
# Datto, Inc.

## SOC 3

Independent Service Auditor's Report on Management's Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality

November 1, 2023 – October 31, 2024


200 Second Avenue South, Suite 478
St. Petersburg, FL 33701

200 Second Avenue South, Suite 478
St. Petersburg, FL 33701
www.ascendaudit.com

# INDEPENDENT SERVICE AUDITOR'S REPORT

The Management of Kaseya Holdings, Inc. and its affiliate Datto, Inc.
701 Brickell Avenue, Suite 400
Miami, FL 33131

***Scope***

We have examined Kaseya Holdings, Inc. and its affiliate Datto, Inc.'s ("Datto", "Datto, Inc.", or "the Company") description of controls for its Information Technology General Controls (ITGC) system and related transactions throughout the period November 1, 2023 through October 31, 2024, based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report *(With Revised Implementation Guidance – 2022)*(AICPA, *Description Criteria*), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 1, 2023 through October 31, 2024, to provide reasonable assurance that Datto's service commitments and system requirements were achieved based on the trust service criteria for security, availability, and confidentiality 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.*

***Subservice Organizations***

Datto and its business units (i.e., products) utilize the following subservice organizations to provide services and application delivery:

- Bamboo HR for Human Resources information system (HRIS)
- Atlassian for source code repository, version control, and project management
- Salesforce for customer relationship management and support ticketing
- Redcentric, Noris Networks, Tierpoint, Aligned Energy, eStruxture, Equinix, Cyxtera, Aptum Technologies, CoreSite, Verne Global, NextDC, and GlobalConnect for data center services
- Amazon Web Services (AWS) and Microsoft Azure for infrastructure-as-a-service and cloud computing

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Datto, to achieve Datto's service commitments and system requirements based on the applicable trust services criterion of security, availability, and confidentiality. The description presents Datto's controls, the applicable trust services criteria of security, availability, and confidentiality and the types of complementary subservice organization controls assumed in the design of Datto's controls. The description does not disclose the actual controls at the subservice organizations.

Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls. Our examination did not extend to controls at the service organizations listed.

***Datto, Inc.'s Responsibilities***

Datto 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 Datto's service commitments and

system requirements were achieved. In Section II, Datto has provided its assertion titled "Assertion of Datto, Inc. Service Organization Management" about the description and the suitability of design and operating effectiveness of controls stated therein. Datto is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

***Ascend Audit & Advisory's Responsibilities***

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

***Inherent Limitations***

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. 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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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 policies or procedures may deteriorate.

***Opinion***

In our opinion, Datto's controls over the system were effective throughout the period November 1, 2023 through October 31, 2024, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.

*Ascend Audit & Advisory*

St. Petersburg, FL

December 5, 2024

## ASSERTION OF DATTO, INC. SERVICE ORGANIZATION MANAGEMENT

We have prepared the description of Datto, Inc.'s Information Technology General Controls System ("system" or "the system") throughout the period November 1, 2023 through October 31, 2024, ("the description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization System in a SOC 2 Report (With Revised Implementation Guidance – 2022)*(AICPA, *Description Criteria*). The description is intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with Datto Service Organization's system, particularly information about system controls that Datto has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*(AICPA *Trust Services Criteria*).

Datto and its business units (i.e., products) utilize the following subservice organizations to provide services and application delivery:

- Bamboo HR for Human Resources information system (HRIS)
- Atlassian for source code repository, version control, and project management
- Salesforce for customer relationship management and support ticketing
- Redcentric, Noris Networks, Tierpoint, Aligned Energy, eStruxture, Equinix, Cyxtera, Aptum Technologies, CoreSite, Verne Global, NextDC, and GlobalConnect for data center services
- Amazon Web Services (AWS) and Microsoft Azure for infrastructure-as-a-service and cloud computing

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Datto, to achieve Datto's service commitments and system requirements based on the applicable trust services criterion of security, availability, and confidentiality. The description presents Datto's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Datto's controls. The description does not disclose the actual controls at the subservice organizations. The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Datto, to achieve Datto's service commitments and system requirements based on the applicable trust services criteria. The description presents Datto's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Datto's controls.

