Proprietary & Confidential

e-Builder Enterprise - Commercial Edition

SOC 3

Relevant to Security, Availability, and Confidentiality

Integrated SOC 3 Report Prepared in Accordance with the AICPA Attestation Standards and IAASB ISAE No. 3000 (Revised) Standards

OCTOBER 1, 2022 TO SEPTEMBER 30, 2023

MOSSADAMS

Table of Contents

I. Independent Service Auditor's Report

Trimble Inc.
10368 Westmoor Dr.
Westminster, CO 80021

To the Management of Trimble Inc.:

Scope

We have examined Trimble Inc.'s accompanying assertion in Section II titled "Trimble Inc.'s Assertion" (assertion) that the controls within Trimble Inc.'s e-Builder Enterprise – Commercial Edition (system) were effective throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that Trimble Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Trimble Inc. uses Amazon Web Services for hosting services (subservice organization). Our examination did not include the services provided by the subservice organization.

Service Organization's Responsibilities

Trimble Inc. 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 Trimble Inc.'s service commitments and system requirements were achieved. Trimble Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Trimble Inc. is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Trimble Inc.'s service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Trimble Inc.'s service commitments and system requirements based the applicable trust services criteria

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

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.

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

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness 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.

Opinion

In our opinion, management's assertion that the controls within Trimble Inc.'s e-Builder Enterprise – Commercial Edition were effective throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that Trimble Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Moss Adams LLP

Seattle, Washington
December 13, 2023

II. Trimble Inc.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Trimble Inc.'s e-Builder Enterprise – Commercial Edition (system) throughout the period October 1, 2022 to September 30, 2023 to provide reasonable assurance that Trimble Inc.'s service commitments and system requirements relevant to Security, Availability, and Confidentiality were achieved. Our description of the boundaries of the system is presented in Section III titled "Trimble Inc.'s Description of the Boundaries of e-Builder Enterprise – Commercial Edition" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that Trimble Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP Section 100*, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA*, Trust Services Criteria)*. Trimble Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section III titled "Trimble Inc.'s Description of the Boundaries of e-Builder Enterprise – Commercial Edition".

Trimble Inc. uses Amazon Web Services for hosting services (subservice organization). The description does not disclose the actual controls at the subservice organization.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that Trimble Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

III. Trimble Inc.'s Description of the Boundaries of e-Builder Enterprise – Commercial Edition

A. Overview of Operations

1. Overview

COMPANY BACKGROUND

Trimble Inc. (Trimble) (NASDAQ: TRMB) is delivering products and services that connect the physical and digital worlds. Core technologies in positioning, modeling, connectivity, and data analytics enable customers to improve productivity, quality, safety, and sustainability. From purpose-built products to enterprise lifecycle solutions, Trimble software, hardware, and services are transforming a broad range of industries such as agriculture, construction, geospatial, and transportation and logistics. Established in 1978, Trimble has expanded its solutions to serve industries across the globe with over 2,000 issued patents for advances in technology. With over 12,000 employees in over 40 countries, Trimble has core technologies in positioning, modeling, connectivity, and data analytics.

Founded in 1995, e-Builder Inc., a Trimble Company, is the leading cloud-based construction program management software for asset owners and the organizations that act on their behalf. The company develops e-Builder Enterprise – Commercial Edition (e-Builder Enterprise™), a program management solution for owners for capital projects that improves project outcomes by delivering trusted insight, improved process control and reduced cycle times across the entire project lifecycle. Continued development of e-Builder Enterprise is aligned with the development of Trimble Asset Lifecycle Management solutions, to help customers manage 350,000 active capital projects worth over $1 trillion (USD). The company is based in Sunrise, Florida.

On February 2, 2018, Trimble acquired privately held e-Builder Inc. to expand its technology portfolio to serve asset owners. The company is referred to herein as "Trimble," whereas references to the in-scope system are referred to as "e-Builder" or "e-Builder Enterprise."

