Datto, Inc.

Workplace and File Protection (DWP)

SOC 3

Independent Service Auditor's Report on Management's Description of a Service Organization's System Relevant to Security and Availability

November 1, 2021 to October 31, 2022

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 Datto, Inc.
701 Brickell Avenue, Suite 400
Miami, FL 33131

Scope

We have examined Datto, Inc.'s ("Datto", or "the Company") accompanying assertion titled "Assertion of Datto, Inc. Service Organization Management" (assertion) that the controls within Datto's Workplace and File Protection system (system) were effective throughout the period November 1, 2021 through October 31, 2022, to provide reasonable assurance that Datto's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability 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*.

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. Datto has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Datto 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.

Ascend Audit & Advisory's Responsibilities

Our responsibility is to express an opinion, based on our examination, on 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 Datto'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 Datto's 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 Datto's Workplace and File Protection system were effective throughout the period November 1, 2021, to October 31, 2022, to provide reasonable assurance that Datto's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Ascend Audit & Advisory

ASCEND
AUDIT & ADVISORY

St. Petersburg, FL

December 29, 2022

ASSERTION OF DATTO, INC. SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Datto Service Organization's (Datto's) Workplace and File Protection system (system) throughout the period November 1, 2021, to October 31, 2022, to provide reasonable assurance that Datto's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (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*. Our description of the boundaries of the system is presented in the 'Description of Datto, Inc.'s Workplace and File Protection System' 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 November 1, 2021, to October 31, 2022, to provide reasonable assurance that Datto's service commitments and system requirements were achieved based on the applicable trust services criteria. Datto '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 'Principal Service Commitments and System Requirements'.

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 November 1, 2021, to October 31, 2022, to provide reasonable assurance that Datto's service commitments and system requirements were achieved based on the applicable trust services criteria.

By: /S/ Jason Manar

Jason Manar
Chief Information Security Officer

December 29, 2022

DESCRIPTION OF DATTO, INC.'S WORKPLACE AND FILE PROTECTION SYSTEM

Company Overview

Datto, founded in 2007, and headquartered in Miami, Florida, is a leading provider of enterprise-level technology to small and medium sized businesses. The product was renamed 'Datto Workplace and Datto File Protection' (Datto Workplace Cloud System or DWP) and maintains its functionality and purpose. The services are provided on a subscription basis to its customers, which embodies cloud-based services for managing teams and their documents online, Datto's client software tools for syncing with and integrating documents into desktop and laptop computers, and Datto's mobile apps for working with and sharing documents from smartphones and tablet devices.

On June 23, 2022, Kaseya, LLC purchased Datto becoming the parent company of Datto under the name Kaseya, Inc. This combination of companies brought the best of both enterprises under one umbrella with the creation of IT Complete by providing better opportunities and an industry leading set of solutions to customers.

Services Overview

Datto's Workplace Cloud System offers the following important benefits to its business customers:

- **Mobile Collaboration** – Anywhere, anytime 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 on any type of business content from users preferred mobile devices. The Datto Workplace One-App concept and team-based sharing ensures 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 that has 99.986% uptime 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.

Datto's Workplace Cloud System is based on the following key capabilities:

- **Secure File Sharing** – Enables management of a company's business content with granular share permission controls and user roles, team and public link customization, and full audit trails.

- **Teamwork** – Enables easy sharing and collaboration on business content and projects within a company's internal team members and external connections, like clients, partners, or suppliers.

- **Mobile Productivity** – Transforms mobile devices into productivity tools – allows users to access, create, edit, annotate, and share business content from anywhere with a mobile device in one seamless and integrated application.

- **Permissions and Control** – From a dedicated Admin Interface, enables and manages entire teams of users and sets access and permission levels at an individual and group level.

- **Projects** – Centralizes an entire organization's business content into functional projects and makes users more productive with intuitive version management and a formal and organized file sharing structure.