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

a. The description presents Datto's system that was designed and implemented throughout the period of November 1, 2023 to October 31, 2024, in accordance with the description criteria.

   i. The description contains the following information:

      (1) The types of services provided.

      (2) The components of the system used to provide the services, which are the following:

      - *Infrastructure* – The physical and hardware components of a system (facilities, equipment, and networks).
      - *Software* – The programs and operating software of a system (systems, applications, and utilities).
      - *People* – The personnel involved in the operation and use of a system (developers, operators, users, and managers).
      - *Procedures* – The automated and manual procedures involved in the operation of a system.

- *Data* – The information used and supported by a system (transaction streams, files, databases, and tables).

(3) The boundaries or aspects of the system covered by the description.

(4) How the system captures and addresses significant events and conditions.

(5) The process used to prepare and deliver reports and other information to user entities and other parties.

(6) If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization and other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

(7) For each category being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the Company's system.

(8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the Company, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria; and for privacy, the types of activities that the subservice organization would need to perform to comply with privacy commitments.

(9) Any applicable trust services criteria that are not addressed by a control at the Company or a subservice organization and the reasons, therefore.

(10) Other aspects of the Company's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

(11) Relevant details of changes to the Company's system during the period covered by the description.

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

b. The controls stated in the description were suitably designed throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that Datto's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Datto's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that Datto's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Datto's controls operated effectively throughout that period.

# DESCRIPTION OF DATTO, INC.'S INFORMATION TECHNOLOGY GENERAL CONTROLS SYSTEM

## Company Overview

Datto, now a Kaseya company, is a leading global provider of security and cloud-based software solutions purpose-built for Managed Service Providers (MSPs), Datto believes there is no limit to what small and medium businesses (SMBs) can achieve with the right technology. Datto's proven Unified Continuity, Networking, Endpoint Management, and Business Management solutions drive cyber resilience, efficiency, and growth for MSPs. Delivered via an integrated platform, Datto's solutions like DBMA, BCDR, BitDam, Cloud Continuity for PC, Kaseya Quote Manager, Networking, RMM, SaaS Protection, Workplace, and PSA Autotask help its global ecosystem of MSP partners serve over one million businesses around the world. From proactive dynamic detection and prevention to fast, flexible recovery from cyber incidents, Datto's solutions defend against costly downtime and data loss in servers, virtual machines, cloud applications, or anywhere data resides. Datto has won awards for its rapid growth, product excellence, superior technical support, and for fostering an outstanding workplace. Datto's corporate headquarters is in Miami, FL, with offices in North America, EMEA, and APAC regions.

## Products and Services Overview

### Autotask PSA

Datto's cloud-based IT business management tool, Autotask PSA, is a robust IT Business Management solution that combines service desk, contracts, SLAs, projects, CRM, time, and billing. The Autotask PSA platform allows technology providers to provide better, more efficient service at peak profitability – and gives them a real-time view of critical business information on a single pane of glass. Autotask PSA tool provides the following features:

- CRM (Customer Relationship Management)
- Ticketing
- Project Management
- Customizable Dashboards
- Time tracking and billing
- LiveMobile App
- Invoicing
- Reporting

### Backupify (SaaS Protection)

Datto's Backupify/SaaS Protection application is a cloud-based backup and recovery solution for application data including Google Apps, and Office 365. Through the report, the SaaS Protection products and services may be referred to as "SaaS Protection" and/or "Backupify." "Backupify" is an alternate trade name that Datto uses for the SaaS Protection product and services. SaaS Protection solution include the following services:

- Automated Continuous Backup
- Flexible Retention
- Admin Audit Log
- Ransomware Protection
- Recover Quickly
- Easy Export
- Predictable Billing
- Cross-user Restore
- Daily Backup Success Report

As more services and organizations migrate from local hard drives to the always-on cloud, SaaS Protection is pioneering the protections and processes that will keep clients' irreplaceable online information safe, available, and under their control. The SaaS Protection service is an easy-to-use solution that enables data backups from multiple SaaS platforms through a single user interface; backups run on demand or on a customer-defined schedule. Backup data is maintained on the Datto Cloud platform, separate from customers' SaaS providers' repositories.

