LOCUS

System and Organization Controls 3 (SOC 3) Report – SOC for Service Organizations: Trust Services Criteria for General Use Report

Report on Locus Robotics' Description of its Autonomous Mobile Robotic Solution System Relevant to Security Throughout the Period February 1, 2023 to January 31, 2024

Bonadio & Co., LLP
Certified Public Accountants

REPORT ON LOCUS ROBOTICS' DESCRIPTION OF ITS AUTONOMOUS MOBILE ROBOTIC SOLUTION SYSTEM RELEVANT TO SECURITY THROUGHOUT THE PERIOD FEBRUARY 1, 2023 TO JANUARY 31, 2024

Table of Contents

SECTION ONE

Independent Service Auditor’s Report

Bonadio & Co., LLP
Certified Public Accountants

INDEPENDENT SERVICE AUDITOR’S REPORT

To: Management of Locus Robotics

Scope

We have examined Locus Robotics’ accompanying assertion titled "Assertion of the Management of Locus Robotics" (assertion) that the controls within Locus Robotics’ Autonomous Mobile Robotic Solution System (the System) were effective throughout the period February 1, 2023, to January 31, 2024, to provide reasonable assurance that Locus Robotics’ service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, (*With Revised Points of Focus—2022*) in AICPA *Trust Services Criteria* and included as Attachment A.

Service Organization's Responsibilities

Locus Robotics 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 Locus Robotics’ service commitments and system requirements were achieved. Locus Robotics has also provided the accompanying assertion about the effectiveness of controls within the System. When preparing its assertion, Locus Robotics 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 AICPA. 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.

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

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 Locus Robotics’ 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 Locus Robotics’ service commitments and system requirements based on the applicable trust services criteria

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

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 Locus Robotics’ Autonomous Mobile Robotic Solution System were effective throughout the period February 1, 2023, to January 31, 2024, to provide reasonable assurance that Locus Robotics’ service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Bonadio & Co., LLP

Amherst, New York
September 12, 2024

SECTION TWO

Assertion of the Management of Locus Robotics

LOCUS

ASSERTION OF THE MANAGEMENT OF LOCUS ROBOTICS

September 12, 2024

We are responsible for designing, implementing, operating, and maintaining effective controls within Locus Robotics' Autonomous Mobile Robotic Solution System (System) throughout the period February 1, 2023 to January 31, 2024, to provide reasonable assurance that Locus Robotics' service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100*, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022), in AICPA Trust Service Criteria*. Our description of the boundaries of the System is presented in attachment A 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 February 1, 2023 to January 31, 2024, to provide reasonable assurance that Locus Robotics' service commitments and system requirements were achieved based on the applicable trust services criteria. Locus Robotics' 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 attachment B.

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 February 1, 2023 to January 31, 2024, to provide reasonable assurance that Locus Robotics' service commitments and system requirements were achieved based on the applicable trust services criteria.

Fouad Khalil

Sr. Director, Enterprise Security, Risk and Compliance

Dustin Pederson

Chief Financial Officer

SECTION THREE

Management's Description of Locus Robotics' Autonomous Mobile Robotic Solution System Throughout the Period February 1, 2023 to January 31, 2024

INTRODUCTION

Company Background

Founded in 2015, Locus Robotics (“Locus” or “the Company”), develops and provides an intelligent Autonomous Mobile Robotic (AMR) Solution System (“the Locus Solution”, “AMR Solution”, “LocusBots”, or “the System”) used at warehouses and logistics centers around the world. The Locus Solution, classified as a Robots as a Service (RaaS) model, is an innovative, subscription-based program that makes it easy to add powerful AMR automation to a warehouse operation. Locus RaaS allows warehouse operators to shift capital expenses for automation to operational or labor expenses. The minimal initial investment means a simpler budget approval process and dramatically shortens the time of return on investment (ROI) from years to months.

Locus Robotics has two facilities, one located in Wilmington, Massachusetts, United States (US). The second corporate site is located in Amsterdam, Netherlands.

Services Provided

The Locus Solution is an innovative and award-winning multi-bot picking system that eliminates unproductive walking time to lower cycle times, improve workplace ergonomics, and process orders more rapidly. LocusBots work collaboratively with workforce members, transporting items to enhance throughput. Locus Robotics’ innovative AMRs make it easy for warehouse managers to optimize warehouse operations and respond to e-commerce volume growth and seasonal peaks while giving them control over labor costs.