System Description

Principal Service Commitments and System Requirements

Datto's Security and Availability commitments to customers are documented and communicated to customers in the Master Services Agreement and the description of service documents published on the customer-facing website. The principal Security and Availability commitments include, but are not limited to:

- Maintain appropriate administrative, physical, and technical safeguards to protect the security and availability of the Datto Workplace and File Protection platform and the customer data in accordance with Datto's security requirements.
- Perform annual third-party security and compliance audits of the environment, including, but not limited to:
    - Reporting on Controls at a Service Organization Relevant to Security and Availability.
    - International Organization for Standardization (ISO) 27001:2013 certification reviews.
- Use formal HR processes, including background checks, code of conduct and company policy acknowledgements, security awareness training, disciplinary processes, and annual performance reviews.
- Follow formal access management procedures for the request, approval, provisioning, review, and revocation of Datto personnel with access to any production systems.
- Prevent malware from being introduced to production systems.
- Continuously monitor the production environment for vulnerabilities and malicious traffic.
- Use industry-standard secure encryption methods to protect customer data at rest and in transit.
- Transmit unique login credentials and customer data via encrypted connections.
- Maintain a disaster recovery and business continuity plan to ensure availability of information following an interruption or failure of critical business processes.
- Maintain and adhere to a formal incident management process, including security incident escalation procedures.
- Maintain confidentiality of customer data and notify customers in the event of a data breach.
- Identify, classify, and properly dispose of confidential data when retention period is reached and/or upon notification of customer account cancellation.

Datto establishes system and operational requirements that support the achievement of the principal service commitments, applicable laws and regulations, and other system requirements. These requirements are communicated in Datto's policies and procedures, system design documentation, and/or in customer contracts. Information Security policies define how systems and data are protected. These policies are updated as appropriate based on evolving technologies, changes to the security threat landscape, and changes to industry standards, provided any updates do not materially reduce the service commitments or overall service provided to customers as described in the customer contracts.

Datto regularly reviews the security, availability, and performance metrics to ensure these commitments are met. If material changes occur that reduce the level of security and availability commitments within the agreement, Datto will notify the customer via the Datto website or directly via email.

Components of the System

The System is comprised of the following components:

- Infrastructure (facilities, equipment, and networks)
- Software (systems, applications, and utilities)
- Data (transaction streams, files, databases, and tables)
- People (developers, operators, users, and managers)
- Procedures (automated and manual)

Infrastructure

The overall Datto Workplace infrastructure consists of multiple and geo-redundant data centers (composed of modules called data center cells), and Datto components installed on users' computers where users' files reside and, optionally, on users' mobile devices such as smartphones and tablets.

This architecture has proven to be highly modular and scalable from a storage and capacity perspective and fully automated from a control and management perspective. Due to this modularity, Datto can add significant new data center capacity in less than a few weeks, which is required for scalability and agility in a rapidly evolving Software as a Service (SaaS) business model. As a result, Datto has been able to employ a near-real-time systems development methodology that supports business objectives and customer requirements that drive all aspects of scaling and managing Datto's Network Operations and IT systems.

All locations are carrier-grade data center hosting facilities that are operated by their respective owners. These facilities are audited by independent service auditors for SOC 2, CSAE 3416, and ISAE 3402 controls for operating effectiveness as required. Each facility houses servers for dozens of major telecommunications, media, technology, entertainment, financial services, web services, and other companies in addition to hosting geo-redundant instances of Datto's Workplace Cloud System.

Data Center Cells

The fundamental component of the Datto Workplace architecture is the data center cell. Several data center cells are operated simultaneously and internal replication of data from cell to cell protects against failure of any one cell. Each cell consists of the following server components:

- Management Server. The Management server is the main management component in the cell and handles several key functions:
    - Secure login access
    - PXE boot images and server configurations
    - Internal DNS server
    - SMTP gateway

- Nagios Surveillance Server. The Nagios system keeps track of all servers running in the Datto data centers. Each server records what version of software is loaded and running. Nagios monitors multiple operational parameters every 60 seconds and reports any consistent problems to Datto Network Operations staff.