DESCRIPTION OF SERVICES PROVIDED

e-Builder Enterprise is a cloud-based, construction program management information solution (PMIS) for capital projects that delivers trusted insight into performance across the entire project lifecycle, reducing risk and improving performance. e-Builder Enterprise centralizes information related to customers' projects from data, documentation, change orders, resource management, and invoicing for visibility and transparency into projects.

e-Builder solutions manage major capital projects in the following industries:

- Commercial markets
- K-12 schools
- Higher education
- Healthcare
- Utilities
- Government

The following phases of a capital improvement program (CIP) are tracked and managed from the planning phase through completion:

- *Planning* – informed decision making and streamlined communication.
- *Design* – design review facilitated with building information models (BIM).
- *Procurement* – save time and costs with streamlined bidding processes.
- *Construction* – real-time data keeps projects on-time and on-budget.
- *Operations* – centralize document management during facility maintenance.

PLANNING

e-Builder Enterprise's capital planning tools automate the process of keeping stakeholders in the loop on planned and approved project statuses.

Current historical and potential project planning data are maintained in one central location, so that data from past projects can be used to define contingency budgets and accurately predict the cost-to-complete and cash flow needs.

A summary of the e-Builder Enterprise planning functionalities is listed below:

- Capital planning
- Portfolio analysis
- Funding allocation
- Historical performance
- Risk and exposure

DESIGN

Customers can manage the design phase of their CIP with one control location, and process submission and approvals with vendors, partners, and stakeholders.

Additionally, automatic version control for design files provides the ability to redline and mark up drawings as needed. Customers can view 2D computer-aided design (CAD) files from within their browser. Automated workflows ensure the designs are reviewed in a timely manner and allow customers to track and choose out design issues.

A summary of the e-Builder Enterprise design functionalities is listed below:

- Schematic and design development
- Design review and approvals
- Constructability
- Design standards

PROCUREMENT

Open bids invite a predefined set of potential bidders (including public bidding), distribute bid packages and issue addenda, respond to questions and update bidders, and compile bid responses in a standard format, in a central location.

A summary of the e-Builder Enterprise procurement functionalities is listed below:

- Bid and request for proposal (RFP) management
- Work package estimates
- Bid tabulation
- Bid-leveling and awards
- Vendor and small business enterprise (SBE) / disadvantaged business enterprise (DBE) tracing

CONSTRUCTION

In the construction phase of a project, e-Builder Enterprise provides accurate, real-time monitoring and forecasts, to avoid surprises and to reduce risk.

e-Builder Enterprise's integrated modules eliminates data silos and allows for real-time tracking and visibility into the entire project. In the event of any "risk" such as change order or resource management changes or shift, e-Builder Enterprise immediately confirms how that "risk" impacts the overall project, providing transparency.

In addition, reporting and business intelligence (BI) tools provide graphically rich dashboards to gain insight into project performance.

A summary of the e-Builder Enterprise construction functionalities is listed below:

- Schedule and resource management
- Cost control
- Construction administration (submittals and requests for information (RFIs))
- Change management
- Inspections and payments
- Funding management
- Claims mitigation
- Dashboards and BI

OPERATIONS

Once the project is complete, e-Builder Enterprise will serve as a central repository to store everything from as-built documents to warranty information to BIM reference models.

Having documentation in one place allows for team members to pull the latest final information to keep the facility running smoothly. Additionally, when maintenance or renovation is required, structural documents are available.

A summary of the e-Builder Enterprise operations functionalities is listed below:

- As-built documents
- Punch lists
- Commissioning
- Warranty

- Occupancy and records retention
- BIM reference model

2. Infrastructure and Software

INFRASTRUCTURE

e-Builder's production infrastructure resides in the AWS Elastic Cloud Compute (EC2) VPC environment.

For high availability and infrastructure resilience, the AWS production infrastructure is distributed across availability zones within the following geographically diverse AWS regions: United States (US) East (N. Virginia) (us-east-1), US West (N. California) (us-west-1), US West (Oregon) (us-west-2), and Canada (Central) (ca-central-1) regions.

Availability zones within AWS are one or more discrete data centers with redundant power, networking, and connectivity in an AWS region. Availability zones provide the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible from a single data center. Availability zones in an AWS region are interconnected with high-bandwidth, low-latency networking, over redundant, dedicated metro fiber providing high-throughput, low-latency networking between availability zones. Traffic between availability zones is encrypted.