The Locus Solution consists of the following:

- LocusBots: Autonomous, intelligent robots that eliminate unproductive walking time and ensure order accuracy.
- LocusServer: The integration point for warehouse management and warehouse control systems.
- LocusCloud: Cloud-based system updates for ensuring functionality and quality.
- LocusManager: An iOS and Android compatible app used to manage operations and reporting from anywhere.
- LocusApp: Mobile device app with integrated scanner for fluid pick and drop operation.

The Locus Solution integrates seamlessly with existing warehouse infrastructures, quickly configuring to warehouse operations. The solution seamlessly matches the workflow, routines, and processes, already in place.

The Locus Solution is used for order fulfillment across the following industries:

- Third-party logistics (3PL)
- Retail
- Healthcare
- Industrial

The Locus management dashboards and reporting tools give warehouse management unparalleled, real-time management metrics and insight to effectively monitor and optimize performance and throughput — across all floors. Customers will have actionable insight that can be used to stay focused on meeting daily, monthly, and annual company performance metrics, including, the following:

Services Provided (Continued)

- Monitor activity across levels in real-time.
- Track productivity rates, completed and unassigned work, pick pace, and more with active heat maps that give full visibility into operations.
- View all floors or each floor individually across one site and multiple, individual sites.

Locus Robotics software integrates with warehouse management and warehouse control systems (WMS systems). The Locus server's lightweight software is designed to integrate easily with existing WMS systems, infrastructure, and workflow without disrupting business operations.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

Infrastructure

The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization uses to provide the services.

Locus' infrastructure includes the following:

- Dell servers: used for operating system and platform for the Locus Solution and business applications.
- APC uninterruptible power supply (UPS): used as a battery backup power system.
- Meraki MX67 Security Appliance: used as a firewall and allows access to integrated systems. This appliance provides connectivity to the Locus support team.
- Meraki 210-24P Switch: provides connectivity from servers to wireless access points, power and connect wireless access point. Provides connectivity to the Meraki security appliance.
- NEMA 5-15R: used for power connection.
- Type C/E/F-R Plugs: used for power connection.

Locus Robotics uses G-Suite for documentation storage and as a workspace for editing policies, procedures, other processes relating to corporate infrastructure, and cloud hosting services. Locus Robotics reviews the G-Suite SOC2 Type 2 report on an annual basis. Any nonconformities identified in a subservice organization's reports are analyzed for relevance to Locus Robotics' organization and its users.

Locus Robotics uses Microsoft Office 365 for documentation editing, internal and external communication and other processes relating to customers, corporate infrastructure, and cloud hosting services. Locus Robotics reviews the Microsoft Office 365 SOC2 Type 2 report on an annual basis. Any nonconformities identified in a subservice organization's reports are analyzed for relevance to Locus Robotics' organization and its users.

Software

The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.

Locus Robotics maintains an inventory of open source and Software-as-a-Service (SaaS) software that are used to support the Locus Solution, business services, and corporate infrastructure.

To support its product and business operations, Locus Robotics incorporates the following software components. Please note that this is not a complete listing of applications used throughout Locus Robotics.

- Datto: used for data backup and restoration services.
- Cisco Meraki: used for network device management, including cloud virtual private network (VPN), firewall, and threat management.
- Sophos: used for antivirus.
- Rapid7: used for vulnerability monitoring.
- Salesforce: used for customer relationship management software.
- GitHub: used for software development and version control.

People

The personnel involved in the governance, management, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).

The organizational structure includes a separation of administrative, technology, finance, customer success, marketing, compliance, and engineering. The overall Company supports the framework for an effective control environment, and is comprised of the following functional areas:

Executive Management: provides strategic direction and leadership for Locus Robotics. Executive Management oversees and is ultimately responsible for all aspects of service delivery (including business development, marketing, and quality assurance), and all corporate services functions including but not limited to operations, finance, engineering, internal information technology (IT) support, human resources, legal, and customer success.

People Operations: responsible for managing all functions related to recruiting and hiring, benefits, employee relations, performance management, resource management, and career assistance. The Human Resources team partners proactively with Executive Management and business units to ensure that all initiatives are appropriately aligned with Locus' mission, vision, and values. Locus Robotics is committed to equal opportunity of employment and all employment decisions are based on merit, qualifications, and abilities.

Internal IT Support team: provides IT services to all internal employees. The team has overall responsibility and accountability for the enterprise computing environment, including corporate software, corporate applications, operating system issues, software license requests, and network connectivity. IT personnel work closely with the end users of other functional areas to develop and implement guidelines and procedures to ensure that the enterprise computing environment is functioning both efficiently and effectively with regard to Locus Robotics business objectives and requirements.