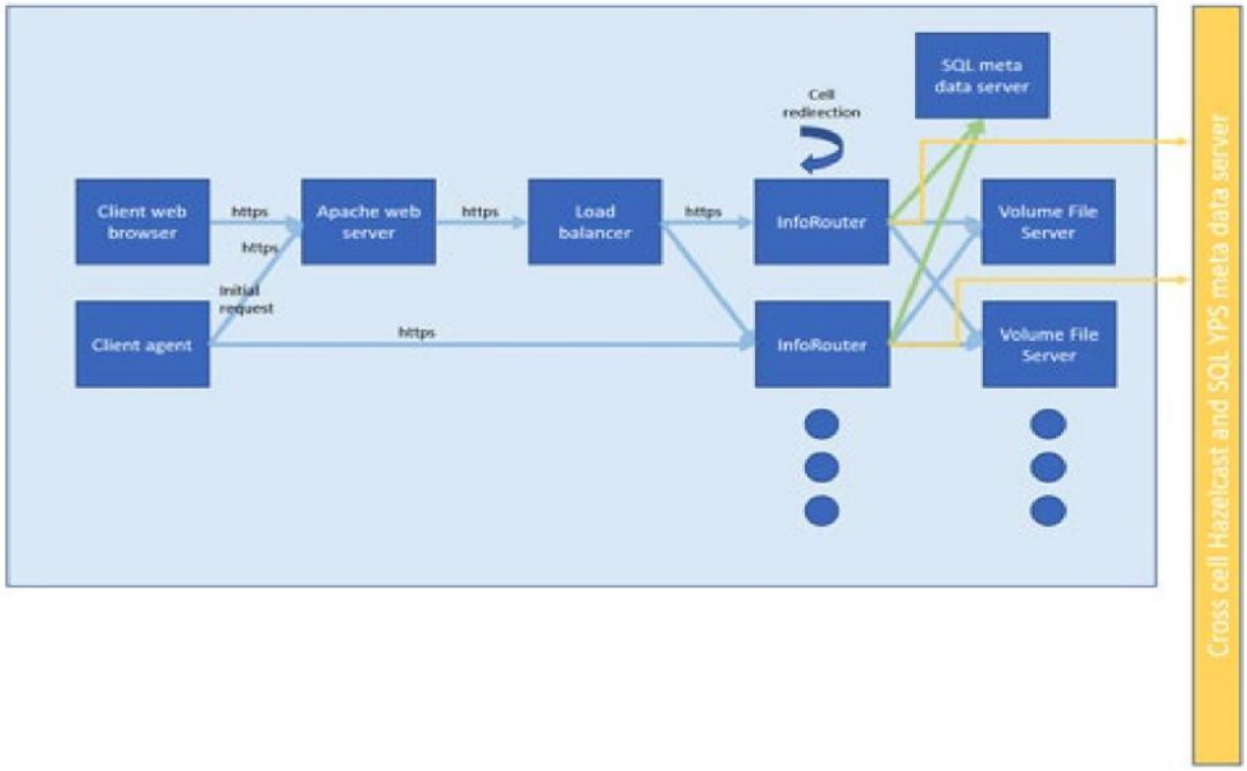
- Load Balance Server. The Load Balance server distributes the full external load on the data center cell into multiple channels through the entire service so there is no overload at internal points.

- Application Servers. The application servers are where the Datto application software runs. Each application server is capable of handling Desktop Agent connections, as well as Web and mobile HTTPS sessions.

- Metadata Server. The Metadata Server stores the metadata about all the objects that each Datto user has stored in the system.

- Storage Servers. To provide mass storage for objects that require persistent storage, servers are used that are each capable of storing 24TB in a RAID 6 configuration. As the need for storage capacity grows, additional storage servers are introduced and attached to the internal network.

The following diagram depicts the data flow within a single cell. Note that Volume File Servers can be shared among multiple cells inside a Data Center. Hazelcast and a global (replicated) SQL DB is used to communicate across cells:



Software

The Datto Workplace architecture includes two components installed on users' equipment physically separate from the Datto data center which include the Desktop Agent (in the form of a downloadable installer file for Windows, and Mac computers), and the Mobile Client (in the form of a mobile application from respective application stores for iOS and Android).

Desktop Agent Software

An essential component of Datto's Workplace Cloud System, the Desktop Agent, is a small client application that is installed on users' desktop and laptop computers. Users are required to read and accept the Datto End User License Agreement (EULA) document that covers security and availability obligations before the application will install. The Desktop Agent is used to keep the files in the system updated at all times. The Desktop Agent establishes a secure connection to Datto's Workplace Cloud System and is responsible for transferring selected information from the users' computer to Datto's Workplace Cloud System for persistent mobile access. The Desktop Agent authenticates itself with

the user ID and secret keys for the proper Datto account. The Desktop Agent includes several advanced security features.