**BCDR**

Datto's Business Continuity & Disaster Recovery (BCDR) solution has been used by companies nationwide. Datto's cloud-based storage and data recovery services and their related controls are key differentiators in providing and maintaining a secure cloud-based storage and recovery solution to its customers. The solution consists of a hybrid cloud backup solution, which indicates a local appliance that takes backups of a protected machine and a set of replicated cloud backups, stored in the Datto Cloud, providing MSP's and their clients with:

- Ransomware Protection
- Fast Recovery
- Immutable Backup
- Enhanced 1-Click Disaster Recovery

**BitDam**

BitDam is a SaaS platform making enterprise communications safe to click. BitDam cyber security solutions protect enterprise communications from advanced content-borne threats. BitDam's mission is to prevent cyber-attacks on hardware and logical exploits, N-Day, Phishing, Ransomware and Zero-Day attacks from within the communication stream. BitDam's cloud-native architecture provides seamless application protection with real-time threat intelligence, easy management via a centralized portal, and specialized defenses against Business Email Compromise (BEC) attacks.

**Cloud Continuity**

Datto's Cloud Continuity (CC) solution has been used by companies nationwide. Datto's cloud-based storage and data recovery services and their related controls are key differentiators in providing and maintaining a secure cloud-based storage and recovery solution to its customers.

Cloud continuity has numerous features to help users easily and securely store and access their data.

- Streamline Recovery – easily restore individual files and folders, rollback from ransomware, or restore the entire PC image to a new device.

- Screenshot Verification – ensure backups are verified for reliable recovery with integrity checks that validate every backup and provide an alert if there are issues.

- RMM Integration – save time and perform mass deployments easily and efficiently by utilizing RMM alongside Cloud Continuity.

- Enhanced 1-Click Disaster Recovery: Simplifies the disaster recovery process, allowing for quick and efficient recovery with a single click.

- Cloud Deletion Defense: Provides end-to-end protection and ensures that deleted data can be recovered.

**DWP**

Datto's Workplace Cloud System, formally known as DWP, offers the following important benefits to its business customers:

- Mobile Collaboration – Flexible access to the most up-to-the-minute business content empowers employees to make better and more informed decisions to help drive the business forward faster. Datto Workplace facilitates optimized content delivery and rendering of any type of business content from users' mobile devices. The Datto Workplace One-App concept and team-based sharing helps ensure that corporate content stays in the right hands.

- Enterprise-Grade Security – Critical business content needs to be secured. Policy-based control of content, seats, and devices is paramount to maintain corporate security. Datto Workplace is an enterprise-grade service with stringent levels of security. With geo-redundant data centers in the U.S., EU, Canada, and Australia, Datto adheres to local regulations for data in all major regions of the world.

- Purpose-Built for Business and Users – Datto Workplace is flexible and open, designed for the specific needs of IT departments in larger companies where control and management of cloud services is critical to business operations. With policy-based control of content, seats, and devices, providing secure access for employees and partners to work together on projects with the proper controls is a top priority.

- Advanced Management and Reporting – Datto Workplace offers sophisticated admin controls, customizable user and group configurations, and policy controls to ensure the right users have the proper access. Integration with Active Directory and Single Sign-On (SSO) tools simplifies user management and enhances security. Multi-tenant management allows for easy deployment and monitoring across multiple clients from a single cloud management portal.

- Ransomware Detection and Management – Datto Workplace actively scans files as they upload. If a threat is detected, alert notifications are triggered, and files are immediately quarantined to prevent the threat from spreading. Reverting files to their last good state is done in just a few clicks.

