protect from malicious software	Inspected that there are minimum device configuration settings.	No Exceptions Noted
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.			
System Operations	CC7.1	1	*Uses Defined Configuration Standards—Management has defined configuration standards.*	There are minimum device configuration settings established.	Inspected that there are minimum device configuration settings.	No Exceptions Noted
System Operations	CC7.1	2	*Monitors Infrastructure and Software—The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the*	Ignite Procurement has implemented tools for automated threat detection to the production network.	Inspected that there are threat detection and monitoring enabled on Ignite's network.	No Exceptions Noted

			entity's objectives.			
System Operations	CC7.1	3	*Implements Change-Detection Mechanisms—The IT system includes a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files.*	Ignite Procurement has a Change Management Policy governing the system development lifecycle (infrastructure, data, software, and procedures), including procedures for tracking, testing, approving, and validating changes.	Inspected the Change Management Policy.	No Exceptions Noted
System Operations	CC7.1	4	*Detects Unknown or Unauthorized Components—Procedures are in place to detect the introduction of unknown or unauthorized components.*	Ignite Procurement has a Change Management Policy governing the system development lifecycle (infrastructure, data, software, and procedures), including procedures for tracking, testing, approving, and validating changes.	Inspected the Change Management Policy.	No Exceptions Noted
System Operations	CC7.1	5	*Conducts Vulnerability Scans—The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis.*	Ignite Procurement has a policy for vulnerability and patch management to guide it in the detection and remediation of vulnerabilities.	Inspected the Information Security Policy.	No Exceptions Noted
System Operations	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.			
System Operations	CC7.2	1	*Implements Detection Policies, Procedures,*	Ignite Procurement has a Change	Inspected the Change	No Exceptions

			and Tools—Detection policies and procedures are defined and implemented, and detection tools are implemented on Infrastructure and software to identify anomalies in the operation or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management that includes provision of resources; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities.	Management Policy governing the system development lifecycle (infrastructure, data, software, and procedures), including procedures for tracking, testing, approving, and validating changes.	Management Policy.	Noted
System Operations	CC7.2	2	*Designs Detection Measures—Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software.*	Ignite Procurement has a Change Management Policy governing the system development lifecycle (infrastructure, data, software, and procedures), including procedures for tracking, testing, approving, and validating changes.	Inspected the Change Management Policy.	No Exceptions Noted
System Operations	CC7.2	3	*Implements Filters to Analyze Anomalies—Management has implemented procedures to filter, summarize, and analyze anomalies to*	Ignite Procurement maintains an inventory of assets, including system components and company devices. Each	Inspected the Compliance and Asset Management Policy.	No Exceptions Noted

			identify security events.	asset has an assigned asset owner, and such inventory list is reviewed at least annually.		
System Operations	CC7.2	4	*Monitors Detection Tools for Effective Operation—Management has implemented processes to monitor the effectiveness of detection tools.*	Ignite Procurement has a Change Management Policy governing the system development lifecycle (infrastructure, data, software, and procedures), including procedures for tracking, testing, approving, and validating changes.	Inspected the Change Management Policy.	No Exceptions Noted
System Operations	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.			
System Operations	CC7.3	1	*Responds to Security Incidents—Procedures are in place for responding to security incidents and evaluating the effectiveness of those policies and procedures on a periodic basis.*	Ignite Procurement has assigned responsibility for the creation, implementation, and management of company policies and procedures. All policies are reviewed at least annually and updated as necessary by Ignite Procurement management.	Inspected that Ignite Procurement has policy owners with direct responsibility over portions of the Ignite Procurement Information Security Programs.	No Exceptions Noted
System Operations	CC7.3	2	*Communicates and Reviews Detected Security Events—Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary.*	Ignite Procurement has assigned responsibility for the creation, implementation, and management of company policies and procedures. All policies are reviewed at least annually and updated as necessary by Ignite Procurement management.	Inspected that Ignite Procurement has policy owners with direct responsibility over portions of the Ignite Procurement Information Security Programs.	No Exceptions Noted