128-bit or 256-bit SSL (depending on the Agent type) is used for all communications to the service. The Desktop Agent and Datto Workplace servers communicate using proprietary methods, further ensuring that information is unintelligible to outside systems. The Desktop Agent interacts only with the Datto servers, making it difficult to redirect information. Users can also choose what types of data can be accessed remotely, including files, folders, and email messages. Any information outside explicitly shared content is excluded.

Mobile Client Software

The Mobile Client is an optional application that can be installed on mobile devices. The Datto Workplace Mobile Client allows the exchange of data from the handset to the system and back to the users' desktop computer. Similar to the Desktop Agent, the Mobile Client establishes a secure connection to Datto's Workplace Cloud System and is responsible for transferring selected information from the users' smartphone or tablet to Datto's Workplace Cloud System for persistent mobile access. The Mobile Client authenticates itself with the user ID and secret keys for the proper Datto account. The Mobile Client also includes the same type of advanced security features as the Desktop Agent.

Data

User data (customer information) means information that is stored and managed by Datto's services and includes backed-up or synced files, personal identifiable information, and any related metadata. Datto's security begins with the design of the system and flows through to the physical security of the data center and the protection of users' private data. These protections include:

- SSL (128/168-bit or 256-bit AES depending on the capabilities of the host environment) encryption of all data transmissions.
- Proprietary communications protocols to discourage hacking.
- A modular data center design to provide ease of scalability, redundancy, and protection of data.
- Data centers that are hosted in SOC, ISAE 3402, and/or CSAE 3416 audited facilities.
- Encryption of files at rest on the servers using 256-bit AES with dynamic key injection and rotation.
- HTTPS based on VeriSign certificates.
- Virus scanning of all files transmitted through the system.
- Role-based access and user authentication.
- Device security (no persistent data, cookie management).

Physical Security of Data

The Datto Workplace data centers are guarded and monitored by closed-circuit video. Personnel access is controlled through multilevel security: biometric hand scans, badge, and PIN, all three of which must be negotiated successfully before access is granted. Datto Workplace's servers reside in a locked cage and are not shared. To assure an ongoing high level of security, hosting facilities used by Datto Workplace are subject to periodic System and Organizational Control (SOC) audits as defined by the Association of International Certified Professional Accountants (AICPA), or alternative auditing standards such as Canadian Standard on Assurance Engagements (CSAE) 3416 and International Standards for Assurance Engagements (ISAE) 3402 for Canadian and European service organizations as required by their respective operators.

Network Security of Data

Datto Workplace follows strict procedures to monitor and control network traffic to and from the Datto Workplace data centers which include:

- Making sure each of the data cells receives traffic only on permitted TCP ports.
- Maintaining a whitelist of source IP addresses that are allowed on all other ports.
- Logging detailed statistics of traffic to and from each of the data cells.
- Performing egress filtering to prevent data cells from leaking unwanted traffic (deny and react by raising an alarm to spoofed traffic originating from the cell).
- Using SELinux security module for server systems to restrict application capabilities and limit risks from viruses and otherwise potential intrusions.
- Performing periodic penetration testing and crystal box testing of Datto Workplace Cloud System components by independent third parties to identify vulnerabilities against hackers or authorized access to users' data.

Platform Security for Data

All Datto Workplace servers operate using the CentOS operating system and are thus not at risk by attacks launched against other server operating systems. Servers are updated daily with any relevant patches that are released for the operating system and applications. Periodic penetration and crystal box testing of Datto's platform components are performed to identify and mitigate security vulnerabilities in the systems.

Storage Network for Data

The background store (storage network) for user data is based on RAID 6 drives connected to redundant iSCSI. User data in the background store is logically separated from other users at rest through a top-level folder associated with the Desktop Agent for each unique user. The logical partitioning ensures the secure separation of user data and enforcement of ownership rights. In the event that user data must be purged or removed from Datto's Workplace Cloud System, the agent and the top-level folder are purged to ensure removal of all user-associated data. All files, including files maintained for versioning belonging to a unique user if stored within the top-level folder, are purged, and therefore the purge operation also removes all file versions.