Production data is stored in Microsoft SQL Server databases. SQL server replication is utilized such that production data from the primary SQL server instance is replicated to a secondary replica located in a separate availability zone within the region. Amazon EC2 virtual server instances running on both Linux and Windows operating systems are utilized to support e-Builder Enterprise. Active Directory and Okta are utilized to restrict access to the front-end AWS management console via Single Sign-On (SSO) and an identity provider (IDP) trust relationship with e-Builder's AWS account. Back-end access to the production environment via the AWS command line interface (CLI) via secure shell (SSH) client requires users to first authenticate to Okta and the Pritunl virtual private network (VPN) utilizing their Active Directory credentials.

Active Directory, Okta, and Pritunl VPN are managed by Trimble's corporate information technology (IT) team and therefore controls around the administration of these systems was considered outside the boundaries of this examination. Testing of these systems was limited to how the systems are utilized to restrict access to e-Builder production resources such as the AWS production environment and the SQL production databases (e.g., authentication and security configurations such as SSO, MFA, and encrypted connections as well as Active Directory groups utilized to restrict access to e-Builder systems).

The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
Active Directory (AD)	Network domain supporting SSO to the in-scope systems.	Windows	AWS (us-east-1, us-west-1, us-west-2, ca-central-1)
Amazon EC2	Amazon EC2 instances are virtual servers supporting the e-Builder Construction PMIS system.	Amazon Linux Amazon Machine Image (AMI) 2015.08; Windows Server 2019	
Microsoft SQL Server Databases	Relational database management system (RDBMS) supporting the e-Builder Construction PMIS system.	Microsoft SQL Server 2019	
Security Groups	Act as virtual firewalls for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level. Security groups are managed within the AWS management console.	AWS EC2 VPC	
Amazon EBS	Block-level storage service for use with Amazon EC2 for both throughput and transaction intensive workloads. Microsoft SQL Server relational databases are deployed on Amazon EBS.	Amazon Proprietary	
Amazon S3	Object storage service utilized to store and protect data by providing availability, security, and performance.		
Pritunl VPN	Encrypted VPNs requiring MFA for remote access to certain production resources.	Pritunl	AWS (us-east-1)

3. People

The following groups are responsible for providing services related to Trimble's e-Builder Enterprise:

- *Trimble Executive Management* – responsible for overseeing company-wide activities, establishing, and accomplishing goals, controls, and overseeing objectives.
- *Trimble Audit Committee* – select members of the board who monitor the corporate financial reporting and the internal and external controls and audits of Trimble.
- *Business Operations*/*Sector Leadership* – provides strategic and tactical guidance to divisions in support of commitments to customers.

- *People eXperience* (typically known as Human Resources (HR)) – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).
- *Cybersecurity* (*Cyber*) *team* – the corporate function responsible for managing global security controls, policies, and processes. The Vice President of Cybersecurity leads the Cyber organization and reports to Trimble's Board of Directors on the effectiveness of controls.
- *IT and Operations personnel* – responsible for risk management; identification, containment, and resolution of security issues and incidents throughout the service delivery infrastructure; and 24x7 monitoring of systems, applications, and incidents for products within their review.
- *Product Development* – dedicated product development and quality assurance teams are responsible for maintaining and enhancing Trimble's e-Builder Enterprise. These teams adhere to a secure software development lifecycle.
- *Customer Success and Support* – responsible for supporting customers.

4. Data

Documented information classification policies, as well as customer data retention and disposal procedures, are in place to guide personnel with use, handling, retention, and disposal of customer data. Trimble data is categorized according to the information classification policies and is protected according to its classification.

Information is classified in the following categories:

- *Public* – information intended for general public use.
- *Internal* – information must be protected in such a manner that it is only accessible to authorized Trimble personnel and business partners.
- *Confidential* / *Restricted* – information must be protected to the highest degree and access must be restricted to specific roles within the organization on a need-to-know basis. This includes customer and proprietary data.

Restricted data is encrypted. Access to encryption keys is restricted to user accounts accessible by authorized personnel. From there, various queries and algorithms are utilized to process the data, with the purpose of making it accessible to Trimble's customers. Data is owned by customers and is accessible via various modules and services where customers manage access amongst their users. Web communications between Trimble servers and the customer portals are encrypted utilizing TLS encryption protocol.

Upon termination or expiration of a customer agreement, all customer data is retained for 90 days (the "Retention Period"). Within 90 days of the conclusion of the Retention Period, customer data is deleted from the database and project documents are deleted from the file store. Customer data and project documents remain part of the database backups for 90 days after deletion from the database and file store.