System Operations	CC7.3	3	*Develops and Implements Procedures to Analyze Security Incidents—Procedures are in place to analyze security incidents and determine system impact.*	Ignite Procurement has implemented tools for automated threat detection to the production network.	Inspected that Ignite Procurement automatically detects threats to the production network.	No Exceptions Noted
System Operations	CC7.3	4	*Assesses the Impact on Personal Information—Detected security events are evaluated to determine whether they could or did result in the unauthorized disclosure or use of personal information and whether there has been a failure to comply with applicable laws or regulations.*	Ignite Procurement uses tools to log security events, user activity, application states and system performance from its cloud infrastructure. Such logs are reviewed to identify and report unusual or malicious activities.	Inspected that Ignite Procurement enables logging to track activity and configuration changes.	No Exceptions Noted
System Operations	CC7.3	5	*Determines Personal Information Used or Disclosed—When an unauthorized use or disclosure of personal information has occurred, the affected information is identified.*	Ignite Procurement uses tools to log security events, user activity, application states and system performance from its cloud infrastructure. Such logs are reviewed to identify and report unusual or malicious activities.	Inspected that Ignite Procurement enables logging to track activity and configuration changes.	No Exceptions Noted
System Operations	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.			
System Operations	CC7.4	1	*Assigns Roles and Responsibilities—Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are assigned, including the use of external resources when necessary.*	All positions at Ignite Procurement have detailed job descriptions that define roles and responsibilities and are freely available to personnel.	Inspected that Ignite Procurement has job descriptions that are available and reviewed at least once per year.	No Exceptions Noted

System Operations	CC7.4	2	*Contains Security Incidents—Procedures are in place to contain security incidents that actively threaten entity objectives.*	A Security Incident Response Plan is in place. Such plan includes (i) creation of a security incident response team that assesses, prioritizes and resolves identified risks and (ii) communicates to users where to report suspected security issues.	Inspected that Ignite Procurement has a Security Incident Response Plan in place to deal with security incidents.	No Exceptions Noted
System Operations	CC7.4	3	*Mitigates Ongoing Security Incidents—Procedures are in place to mitigate the effects of ongoing security incidents.*	A Security Incident Response Plan is in place. Such plan includes (i) creation of a security incident response team that assesses, prioritizes and resolves identified risks and (ii) communicates to users where to report suspected security issues.	Inspected that Ignite Procurement has a Security Incident Response Plan in place to deal with security incidents.	No Exceptions Noted
System Operations	CC7.4	4	*Ends Threats Posed by Security Incidents—Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions.*	A Security Incident Response Plan is in place. Such plan includes (i) creation of a security incident response team that assesses, prioritizes and resolves identified risks and (ii) communicates to users where to report suspected security issues.	Inspected that Ignite Procurement has a Security Incident Response Plan in place to deal with security incidents.	No Exceptions Noted
System Operations	CC7.4	5	*Restores Operations—Procedures are in place to restore data and business operations to an interim state that permits the achievement of entity objectives.*	A Business Continuity and Disaster Recovery Plan is in place and tested annually.	Inspected that Ignite Procurement has a Business Continuity and Disaster Recovery Plan in place to handle backups, and the steps necessary to recover from potential	No Exceptions Noted

					disasters.	
System Operations	CC7.4	6	*Develops and Implements Communication Protocols for Security Incidents—Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives.*	Ignite Procurement uses tools to monitor its cloud infrastructure and network activity. Ignite Procurement uses automatic alerts to identify system performance and potential malicious activities. Such alerts are sent to the appropriate team members via email or another communication channel. Identified incidents are resolved according to Ignite Procurement policies.	Inspected that Ignite Procurement enables monitoring on its servers, databases, message queues, and load balancers.	No Exceptions Noted
System Operations	CC7.4	7	*Obtains Understanding of Nature of Incident and Determines Containment Strategy—An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach.*	After any identified security incident has been resolved, management provides a "Lessons Learned" document to the team in order to continually improve Ignite Procurement security and operations.	Inspected that Ignite Procurement provides a "Lessons Learned" document to the team after any identified security incidents.	No Exceptions Noted
System Operations	CC7.4	8	*Remediates Identified Vulnerabilities—Identified vulnerabilities are remediated through the development and execution of remediation activities.*	Ignite Procurement has a policy for vulnerability and patch management to guide it in the detection and remediation of vulnerabilities.	Inspected that Ignite Procurement has a Vulnerability Management Policy in place to govern the detection and remediation	No Exceptions Noted

