Datto, Inc.

BCDR Cloud Services

SOC 3

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

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 BCDR Cloud Services 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 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 BCDR Cloud Services 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

St. Petersburg, FL

December 20, 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) BCDR Cloud Services 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 (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 BCDR Cloud Services 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 20, 2022

DESCRIPTION OF DATTO, INC.'S BCDR CLOUD SERVICES SYSTEM

Company Overview

Datto, Inc. (Datto), founded in 2007, is a leading provider of enterprise-level technology to small and medium sized businesses. Datto's Business Continuity & Disaster Recovery (BCDR) solution has been used by companies nationwide. Headquartered in Miami, Florida, Datto serves an extensive and diverse client base, and has long maintained a reputation for excellence in both technologies and services qualities. 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.

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 business continuity and disaster recovery (BCDR) products are set up, configured, managed, and serviced by MSPs for their SMB customers. Datto's BCDR products offer data backup, recovery, and business continuity protection for local, virtual, and cloud environments, all within a single platform. The solution consists of a hybrid cloud backup solution, which includes a local appliance that takes backups of a protected machine and a set of replicated cloud backups, stored in the Datto Cloud, providing MSPs and their clients with:

- **Ransomware protection**: MSPs can quickly recover from a ransomware attack by rolling back their clients' files to a point before the infection hits, without paying a ransom.
- **Peace of mind**: Meet and exceed clients' expectations by offering a simple, yet effective BCDR solution that works to eliminate business downtime and prevent data loss.
- **Fast recovery**: Cut out the stress and cost of business downtime by quickly and easily failing over operations locally or in the Datto Cloud.

System Description

Principal Service Commitments and System Requirements

Datto's Security 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 commitments include, but are not limited to:

- Maintain appropriate administrative, physical, and technical safeguards to protect the security of the Datto BCDR Cloud Services 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.
    - 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 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:

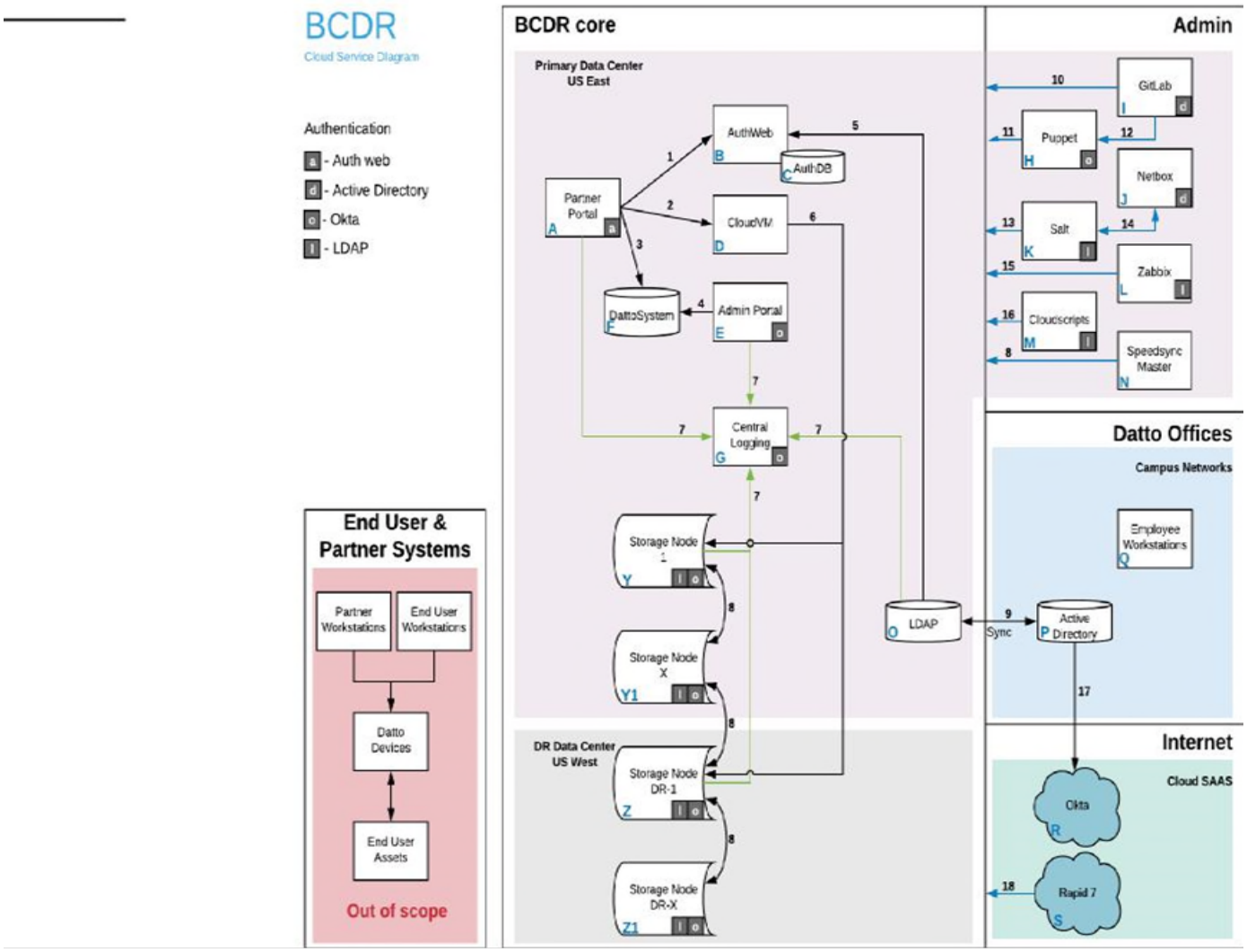
- Infrastructure (facilities, equipment, and networks)
- Software (systems, applications, and utilities)
- Data (transaction streams, files, databases, and tables)
- People (developers, operators, users, and managers)
- Procedures (automated and manual)

