Proprietary & Confidential

Cityworks

SOC 3

Relevant to Security, Availability, Processing Integrity, 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 Cityworks (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 organizations.

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 Cityworks 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 Cityworks (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, Processing Integrity, 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 Cityworks" 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, Processing Integrity, 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 Cityworks".

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 Cityworks

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.

Cityworks, a Trimble company, is the leading geographical information system (GIS)-centric solution for public asset management, fully leveraging the power of Esri® ArcGIS® to help communities work smarter and better serve their residents.

Cityworks is a full-service company focused on the development of GIS-centric software applications. Cityworks is capable of providing complete implementation, integration, data conversion, and process review services, as well as re-engineering, training, and ongoing maintenance.

DESCRIPTION OF SERVICES PROVIDED

Cityworks Asset Management Solution (AMS) provides powerful tools for asset management, customer care, work management, and data analysis, while Cityworks Permits, Licensing, and Land (PLL) provides tools for tracking permits, licenses, planning applications, business and regulatory processes, engineering approvals, and code enforcement cases from beginning to end. Cityworks AMS and PLL are fully integrated, allowing GIS asset data, service requests, work orders, and inspections to be viewed in the same environment as GIS parcel data, permits, and licenses.

Cityworks is designed with applications that provide end users with optimized office or mobile experiences for their specific tasks:

- *Respond* – enables mobile service requests, work orders, inspections, and PLL case management on an interface optimized for tablets and other mobile devices. It is designed to support screen readers.
- *Mobile* – for iOS and Android are available for task-based usage when completing service requests, work orders, inspections, and PLL cases. While Respond requires a constant network connection, the mobile apps can be used when a network connection is not available.

- *Office for AMS* – enables full asset management functionality and is designed for a desktop environment.
- *Tablet for AMS* – enables full asset management functionality on mobile laptops and tablets.
- Other specialized apps have been developed including Admin, Contracts, Equipment Check Out, Operational Insights, OpX, Pavement Management, Performance Budgeting, Public Access, Storeroom, Style, Web Map Manager, and Workload.

Cityworks can be set up on-premises or as a managed deployment of Software as a Service (SaaS) with Cityworks Online (CWOL) hosted in a cloud environment. Cityworks utilizes cloud computing to access resources on the Cityworks platform, either on-premises or from CWOL coupled with ArcGIS Online.

Within the cloud, Cityworks generates data requests for the various Cityworks apps including Cityworks web forms and the Esri web map. Cityworks initiates data requests to feature services for resources available on ArcGIS Server or ArcGIS Online. A Representational State Transfer (REST) service is used to return a snapshot of the relevant GIS data to the Esri web map used by the Cityworks apps.

In addition to Cityworks apps, JavaScript Object Notation (JSON) web services APIs have been developed to allow integration with third-party applications to satisfy the needs of organizations. APIs are licensed separately and require configuration services.

WEB GIS-CENTRIC

Cityworks fully leverages an organization's investment in spatial data. It is designed on the premise that a GIS is a superior platform with which to organize, store, and manage asset data (both networked and non-networked infrastructure), including location, connectivity, detailed attributes, maintenance and case activities, and historical data. The following are characteristics of a Cityworks web GIS-centric solution:

- Utilizes the ArcGIS geodatabase and only the geodatabase as the authoritative asset database for assets dispersed or condensed (without variance), requiring no interface, no syncing, and no redundancy.
- Allows for maximum flexibility in designing the asset database for virtually any asset, dispersed, or condensed. Design and create it in the geodatabase and a GIS-centric software is configurable to it and not the other way around.
- Builds on the geodatabase as an "open" and interoperable database, inherently spatial, with well-known and understood data structure elements. The asset data cataloged and maintained by an organization in the geodatabase are not owned by the software vendor. The organization fully owns and controls their data.
- Relies solely on the ArcGIS feature services and database connection methods to update and access the authoritative asset data to assure data integrity, quality assurances, and constraints are maintained.
- Can access an ArcGIS web map without constraints. The applications are configurable to use the web map as is and do not require a vendor-specific web map.
- Supports single sign-on identity. An organization can choose ArcGIS Online or Portal for ArcGIS as their identity storehouse and the GIS-centric software and associated apps will support this with a single sign-on.

SYSTEM OF RECORD

Asset management can only be performed with an accurate asset inventory. Using embedded ArcGIS software, Cityworks brings together powerful technologies in an easy-to-use platform while performing both asset and maintenance management.

The inventory of capital assets and infrastructure is maintained in the geodatabase. By using the GIS tools available in Esri's ArcGIS and Cityworks, users have complete and comprehensive asset data creation, editing, management, and analysis tools at their disposal.