					of vulnerabilities.	
System Operations	CC7.4	9	*Communicates Remediation Activities—Remediation activities are documented and communicated in accordance with the incident response program.*	Security Incident Response Plan is in place. Such plan includes (i) creation of a security incident response team that assesses, prioritizes and resolves identified risks and (ii) communicates to users where to report suspected security issues.	Inspected that Ignite Procurement has a Security Incident Response Plan in place to deal with security incidents.	No Exceptions Noted
System Operations	CC7.4	10	*Evaluates the Effectiveness of Incident Response—The design of incident response activities is evaluated for effectiveness on a periodic basis._*	Ignite Procurement has assigned responsibility for the creation, implementation, and management of company policies and procedures. All policies are reviewed at least annually and updated as necessary by Ignite Procurement management.	Inspected that Ignite Procurement has policy owners with direct responsibility over portions of the Ignite Procurement Information Security Programs.	No Exceptions Noted
System Operations	CC7.4	11	*Periodically Evaluates Incidents—Periodically, management reviews incidents related to security, availability, processing integrity, confidentiality, and privacy and identifies the need for system changes based on incident patterns and root causes.*	After any identified security incident has been resolved, management provides a "Lessons Learned" document to the team in order to continually improve Ignite Procurement security and operations.	Inspected that Ignite Procurement provides a "Lessons Learned" document to the team after any identified security incidents.	No Exceptions Noted
System Operations	CC7.4	12	*Communicates Unauthorized Use and Disclosure—Events that resulted in unauthorized use or disclosure of personal information are communicated to the data subjects, legal and regulatory authorities, and others as required.*	Ignite Procurement notifies its customer about critical changes (such as changes to terms, services, security, confidentiality or availability) as appropriate.	Inspected that Ignite Procurement provides updates on critical changes through a public URL (change log, status page, or blog), through	No Exceptions Noted

					email or other communication means, as appropriate.	
System Operations	CC7.4	13	*Application of Sanctions—The conduct of individuals and organizations operating under the authority of the entity and involved in the unauthorized use or disclosure of personal information is evaluated and, if appropriate, sanctioned in accordance with entity policies and legal and regulatory requirements.*	Violations of Ignite Procurement policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	Inspected that Ignite Procurement's policies contain a discipline statement that is clearly documented and available.	No Exceptions Noted
System Operations	CC7.5		The entity identifies, develops, and implements activities to recover from identified security incidents.			
System Operations	CC7.5	1	*Restores the Affected Environment—The activities restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, and changing configurations, as needed.*	Ignite Procurement has a policy for vulnerability and patch management to guide it in the detection and remediation of vulnerabilities.	Inspected that Ignite Procurement has a Vulnerability Management Policy in place to govern the detection and remediation of vulnerabilities.	No Exceptions Noted
System Operations	CC7.5	2	*Communicates Information About the Event—Communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are made to management and others as appropriate (internal and*	After any identified security incident has been resolved, management provides a "Lessons Learned" document to the team in order to continually improve Ignite Procurement security and operations.	Inspected that Ignite Procurement provides a "Lessons Learned" document to the team after any identified security incidents.	No Exceptions Noted

			external).			
System Operations	CC7.5	3	*Determines Root Cause of the Event—The root cause of the event is determined.*	A Security Incident Response Plan is in place. Such plan includes (i) creation of a security incident response team that assesses, prioritizes and resolves identified risks and (ii) communicates to users where to report suspected security issues.	Inspected that Ignite Procurement has a Security Incident Response Plan in place to deal with security incidents.	No Exceptions Noted
System Operations	CC7.5	4	*Implements Changes to Prevent and Detect Recurrences—Additional architecture or changes to preventive and detective controls, or both, are implemented to prevent and detect recurrences on a timely basis.*	Ignite Procurement has a Change Management Policy governing the system development lifecycle (infrastructure, data, software, and procedures), including procedures for tracking, testing, approving, and validating changes.	Inspected that Ignite Procurement patches its systems in accordance with its Change Management Policy to protect from new risks.	No Exceptions Noted
System Operations	CC7.5	5	*Improves Response and Recovery Procedures—Lessons learned are analyzed, and the incident response plan and recovery procedures are improved.*	After any identified security incident has been resolved, management provides a "Lessons Learned" document to the team in order to continually improve Ignite Procurement security and operations.	Inspected that Ignite Procurement provides a "Lessons Learned" document to the team after any identified security incidents.	No Exceptions Noted
System Operations	CC7.5	6	*Implements Incident Recovery Plan Testing—Incident recovery plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential*	All policies are reviewed at least annually and updated as necessary.	Inspected that Ignite Procurement's Information Security Policy and Plans are reviewed annually by the applicable policy owner.	No Exceptions Noted