**RMM**

Datto RMM is a cloud based remote monitoring and management platform that enables customers to administer their clients efficiently and effectively at scale. The scope of this audit is to review the Security, Availability and Confidentiality Trust Services Principles for the Datto RMM service offering. While the vast majority of the service components making up regional clouds are identical, the focus of this audit will be centered on the services and systems supporting the U.S. (United States) and Canada Datto RMM environment.

Partners and end users deploy a software agent to machines they wish to protect and manage through the platform. These agents communicate back to the RMM cloud data center, where services enable remote access, performance monitoring, software management, and a long list of other functionalities once the agent is enrolled. RMM solutions include the following:

- Flexible, Automated Patch Management
- Automation and Scripting
- Real-Time Monitoring
- Network Topology Mapping
- Ransomware Detection
- Flexible Reports and Dashboards
- Advanced Software Management

- Seamless RMM PSA Integration
- Rapid Remote Access & Support

**Datto Networking**

Datto Networking enables MSPs to efficiently deploy a suite of comprehensive managed networking services. Fully managed in the cloud, Datto Networking simplifies network deployments with smarter devices, always connected networking and fully integrated failover enabling MSPs to cost effectively support at a competitive recurring revenue price point. Key offerings include the following:

- Network Appliance
- Networking Switches
- Networking Wi-Fi
- Datto Secure Edge
- Datto Network Manager

**Azure Protect**

Datto's cloud-based storage and data recovery services and their related controls are key differentiators in providing and maintaining a secure cloud-based storage and recovery solution to its customers. Datto Continuity for Microsoft Azure has numerous features to help users easily and securely store and access their data:

- Efficient deployment
- Hybrid data protection
- Multi-cloud replication
- End-to-end protection
- Cloud Deletion Defense
- Virtualization to the Datto Cloud
- Automatic boot verification of backups

**Datto Commerce (Kaseya Quote Manager)**

The solution automates the processes of product selection, quoting, and sales of IT products and services for MSP clients. Its SaaS platform includes an efficient selling or quoting feature and a simple user interface to streamline sales, resulting in significant time savings and efficiency for MSPs. The well-designed UX creates easy-to-edit proposals for MSPs in minutes or less. The simplified UI (User Interface) makes product search simple for SMB (Server Message Block) clients to receive access, shop, and purchase from approved devices catalogued by MSPs, improving the customer experience. Key features include:

- Simple Navigation
- Quick and Effective Quoting and Selling
- Purchasing Optimizer
- Integration with PSA Systems
- Industry-Best Product Information
- Advanced Reporting and Analytics

## System Description

### Service Commitment and System Requirements

Datto's security, availability, and confidentiality commitments to customers are documented and communicated to customers in the Datto Master Services Agreement and the description of service documents published on the customer facing Web site. The principal security, availability, and confidentiality commitments include, but are not limited to:

- Maintaining appropriate administrative, physical, and technical safeguards to protect the security and availability of the Datto Products platform and the customer data in accordance with Datto's security requirements.
- Performing annual third party security and compliance audits of the environment, including, but not limited to, reporting on System and Organization Controls (SOC) relevant to security, availability, and confidentiality.
- Using formal HR (Human Resources) processes, including background checks, code of conduct and company policy acknowledgements, security awareness training, disciplinary processes, and annual performance reviews.
- Accessing management procedures for the request, approval, provisioning, review, and revocation of Datto personnel with access to production systems.
- Preventing malware from being introduced to production systems.
- Monitoring the production environment for vulnerabilities and malicious traffic.
- Using industry standard secure encryption methods to protect customer data at rest and in transit.
- Transmitting unique login credentials and customer data via encrypted connections.
- Maintaining a disaster recovery and business continuity plan to ensure availability of information following an interruption or failure of critical business processes.
- Maintaining and adhering to a formal incident management process, including security incident escalation procedures.
- Maintaining confidentiality of customer data and notifying customers in the event of a data breach.
- Identifying, classifying, and properly disposing of confidential data when retention periods are reached and/or upon notification of customer account cancellations.