Information Security team: responsible for incident response, disaster recovery, data backup and restoration.

Enterprise Security, Risk and Compliance team: responsible for company security and governance, management, and execution and of all non-financial audit activity, company-wide risk management program (including vulnerability management), vendor risk management and security awareness and training.

Marketing: responsible for the strategic deployment of the Locus Robotics brand and for building awareness through multiple media channels including the internet, public relations, advertising, and industry associations.

Finance: primarily responsible for the accuracy of financial reporting. Finance personnel are responsible for corporate treasury matters, invoicing and payment applications, payroll, and procurement processing. Finance provides support and assistance as needed to client services.

Data

The types of data used by the system, such as transaction streams, files, databases, tables, and other output used or processed by the system.

Locus Robotics stores limited types of customer and company data in the Locus Solution. Sensitive data is protected through secure encryption methodologies during transit. The Locus Solution does not create, collect, store, process, transmit, or use customer data.

Data (Continued)

The principal types of data that the Locus Solution creates, collects, processes, transmits or uses is limited to the following customer information:

- Username
- Business email
- Username for warehouse management

Additionally, the Company collects the following as part of third-party contractual obligations which may contain sensitive data:

- Non-Disclosure Agreements (NDAs)
- User Agreement for Access to Locus Robotics Corporate Information Systems
- Data Protection Agreements (DPAs)

Processes and Procedures

The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information are prepared.

Locus Robotics has a developed Security Review Board (SRB) that is responsible for the design and oversight of security and privacy initiatives. The SRB consists of individuals from the following areas: IT, Security, Privacy, Compliance, Finance and Human Resources. The Security Policy framework describes the procedures followed to ensure the performance of consistent processes over the security, availability, confidentiality, and operation of the Locus Solution and corporate infrastructure. All IT and Security policies are reviewed on an annual basis, and on an as needed basis.

All employees are expected to adhere to the Locus Robotics Security Policy framework as acknowledged during the new hire onboarding process and during annual security awareness training. The Security Policy framework includes procedures that provide guidance on the consistent performance of controls and processes necessary to meet service commitments and system requirements.

Locus Robtics has the following written Policies and procedure:

- Information Security Policy
- Acceptable Use Policy
- BYOD Policy
- Data Protection and Governance Policy
- Data Retention Policy
- Data Classification and Handling Standard
- Electronic Media Protection Standard
- Event Logging and Monitoring Standard
- Identity & Access Management Standard
- Personnel Security Standard

Processes and Procedures (Continued)

- Physical and Environmental Standard
- Security Awareness Training Standard
- Visitor Management Standard
- Document Control and Management Standard
- Organizational Communication Policy
- Standard and Procedure Exception Policy
- Sanctions Policy

ATTACHMENT A

AICPA Trust Services Categories and Criteria

AICPA TRUST SERVICES CATEGORIES AND CRITERIA

This attachment includes the Trust Services Criteria (TSC) included in the scope of the engagement relevant to the security category set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria*.

CC1.0 – Common Criteria Related to Control Environment	
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
CC2.0 – Common Criteria Related to Information and Communication	
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.
CC3.0 – Common Criteria Related to Risk Assessment	
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.
CC4.0 – Common Criteria Related to Monitoring Activities	
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
CC4.2	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.
CC5.0 – Common Criteria Related to Control Activities	
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
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.

CC6.0 – Common Criteria Related to Logical and Physical Access Controls	
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity’s objectives.
CC6.4	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.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.
CC7.0 – Common Criteria Related to System Operations	
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.
CC8.0 – Common Criteria Related to 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.
CC9.0 – Common Criteria Related to Risk Mitigation	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.

ATTACHMENT B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Locus designs its processes and procedures related to the System to meet its objectives for its services. Those objectives are based on the service commitments that Locus makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that Locus has established for the services. Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Formalized policies and procedures for all internal control requirements.
- System logging and monitoring.
- Patch and change management.
- Vulnerability remediation.
- Antivirus (AV) software.
- Identity and access (logical and physical) management.
- Multi-Factor authentication (MFA).
- Secured remote access.
- Firewall management.
- Backup management.
- Incident management.
- Vendor management.
- Password management.
- Encryption standards.
- Hiring practices and employee training.

Locus establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Locus system policies and procedures, system design documentation, and 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 Locus Robotics' AMR Solution.