			for the lack of availability of key personnel; and (4) revision of continuity plans, and systems based on test results.			
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.			
Change Management	CC8.1	1	*Manages Changes Throughout the System Lifecycle—A process for managing system changes throughout the lifecycle of the system and its components (infrastructure, data, software, and procedures) is used to support system availability and processing integrity.*	To manage, authorize, design, develop, and document changes, a version control system manages source code, documentation, release labeling, and other change management tasks.	Inspected that Ignite Procurement utilizes a version control system for version control management.	No Exceptions Noted
Change Management	CC8.1	2	*Authorizes Changes—A process is in place to authorize system changes prior to development.*	Ignite Procurement requires approval from 1 or more independent engineers prior to deploying a change into production. Changes cannot be deployed without independent approval.	Inspected that Ignite Procurement has an approval process in place prior to the deployment of changes to production.	No Exceptions Noted
Change Management	CC8.1	3	*Designs and Develops Changes—A process is in place to design and develop system changes.*	Ignite Procurement has a Change Management Policy governing the system development lifecycle (infrastructure, data, software, and procedures), including procedures for tracking, testing, approving, and validating changes.	Inspected that Ignite Procurement patches its systems in accordance with its Change Management Policy to protect from new risks.	No Exceptions Noted
Change Management	CC8.1	4	*Documents Changes—A process is in place to document system changes to support*	Ignite Procurement requires that configuration changes are reviewed, tested	Inspected that configuration changes are	No Exceptions Noted

			ongoing maintenance of the system and to support system users in performing their responsibilities.	(where applicable), and approved prior to being deployed into production.	reviewed, tested, and approved.	
Change Management	CC8.1	5	*Tracks System Changes—A process is in place to track system changes prior to implementation.*	To manage, authorize, design, develop, and document changes, a version control system manages source code, documentation, release labeling, and other change management tasks. Only system administrators can provide access.	Inspected that Ignite Procurement utilizes a version control system for version control management.	No Exceptions Noted
Change Management	CC8.1	6	*Configures Software—A process is in place to select and implement the configuration parameters used to control the functionality of software.*	Ignite Procurement requires that configuration changes are reviewed, tested (where applicable), and approved prior to being deployed into production.	Inspected that configuration changes are reviewed, tested, and approved.	No Exceptions Noted
Change Management	CC8.1	7	*Tests System Changes—A process is in place to test system changes prior to implementation.*	Ignite Procurement tests changes prior to deploying into production.	Inspected that Ignite Procurement uses continuous integration to test changes before deploying to production.	No Exceptions Noted
Change Management	CC8.1	8	*Approves System Changes—A process is in place to approve system changes prior to implementation.*	Ignite Procurement requires approval from 1 or more independent engineers prior to deploying a change into production. Changes cannot be deployed without independent approval.	Inspected that Ignite Procurement has an approval process in place prior to the deployment of changes to production.	No Exceptions Noted
Change Management	CC8.1	9	*Deploys System Changes—A process is in place to implement system changes.*	Ignite Procurement has a Change Management Policy governing the system development lifecycle (infrastructure,	Inspected that Ignite Procurement patches its systems in accordance	No Exceptions Noted