These GIS functions include:

- User-definable assets (features and related objects)
- User-definable field attributes
- Support of X, Y, Z coordinates
- Asset inventory directly linked to work management functions
- Assets managed within a visual hierarchy
- Assets directly linked to electronic documents
- Assets used in capital budgeting, planning, and rehabilitation
- Asset functions for changeout, readings, lookup, search, split, and table editor
- Asset barcodes

Cityworks PLL streamlines and automates permit, licensing, and land management processes while working with Cityworks AMS and Esri® GIS. This allows users to view permit, license, and land data in the same application as work orders, service requests, and GIS asset data. Cityworks PLL and AMS records can also be linked together, which allows organizations to capitalize on the major applications of the Cityworks platform.

Cityworks allows organizations to track permits, planning and development, engineering processes, business and regulatory processes, and code enforcement cases from inception to completion. GIS features can be tracked and may include parcels, street segments, intersections, addresses, or any other defined GIS feature classes.

Most permits and applications span an array of departments, including building, planning, and engineering. Cityworks enables agencies to share and access information easily and efficiently, streamline the application and review process across departments, and deliver substantially higher levels of customer service for contractors and citizens.

Cityworks tracks addresses, personnel, conditions, tasks, inspections, corrections, fees, and payments for any given permit type, which can include:

- Building
- Electrical
- Mechanical
- Plumbing
- Demolition
- Right-of-way

- Utility cut
- Fire and zoning

PLL streamlines and automates work processes, including:

- Application routing
- Plan review
- Fee calculation and collection
- Licensing renewals
- Workflow and tasks
- Inspections and scheduling
- Management signoff and tracking
- Reporting

Cityworks is designed with built-in apps (Office, Tablet, and others) and other apps built outside of the platform (including Respond, Public Access, mobile apps for iOS and Android, Admin, Style, and others), which provide the end user with an optimized office or mobile experience using various devices. Office contains full PLL functionality and is designed for an office environment, while Tablet enables PLL management on mobile laptops and tablets and utilizes a map that displays on a separate browser tab. Respond is a mobile application which utilizes a resizable map. Respond is also designed and developed to support use of screen readers.

2. Infrastructure and Software

The Cityworks is hosted within Amazon's Elastic Compute Cloud (EC2) and consists of a multi-tier virtualized architecture comprised of Windows-based application servers, Microsoft SQL (MS SQL) databases deployed using Amazon's Relational Database Service (RDS), storage and content delivery systems, and server and application monitoring and logging tools.

Trimble does not own or maintain hardware located in the AWS data centers, and operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure (e.g., physical infrastructure, geographical regions, availability zones, edge locations) and Trimble is responsible for securing the platform deployed in AWS (e.g., customer data, applications, identity access management, operating system and network firewall configuration, network traffic, server-side encryption).

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

Primary Infrastructure			
Production System	**Business Function Description**	**Operating System**	**Physical Location**
Cityworks	Primary application supporting Trimble's Cityworks services.	Windows	AWS
Managed Active Directory (AD)	Client / server protocol utilized to access the production environment (e.g., servers and databases) and manage directory information.	AWS	
Amazon RDS	Cloud-based managed database service supporting the MS SQL database.	AWS	
Amazon EC2	Provides virtualized infrastructure over EC2 virtual machines, elastic load balancer, and security groups.		
AWS Identity	Enables the ability to securely control access to AWS services and resources for users.		

3. People

The following groups are responsible for providing services related to Trimble's Cityworks:

- *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 Cityworks. 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 of Cityworks customer contracts, customer data is deleted after 30 days using automated purge scripts and manual disposal processes per Trimble's data disposal commitments.

Data Used and Supported by the System	Data Reporting	Data Reporting Classification
Company data, username and e mail address collected for authentication, authorization, and notification proposes.	Customers may access account related data via the Cityworks customer portals.	Confidential / Restricted
Application data, including GIS data, asset data, lease data, licensing data, planning data, and analytics.	Customers may access application data via the Cityworks customer portal and custom reports.	
Includes marketing details, user documentation, public announcements, etc.	Customers may access data via the company web-page.	Public

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 and legally permitted.

B. Principal Service Commitments and System Requirements

PRINCIPAL SERVICE COMMITMENTS

Trimble designs its processes and procedures related to Cityworks 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 Cityworks, and the financial, operational, and compliance requirements that Trimble has established for the services Cityworks is subject to the relevant regulatory and industry information and data security requirements in which Trimble operates.

Security, availability, processing integrity, and confidentiality 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 Cityworks covering disaster prevention and recovery;
- Trimble shall actively maintain data backups so that in the event of data corruption, inconsistency, or loss, Cityworks can restore data as quickly as possible. Backups are stored securely in an immutable vault;
- Trimble shall monitor the Cityworks system and subject to exclusions in the Service Level Agreement, maintain a 99.9% uptime level, measured monthly;
- Trimble shall perform input data validation that includes checks for out-of-range values, invalid characters in data fields, and missing or incomplete data; and
- 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 Cityworks.

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