### Components of the System

Datto's control environment (the "System") is comprised of the following components:

- Infrastructure (work from home locations, workstations, and cloud hosting)
- Software (cloud-based solutions and applications)
- People (employees, consultants, and users)
- Policies and Procedures (manual and automated)
- Data (transaction streams, files, databases and tables)

The Company's environment and platform are designed and managed with security, availability, and confidentiality in mind. The following sections provide a brief description of the five components comprising the System.

***Infrastructure***

The Datto Information Technology (IT) environment includes global data centers located in Massachusetts, Virginia, New Jersey, Colorado, Georgia, and Florida in the United States; and data centers in Ireland, United Kingdom, Germany, Australia, and Canada. Housed within these data centers are the supporting operating system platforms (Windows and Linux), networking components (firewalls, routers, switches), and data storage devices. Datto also utilizes cloud technologies from Amazon Web Services (AWS) and Microsoft Azure across global regions.

Corporate infrastructure is segregated and managed by the Kaseya Global IT Team on behalf of Datto. Development (Managed by Product Teams), Staging, and Production infrastructure is segregated and managed by the Infrastructure Operations Team.

***Software***

Software utilized by IT and Operations to manage and support the Datto IT environment includes:

- Virtualization Hypervisor
- Backup Management
- Remote Management and System Monitoring
- Network Monitoring
- Security Monitoring
- Change Management
- Help Desk Support

***People***

IT and Operations personnel provide the following core support services for the Datto IT Environment components listed above:

- Systems and Network Monitoring
- Security
- Database Administration
- Backup Operations
- Network Management
- Application Change Management
- Infrastructure Change Management

To provide these services, IT and Operations operate in functional areas: Network Management Services, Systems Management Services, Development, and Support. Below is a brief description of each of these functional areas:

- Network Management Services: This functional area deals with Fault, Configuration, Accounting, Performance, and Security (FCAPS) - It keeps the network up and running smoothly and monitors the network to spot problems as soon as possible, ideally before users are affected, keeping track of resources on the network, and how they are assigned.
- Systems Management Services: This functional area deals with server systems operations and maintenance to support global operations.
- Development: This functional area supports new product developments, client customizations, new releases, and updates for client software.
- Support: This functional area deals with maintenance, repairs, and upgrades attending to user support.

***Corporate Policies and Procedures***

Datto has formalized policies and procedures which are as follows:

- Asset Management Procedures
- Business Continuity and Disaster Recovery Plan
- Change Management Policy
- Code of Conduct
- Confidentiality Agreement
- Electronic Data Destruction Policy
- Employee Handbook
- Enterprise Encryption Guidelines in Information Security Policy
- Hiring and Termination Checklist
- Incident Response Plan
- Information Security Policy
- Offboarding Process
- Onboarding Process
- Patch Management Procedures
- Vendor Risk Management Policy
- Vulnerability Disclosure Policy
- Backup & Restore Policy and Procedure
- Kaseya Disaster Recovery Plan
- Data Classification Matrix & Handling Guide
- Laptop Security Policy
- Acceptable Use Policy
- Environmental Protection Policy
- Password Policy
- Physical Access Security Policy
- Records Retention Policy
- Software Development Life Cycle Policy
- Vendor Management Program
- Corporate IT MFA (Multi Factor Authentication) Admin Policy
- Work-From-Home Resource Center

***Data***

Data management common to multiple products includes:

- Datto stores several types of customer and company data in the cloud solution platform. Sensitive data is protected through secure encryption methodologies.

- Datto retains confidential information to meet legal and regulatory requirements and confidentiality commitments. Requirements for data retention are specified contractually via the customer-specific Datto Terms and Privacy Policy.

- Sensitive data is secured any time it must be transmitted or received via open, public networks. Connectivity to the Datto Cloud utilizes OpenSSH with AES-256-bit encryption to protect backed-up data in transit.
- Encryption practices protect information involved in the Datto Continuity for Microsoft Azure solution from incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, and replay.

***Disclosures***

Informed by Management there were no material incidents reported during the period under review.