				data, software, and procedures), including procedures for tracking, testing, approving, and validating changes.	with its Change Management Policy to protect from new risks.	
Change Management	CC8.1	10	*Identifies and Evaluates System Changes—Objectives affected by system changes are identified, and the ability of the modified system to meet the objectives is evaluated throughout the system development life cycle.*	Ignite Procurement has a Change Management Policy governing the system development lifecycle (infrastructure, data, software, and procedures), including procedures for tracking, testing, approving, and validating changes.	Inspected that Ignite Procurement patches its systems in accordance with its Change Management Policy to protect from new risks.	No Exceptions Noted
Change Management	CC8.1	11	*Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents—Changes in infrastructure, data, software, and procedures required to remediate incidents to continue to meet objectives are identified, and the change process is initiated upon identification.*	Ignite Procurement tests changes prior to deploying into production.	Inspected that Ignite Procurement uses continuous integration to test changes before deploying to production.	No Exceptions Noted
Change Management	CC8.1	12	*Creates Baseline Configuration of IT Technology—A baseline configuration of IT and control systems is created and maintained.*	Configuration standards are in place and required to be utilized when deploying new servers into production.	Inspected that Ignite Procurement has a Configuration and Asset Management Policy that governs system configuration s for new systems.	No Exceptions Noted
Change Management	CC8.1	13	*Provides for Changes Necessary in Emergency Situations—A process is in place for authorizing,*	Ignite Procurement has a Change Management Policy governing the system	Inspected that Ignite Procurement patches its systems in	No Exceptions Noted

			designing, testing, approving, and implementing changes necessary in emergency situations (that is, changes that need to be implemented in an urgent timeframe).	development lifecycle (infrastructure, data, software, and procedures), including procedures for tracking, testing, approving, and validating changes.	accordance with its Change Management Policy to protect from new risks.	
Change Management	CC8.1	14	*Protects Confidential Information—The entity protects confidential information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to confidentiality.*	The Ignite Procurement production, staging and development environments are segregated.	Inspected that Ignite Procurement's production, staging and development environments are segregated.	No Exceptions Noted
Change Management	CC8.1	15	*Protects Personal Information—The entity protects personal information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to privacy.*	The Ignite Procurement production, staging and development environments are segregated.	Inspected that Ignite Procurement's production, staging and development environments are segregated.	No Exceptions Noted
Risk Mitigation	CC9.1		The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
Risk Mitigation	CC9.1	1	*Considers Mitigation of Risks of Business Disruption—Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and*	Ignite Procurement implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks. The risk assessment process determines how to respond and manage risk,	Inspected that Ignite Procurement has a risk assessment policy in place to guide it during its risk assessments.	No Exceptions Noted

			communications to meet the entity's objectives during response, mitigation, and recovery efforts.	including whether to accept, avoid, reduce, or share the risk.		
Risk Mitigation	CC9.1	2	*Considers the Use of Insurance to Mitigate Financial Impact Risks—The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.*	Ignite Procurement implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks.	Inspected that Ignite Procurement has a risk assessment policy in place to guide it during its risk assessments.	No Exceptions Noted
Risk Mitigation	CC9.2		The entity assesses and manages risks associated with vendors and business partners.			
Risk Mitigation	CC9.2	1	*Establishes Requirements for Vendor and Business Partner Engagements—The entity establishes specific requirements for a vendor and business partner engagement that includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.*	Ignite Procurement has a vendor management program in place for evaluating vendor performance and compliance with contractual obligations.	Inspected that Ignite Procurement uses Secureframe to manage its vendor management program and has a Vendor Management Policy in place.	No Exceptions Noted
Risk Mitigation	CC9.2	2	*Assesses Vendor and Business Partner Risks—The entity assesses, on a periodic basis, the risks that vendors and business partners (and those entities' vendors and business partners) represent to the achievement of the entity's objectives.*	Ignite Procurement has a vendor management program in place for evaluating vendor performance and compliance with contractual obligations.	Inspected the vendor management section of the Information Security Policy.	No Exceptions Noted
Risk Mitigation	CC9.2	3	*Assigns Responsibility and Accountability for Managing Vendors and Business Partners—The*	Ignite Procurement has a vendor management program in place for evaluating	Inspected that Ignite Procurement uses	No Exceptions Noted