Data Used and Supported by the System	Data Reporting	Data Reporting Classification
Executive Summary	• Budget vs. estimated at completion • Budget vs. commitments vs. actuals • Construction % complete • Construction schedule variance • Forecasted over / under	Confidential
Administrative	• Document upload (last seven days) • Invoice average turnaround time • Role membership • Number of user logins • User log	
Implementation	• Action items due / past due • Key decision tracker • Master schedule report • Upcoming tasks	
Actual Cost Reports	• Program summary (grouped by company, month, quarter, status) • Project detail (grouped by invoice number) • Project summary (grouped by company, month, quarter, status)	
Bidding	• Awarded bidders • Bid tabulation summary • Bidder activity • Project bid summary	
Budget and Trend Analysis	• Budget approved • Budget cost • Budget variance • Budget change	
Cash Flow	• Program summary (grouped by month, quarter, year) • Project summary (grouped by month, quarter, year) • Cash flow detail (by year, month)	
Commitments and Project Management	• Change orders • Contracts • Purchase orders	

Data Used and Supported by the System	Data Reporting	Data Reporting Classification
Schedule	• Critical tasks • Milestones • Schedule finish variance • Task variance alerts	

5. Processes and Procedures

ACCESS PROVISIONING, REVIEW, AND REVOCATION

Trimble utilizes an automated ticketing system to perform access management and administration activities, including provisioning access, deprovisioning access, and conducting user access reviews. Upon hire, access is provisioned to employees based on their job roles and responsibilities. Requests for access beyond their specific job requirements require explicit approval by management. When an employee is terminated, the employee's manager alerts HR, who submits a termination ticket to communicate access removal responsibilities to the Trimble operations team.

To help ensure access rights are authorized, Trimble performs a full access review of logical access to production infrastructure at least annually. The user access reviews include compiling user account lists, requesting review from system owners, recording anomalies, and confirming that unauthorized access has been rectified. Changes resulting from the review are tracked and approved to help ensure access modifications are controlled.

SYSTEM ACCOUNT MANAGEMENT

Formally documented policies and procedures are in place to guide personnel in the requirements for implementing and maintaining logical security controls when utilizing information assets. Access to the production infrastructure is protected by multiple authentication and authorization mechanisms.

Administrative access privileges within Trimble's production infrastructure, including AD, VPNs, virtualization platforms, production servers, firewalls, cloud management services, are restricted to user accounts accessible by authorized IT and Operations personnel.

CHANGE MANAGEMENT

Application and infrastructure change management policies and procedures are documented to guide personnel in the change and release management process.

Change requests are entered into a ticketing system and/or checklist to track the application and infrastructure change requests through implementation to production. There are quality assurance (Dev/Stage) environments that development teams utilize to validate changes prior to release to the production environment. Changes are developed and tested in environments that are logically and/or physically separated from production and approved prior to implementation.

Trimble utilizes version control software to manage and restrict access to, and modification of, application code. Write access privileges to source code libraries within the version control software are restricted to user accounts accessible by authorized personnel. The version control system provides rollback capabilities and functionality to enforce segregation of duties. The ability to deploy application and infrastructure changes to production environments is restricted to authorized personnel.

DATA BACKUP AND RECOVERY

Backups occur on full, incremental or snapshot basis to meet needs of recovery time objective (RTO)/recovery point objective (RPO)/availability of product or service level need. Backup data is maintained in highly available storage. In the event that a backup job fails, the automated backup systems are configured to send an alert notification to operations personnel. Additionally, redundant architecture is in place to migrate business operations to alternate infrastructure in the event primary processing infrastructure becomes unavailable.

Backup data restoration tests are performed on at least an annual basis to help ensure that system components can be recovered from backup files. Restoration processes are primarily relying on the primary and secondary zone, when the primary zone becomes unavailable; promoting the secondary databases instances to primary to allow for failover of systems and data.

Trimble has implemented disaster recovery plans to mitigate the risk and impact of potential outages. On an annual basis, a disaster recovery test is conducted to help ensure the production environment can be recovered in the event of a disaster.