Connection Persistence for Data

Connections to Datto's Workplace Cloud System occur through three different means:

- From the user's own computer running the Datto Workplace Desktop Agent software.
- Through any web browser on any Internet enabled computer.
- Via an application or browser on any mobile device.

Computer Running Datto Workplace Desktop Agent - When an Internet connection to Datto's Workplace Cloud System is established from a computer running the Datto Workplace Desktop Agent software, that connection stays open and available. This is necessary for Datto Workplace to carry out its primary functions, providing secure access to files residing on that computer at any time from any other authorized computer or mobile phone. The Desktop Agent maintains the connection for as long as the Internet connection is present. If the Internet connection is lost for any reason, the Desktop Agent detects this and attempts periodically to re-initiate Datto's Workplace Cloud System session.

Browser Access from Any Computer - Accessing Datto's Workplace Cloud System via a browser from any other computer (one that is not running the Datto Workplace Desktop Agent) does not maintain a persistent connection. If the user does not explicitly end the Datto Workplace session by logging off or closing the browser window, the session automatically times out after 30 minutes of inactivity (or according to the session timeout value set by the Team Admin), even if the computer is used for other purposes during that time.

Mobile - A Datto Workplace session, initiated from a mobile phone, ends when the user logs off. Should the user neglect to log out of Datto Workplace or close the phone's Internet browser, the session automatically times out after 30 minutes of inactivity (or according to the session timeout value set by the Team Admin). If the "Remember Me" feature is selected, the user can initiate a new connection, unless "Remember Me" settings are prohibited for the Datto Workplace site by the Team Admin through a configuration setting.

Security Scanning of Data

All files that pass-through Datto's Workplace Cloud System's servers are scanned in real time for the presence of viruses and malware.

If a virus is detected in incoming emails, then email and/or attachment download ceases immediately. Since incoming data streams are purged immediately if a virus is detected, it is not possible for infected files to be written to the Datto Workplace servers.

If a virus is detected in user files, then the files enter quarantine, and an alert is generated. This alert is the first step in an efficient workflow that allows administrators to react appropriately to the virus intrusion. A separate workflow scans for suspicious file activity that indicates malware/ransomware. If suspicious activity is identified, an alert is generated. This alert is the first step in an efficient workflow that allows administrators to react appropriately to the malware intrusion.

Application-level code is executed in a server environment confined by SELinux domain to ensure that the software used to run and support the service is free from adverse effects on the system or confidentiality of user data.

Support for Encrypted Access

All access to Datto's systems is through 256-bit SSL encryption (when this is not possible, for example, in the case of much older browsers, 128-bit or 168-bit SSL is used). Individual Datto users can access their Datto information through three mechanisms:

- Datto Workplace Client for Local Access. With this method of access, Datto assumes the user is the owner of the information since the individual is physically working with the computer on which the data is stored. The Datto Workplace Desktop Agent can include authentication for access to the local Datto Workplace client if desired, and the client will honor any access rights and restrictions set through the normal operating system mechanism. When the client communicates with the Datto Workplace servers via the Internet, it uses 256-bit SSL for all operations.

- Web Access from a Browser. When a user logs into Datto's Workplace Cloud System, HTTPS is used for all communications. HTTPS (Hypertext Transfer Protocol over Secure Socket Layer or HTTP over SSL) encrypts and decrypts the page requests and page information between the client browser and the web server using a Secure Socket Layer (SSL).

- Access from a Mobile Device. Datto Workplace uses the HTTPS protocol whenever possible. (The majority of modern mobile handsets support HTTPS).

Server Encryption

User file uploads to and downloads from the Datto Workplace servers are fully encrypted. To render thumbnails and collect metadata for faster access, the files may be stored on the Datto Workplace servers in an unencrypted state for short periods while servers are indexing such files.

Encryption at Rest and User Data Partitioning

Data files are stored on servers with 256-bit AES encryption. This prevents the physical files from being viewed in the unlikely event that the files are removed or copied. Encryption at rest is the ultimate defense against physical security breaches.

Key Management

In order to encrypt files at rest, Datto Workplace uses a proprietary key management scheme that utilizes unique rotating sets of keys throughout the background store on a file basis. The encryption keys are stored in encrypted form in a keystore. The keystore that contains the encryption keys is unlocked by the Remote File Server (RFS) at boot time when the required decryption key for the keystore is injected into memory by system operations. As keys are required to unlock specific files, they are fetched and decrypted from the keystore and used. The keys are never stored in the clear, in non-volatile memory or storage media.