			entity assigns responsibility and accountability for the management of risks associated with vendors and business partners.	vendor performance and compliance with contractual obligations.	Secureframe to manage its vendor management program and has a Vendor Management Policy in place.	
Risk Mitigation	CC9.2	4	*Establishes Communication Protocols for Vendors and Business Partners—The entity establishes communication and resolution protocols for service or product issues related to vendors and business partners.*	The organization communicates using telephone, video conferencing tools, messaging tools, email, physical mail, and in person.	Inspected the Business Continuity and Disaster Recovery Plan.	No Exceptions Noted
Risk Mitigation	CC9.2	5	*Establishes Exception Handling Procedures from Vendors and Business Partners —The entity establishes exception handling procedures for service or product issues related to vendors and business partners.*	Ignite Procurement has a vendor management program in place for evaluating vendor performance and compliance with contractual obligations.	Inspected that Ignite Procurement uses Secureframe to manage its vendor management program and has a Vendor Management Policy in place.	No Exceptions Noted
Risk Mitigation	CC9.2	6	*Assesses Vendor and Business Partner Performance—The entity periodically assesses the performance of vendors and business partners.*	Ignite Procurement has a vendor management program in place for evaluating vendor performance and compliance with contractual obligations.	Inspected that Ignite Procurement uses Secureframe to manage its vendor management program and has a Vendor Management Policy in place.	No Exceptions Noted
Risk Mitigation	CC9.2	7	*Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments—The entity implements procedures for addressing issues identified with vendor and business partner relationships.*	Ignite Procurement has a vendor management program in place for evaluating vendor performance and compliance with contractual obligations.	Inspected that Ignite Procurement uses Secureframe to manage its vendor management program and has a Vendor Management	No Exceptions Noted

					Policy in place.	
Risk Mitigation	CC9.2	8	*Implements Procedures for Terminating Vendor and Business Partner Relationships — The entity implements procedures for terminating vendor and business partner relationships.*	Ignite Procurement has a vendor management program in place for evaluating vendor performance and compliance with contractual obligations.	Inspected Vendor Management within the Information Security Policy.	No Exceptions Noted
Risk Mitigation	CC9.2	9	*Obtains Confidentiality Commitments from Vendors and Business Partners—The entity obtains confidentiality commitments that are consistent with the entity's confidentiality commitments and requirements from vendors and business partners who have access to confidential information.*	Ignite Procurement has a vendor management program in place for evaluating vendor performance and compliance with contractual obligations	Inspected Vendor Management within the Information Security Policy.	No Exceptions Noted
Risk Mitigation	CC9.2	10	*Assesses Compliance with Confidentiality Commitments of Vendors and Business Partners — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's confidentiality commitments and requirements.*	Ignite Procurement has a vendor management program in place for evaluating vendor performance and compliance with contractual obligations	Inspected Vendor Management within the Information Security Policy.	No Exceptions Noted
Risk Mitigation	CC9.2	11	*Obtains Privacy Commitments from Vendors and Business Partners—The entity obtains privacy commitments, consistent with the entity's privacy commitments and requirements, from vendors and business partners who have access to personal information.*	Ignite Procurement has a vendor management program in place for evaluating vendor performance and compliance with contractual obligations	Inspected Vendor Management within the Information Security Policy.	No Exceptions Noted
Risk Mitigation	CC9.2	12	*Assesses Compliance with Privacy Commitments of Vendors and Business Partners— On a*	Ignite Procurement has a vendor management program in place for evaluating	Inspected Vendor Management within the Information	No Exceptions Noted

			periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's privacy commitments and requirements and takes corrective action as necessary.	vendor performance and compliance with contractual obligations	Security Policy.	
Additional Criteria for Availability	A1.2	1	*Identifies Environmental Threats—As part of the risk assessment process, management identifies environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water.*	GCP is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.	Inspected the complementary subservice organization controls within the system description.	No Exceptions Noted
Additional Criteria for Availability	A1.2	3	*Implements and Maintains Environmental Protection Mechanisms—Management implements and maintains environmental protection mechanisms to prevent and mitigate against environmental events.*	GCP is responsible for overseeing the regular maintenance of environmental protections at data centers	Inspected the complementary subservice organization controls	No Exceptions Noted
Additional Criteria for Availability	A1.2	5	*Responds to Environmental Threat Events—Procedures are in place for responding to environmental threat events and for evaluating the effectiveness of those policies and procedures on a periodic basis. This includes automatic mitigation systems (for example, uninterruptable power system and generator back-up subsystem).*	GCP is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.	Inspected the complementary subservice organization controls within the system description.	No Exceptions Noted