Infrastructure

The backbone infrastructure of the Datto Cloud BCDR service is a fleet of systems providing computing power and dense storage capability. These systems receive and store backup data directly from BCDR appliances and allow End Users to restore files, entire systems, or virtualize their infrastructure in the event of a disaster. Depending on End User service levels and subscriptions, backup data may be replicated to a physically separate storage system. In geographical areas with heavy product utilization such as the US, Canada, and Europe, this replication occurs between systems in distinct co-location facilities. In other locations with a growing deployment base this replication occurs between systems resident in the same co-location facility. This replication provides additional levels of data protection and durability needed by End Users to assure data availability in the face of a disaster.

End User and Partner visibility to stored backup data in the Datto Cloud is provided through the 'Partner Portal' which offers status, management, and restoration service capabilities. Employee visibility into systems and services is provided through the 'Admin Portal' which offers additional status, management, and restoration capabilities that are limited to authorized employees.

The Datto BCDR service is additionally supported by a number of other infrastructure, service, and application components. The components of the Datto BCDR Cloud service are represented in the diagram that follows:



System Description (letters)

Letter	Name	Description
A	Partner Portal	Partner Portal is an interface used by End Users and Partners to view the status of their deployed kit and manage the offsite backup recovery services in the Datto Cloud.
B	AuthWeb	AuthWeb is a proprietary authentication service used by Partner Portal. Systems employing AuthWeb are noted with an [a] in the diagram.
C	AuthDB	AuthDB is the database utilized by AuthWeb.
D	CloudVM	CloudVM (a.k.a. Cloud API), from requests initiated through the Partner Portal, provides the ability to perform cloud virtualizations of backed up datasets available in the Datto Cloud.
E	Admin Portal	Admin Portal provides authorized employee access to support Partners and End Users as well as manage backup data and recovery services in the Datto Cloud.