People

The organizational structure includes a separation of administrative, technology, finance, customer experience, general counsel, revenue, and marketing functions. The overall organization supports the framework for an effective control environment, and is comprised of the following functional areas:

Executive Management – provides strategic direction and leadership for Datto. 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 IT support, human resources, legal, facilities, and customer success.

Human Resources – is 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 Datto's mission, vision, and values. Datto is committed to equal opportunity of employment and all employment decisions are based on merit, qualifications, and abilities. Employment-related decisions are not influenced or affected by an employee's race, color, nationality, religion, sex, marital status, family status, sexual orientation, disability, or age. Datto endorses a work environment free from discrimination, harassment, and sexual harassment.

Internal IT Support (ITS) – this team provides IT services to all internal employees to the Datto ecosystem. ITS has overall responsibility and accountability for the enterprise computing environment, including single sign on, 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 the Company's business objectives and requirements.

Internal Operations – provides support to all internal employees at Datto regarding workforce solutions, office services, facilities, and productions. Internal Operations assists with conference room support, office supplies, physical network infrastructure, HVAC, building access, and internal video projects.

Quality Assurance – seeks better methods and processes to help ensure the delivery of quality products. The Quality Assurance team is responsible for ensuring that Datto's suite of core backup products function correctly and achieve their intended business goals, ensuring quality in Datto's internal and external websites, and test all projects that come out of the research and development team.

Information Security – avoids losses in confidentiality, integrity, and availability of Datto end user data and critical services through governance activities and maturation in people, processes, and technology. The Information Security team is responsible for incident response, intrusion detection, security information dissemination, vulnerability reporting and testing, red team operations, user awareness training, as well as governance, risk, and compliance.

Software Engineering – strives to innovate, architect, and implement solutions for the most interesting problems in the MSP business space. Datto SE continues to break into new areas of technology and expertise in order to keep Datto in the frontlines of the MSP market, while also providing solutions to problems that no other company has ever solved.

Partner Success – is focused on Datto's customers' overall health, product adoption, and driving improvement to the customer experience. Partner Success works through two main channels: reactive and proactive engagement. The reactive side is related to escalations, billing issues, credit requests, dial downs and cancellations. Proactive campaigns focus on product adoption, releases, and general product awareness leveraging health and adoption score models.

Marketing – is responsible for the strategic deployment of the Datto brand and for building awareness through multiple media channels including the Internet, public relations, advertising, industry associations, and direct mail.

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

Technology – is responsible for the acquisition and maintenance of hardware, firmware, and backup systems that are responsible for the function of the Workplace and File Protection system. Technology provides on-call services that ensure that systems function within established guidelines and service level agreements that allow for a high level of uptime.

Procedures

Datto has a Chief Information Security Officer (CISO) who is responsible for the design and oversight of security and privacy initiatives. The CISO reports directly to the CTO and indirectly to the Chief Executive Officer (CEO). The IT policy framework describes the procedures followed to ensure the performance of consistent processes over the security, availability, confidentiality, and operation of the Workplace and File Protection Platform. All IT policies are reviewed on an annual basis, or more frequently as needed, by the CISO.

All employees are expected to adhere to Datto's IT policy framework as acknowledged during new hire onboarding and during annual security awareness training. The IT policy framework includes procedures that provide guidance on the consistent performance of controls and processes necessary to meet service commitments and system requirements.

Datto has the following formalized policies and procedures:

- Anti-Corruption Policy
- Asset Management Policy
- Business Continuity and Disaster Recovery Plan
- Change Management Policy
- Code of Conduct
- Confidentiality Agreement
- Data Governance Policy
- Electronic Data Destruction Policy
- Employee Handbook
- Enterprise Encryption Policy
- Hiring and Termination Checklist
- Incident Response Plan
- Information Risk Management Policy
- Information Security Policy
- Offboarding Process
- Onboarding Process
- Patch Management Policy
- Vendor Risk Management Policy
- Vulnerability Assessment Policy

Disclosures

No security incidents were detected or reported during the audit period that would affect Datto's service commitments or system requirements.