INCIDENT MANAGEMENT

Information Security incident management policies and procedures are in place to guide personnel throughout the security incident response process and include guidance on the following:

- Incident priority level definitions
- Responsibilities and procedures
- Reporting information security events and weaknesses
- Assessment and management of information security events
- Containment and resolution of information security incidents
- Collection and preservation of evidence
- Learning from information security incidents
- Incident coordination and communication strategy

A standard incident investigation form and ticketing system are utilized to document details surrounding each phase of the incident response process when security incidents are detected from initial discovery through resolution (e.g., identification, containment, eradication, recovery, and lessons learned). If the security incident requires a change to the system, the standard change control process is followed. Additionally, as part of the quarterly executive oversight board meetings, post-mortem reviews of security incidents are performed to analyze lessons learned and evaluate any areas for improvement in the incident response plan and recovery procedures.

SYSTEM MONITORING

Trimble's Product Development/IT Operations is responsible for assembling, operating, securing, and monitoring the performance of infrastructure resources, including the hardware, dependent services, and logical configurations of the production environment.

Several monitoring systems are in place to monitor the production environment. Performance monitoring tools are utilized to monitor the system up-time and performance, where administrators can review throughput, to support the operations team in making decisions to determine whether to add additional computing resources to improve availability and performance. Additionally, various security monitoring tools are implemented to monitor security events, identify vulnerabilities, and malicious code and alert security personnel. Compromised systems are quarantined, examined, and removed from the network until investigated and remediation is complete.

HUMAN RESOURCES

Trimble'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. Trimble's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities in this area are described below:

- New employees have a hub available showing Trimble policy and procedures and access to development resources.
- New employees are required to complete security awareness training upon hire and directed to Trimble Cybersecurity policies.
- Employee termination procedures are in place to guide the termination process.
- New employees have required courses in Business Ethics and Code of Conduct. The Business Ethics and Code of Conduct document is digitally acknowledged by all new employees.
- Employees are subject to background check procedures where applicable.

B. Principal Service Commitments and System Requirements

PRINCIPAL SERVICE COMMITMENTS

Trimble designs its processes and procedures related to e-Builder Enterprise to meet its business objectives. Those objectives are based on the service commitments that Trimble makes to user entities, the laws and regulations that govern the provisioning of e-Builder Enterprise, and the financial, operational, and compliance requirements that Trimble has established for the services. e-Builder Enterprise is subject to the relevant regulatory and industry information and data security requirements in which Trimble operates.

Security, availability, and confidentiality criteria commitments to user entities are documented and communicated in the Trimble general transaction terms, master terms and conditions, or other governing agreement; in any applicable supplemental terms or schedules, order forms, service level agreements, (SLA), or security addendums; and in any applicable policies or product documentation (collectively for a customer, a Customer Agreement). The principal service commitments are standardized and include the following:

- Trimble shall ensure infrastructure security by; hardened hosts with regular patching, vulnerability scanning tools, isolated virtual private clouds (VPCs), intrusion detection tools, static source code analysis, antivirus scanning tools, multi factor authentication, role-based access control, and network security groups;
- Trimble shall ensure that customer data in transit and at rest is encrypted, via methods such as transport layer security (TLS) and advanced encryption standard (AES);
- Trimble shall logically segregate each customer's data within the in-scope production application(s);
- Trimble shall engage an independent third party to conduct an annual penetration test of network, systems, or product hybrid on a prioritized risk basis;
- Trimble shall maintain a disaster recovery plan for e-Builder Enterprise covering disaster prevention and recovery;
- Trimble shall actively maintain data backups so that in the event of data corruption, inconsistency, or loss, e-Builder Enterprise can restore data as quickly as possible. Backups are stored securely in an immutable vault;
- Trimble shall monitor the e-Builder Enterprise system and subject to exclusions in the Service Level Agreement, maintain a 99.95% uptime level, measured monthly;
- Trimble shall dispose of customer data in accordance with applicable contract (from termination date of single tenant agreement or based upon schedule in a multi-tenant environment).

SYSTEM REQUIREMENTS

Trimble establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements.

Including the use of encryption technologies to protect system user data both at rest and in transit; the use of secure access controls to support the secure deliver of the services; the completion of vulnerability scanning and third-party penetration testing to identify and remediate security vulnerabilities; the implementation of operational procedures to guide internal personal in how to manage and respond to security incidents; and necessary system change management procedures to support the requisite authorization, documentation, testing, and approval of system changes.

Such requirements are communicated in Trimble's policies and procedures and system design documentation. 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, trained, and managed. 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 Trimble's e-Builder Enterprise.

The aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

MOSSADAMS