Letter	Name	Description
F	DattoSystem	DattoSystem is the main database supporting most facets of the Datto Cloud service offering. Contents consist of metadata about appliances, agents, and service levels amongst other information.
G	Central Logging	Datto uses ElasticSearch as a centralized logging environment for key system and audit logs.
H	Puppet	Puppet is an Infrastructure as Code configuration management automation tool that assures configuration of systems in the Datto Cloud.
I	GitLab	GitLab is the source control system. It stores source code and puppet manifests, amongst other data assets. It also manages the build and deployment process for software-based services in the Datto Cloud.
J	Netbox	Netbox is the inventory system used by the Datto Cloud system for asset management.
K	Salt	Salt is an interactive Infrastructure Code configuration management tool that allows remote management of the servers in the Datto Cloud at scale.
L	Zabbix	Zabbix is the primary system and network monitoring tool.
M	Cloudscripts	Cloudscripts is a homebrewed administrative system used by System Administrators to gather data and monitor systems.
N	Speedsync Master	Speedsync Master interfaces with DattoSystem and facilitates load balancing and synchronization of backup data to and between storage systems.
O	LDAP	LDAP is the primary production authentication service used by Datto Cloud systems and is noted with an [l] in the diagram.
P	Active Directory	Active Directory is the primary corporate authentication service used by Datto Employees and is noted with a [d] in the diagram. Employee IDs in AD are replicated with LDAP for federated authentication to Datto Cloud systems.
Q	Employee Workstations	Employee workstations are used to maintain, support, engineer, administer, and troubleshoot components of the Datto Cloud.
R	Okta	Okta is a SaaS service that provides SSO and two factor authentication (2FA) for systems and services noted with an "o" in the environment.
S	Rapid7	Rapid7 is the vulnerability scanning platform that performs vulnerability scans on the environment.
Y	Storage Node 1-X	Storage nodes in the primary data center that store End User backup data and execute Datto Cloud recovery services.

Flow Descriptions (numbers)

Number	Description
1	Partner Portal authenticates users via AuthWeb.
2	Partner Portal interfaces with CloudVM to virtualize a protected agent or facilitate a file recovery from the End User backup data in the Datto Cloud.
3	Partner Portal presents device, agent, and backup metadata from DattoSystem to allow for Partner service insight and administration.
4	Admin Portal presents device, agent, and backup metadata from DattoSystem to allow for Employee insight and administration.
5	LDAP employee accounts are federated with AuthDB to permit access to the Partner Portal.
6	CloudVM (a.k.a. Cloud API) instructs the storage nodes on actions to take to fulfill virtual system and file restore recovery service requested through the Partner Portal.
7	Systems log to Central Logging server.
8	Speedsync facilitates load balancing and synchronization of backup data to and between storage systems.
9	Employee IDs are synchronized and federated between LDAP and Active Directory.
10	GitLab manages and pushes source code to the applications to Datto Cloud systems.
11	Puppet pushes configuration manifests to Datto Cloud systems.
12	GitLab pushes managed configuration manifests to Puppet.
13	Salt Master communicates with Salt Minions deployed on Datto Cloud systems for host management and remote command execution activities.
14	Netbox utilizes Salt for server and network inventory management.
15	Zabbix probes systems in the Datto Cloud to monitor and alert on health conditions.
16	Cloudscripts directly gathers configuration and system state data to be consumed by Engineers.
17	Active Directory is federated with Okta for Single Sign-On and Two Factor Authentication.
18	Rapid7 connects to systems in the Datto Cloud to perform vulnerability scans.

Authentication Systems

- AuthWeb
- authDB
- Okta
- LDAP
- Active Directory
- CentralBan

Infrastructure Administration

- Salt
- Puppet
- GitLab
- Netbox
- CloudScripts

Cloud Services Orchestration

- Speedsync
- dattoSystem

Monitoring

- Zabbix
- Rapid7
- ELK

Software

Datto maintains an inventory of open source and SaaS software that are used to support the BCDR solution and business services.

The development, testing, and migration of application changes to production systems are according to change control processes. Application development is based on NIST guidelines. Formalized procedures guide code development and testing. Additional staging and test systems can be brought online in a separate cloud platform. No development and test environment interacts with the production environment. Developers and employees with production code migration duties are separate.

Datto has deployed a variety of solutions and tools to minimize security vulnerabilities associated with code development and code evaluation prior to deployment to the production environment. Access to source code is restricted through the configuration of GitHub; Datto performs a routine audit of GitHub users to validate the appropriateness of access to the system.

Data

Datto stores various types of customer and company data in the cloud solution platform. Sensitive data is protected through secure encryption methodologies during transit and at rest, when encryption options are selected by the partner. Unique encryption keys are utilized.

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. All connectivity to the Datto Cloud utilizes OpenSSH with AES-256 bit encryption to protect backed-up data in transit between local Datto devices and the Datto Cloud. Encryption practices protect information involved in the BCDR solution from incomplete

transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, and replay.

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) – 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, process, 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, and 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 BCDR 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 BCDR Cloud 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.