



DATTO BCDR CUSTOMER RESPONSIBILITY MATRIX

Powered by ControlCase (C3PAO) and KASEYA

Mark Cline | SVP, Sales
404.307.7235
mcline@controlcase.com



AGENDA



- 1 Access Control (AC)
- 2 Awareness and Training (AT)
- 3 Audit and Accountability (AU)
- 4 Configuration Management (CM)
- 5 Identification and Authentication (IA)
- 6 Incident Response (IR)
- 7 Maintenance (MA)
- 8 Media Protection (MP)
- 9 Personnel Security (PS)
- 10 Physical Protection (PE)
- 11 Risk Assessment (RA)
- 12 Security Assessment (CA)
- 13 System and Communications Protection (SC)
- 14 System and Information Integrity (SI)

DATTO BCDR CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AC.L2-3.1.1[a]	PROVIDER supports different user roles and Role-based access control (RBAC) in Datto portal (e.g., Administrator: Full access to device settings, backups, and recovery options and Technician / Operator: Limited access, usually just monitoring or initiating restores.	CUSTOMER defines in policy, authorized users and roles (i.e., specifies Administrators, Technicians, Operators). Review user access periodically	Managing Employee Roles
AC.L2-3.1.1[c]	PROVIDER provides agents on endpoints (servers, PCs, virtual machines), pre-configured with credentials and unique device IDs. Devices with a valid, registered agent can connect to the BCDR appliance or cloud portal.	CUSTOMER provides procedure(s) for authorization, installs Agents on endpoints, servers, or virtual machines that require backup and ensure devices meet minimum system requirements (OS version, disk space, memory).	Device Management
AC.L2-3.1.1[d]	PROVIDER allows access to backup data to registered users, Datto agents and the Datto authorized portal (when local access is disabled)	CUSTOMER provides assignment and system access to authorized users through local access	Managing Employee Roles
AC.L2-3.1.1[f]	PROVIDER determines and enforces that system access is limited to authorized devices (and other systems)	CUSTOMER provides device access (endpoint agent installation) evidence (e.g., logs)	
AC.L2-3.1.2[a]	PROVIDER determines and enforces that system access is limited to authorized devices (and other systems) Granular permissions (restore, delete, configure, view) and Restriction of backup/restore actions to authorized roles		Managing Employee Roles
AC.L2-3.1.2[b]	PROVIDER determines and enforces that system access is limited to authorized devices (and other systems)		

DATTO BCDR CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AC.L2-3.1.5[a]	PROVIDER determines that privileged accounts are identified through role assignment to a user account(s) Role-based permissions apply and no default full admin for all users	CUSTOMER provides evidence that least privileged roles are (have been) identified, defining which accounts are privileged	Managing Employee Roles
AC.L2-3.1.5[b]	PROVIDER uses security levels (roles) where accounts are assigned against roles compliant with least privilege; actions outside the assigned role are automatically blocked	CUSTOMER determines if access to privileged accounts is (has been) authorized.	
AC.L2-3.1.5[c]	PROVIDER relies on built-in features, configuration, and logging to identify security functions with enforcement	CUSTOMER determines if security functions are (have been) identified. Reviewed periodically.	
AC.L2-3.1.5[d]	PROVIDER enforces and technically restrict access based on roles and permissions assigned by the customer	CUSTOMER provides authorization access to security functions according to least privilege.	
AU.L2-3.3.1[a]	PROVIDER provides audit capability such as login/outs, success/failures, named user, timestamp, target systems	CUSTOMER specifies audit log content (i.e., user login and logout events, privileged actions (role changes, script execution, patch approvals), remote session activities, configuration changes and policy modifications)	Reports and Alerting
AU.L2-3.3.1[b]		CUSTOMER defines, provides evidence of audit log content	Reports and Alerting

DATTO BCDR CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AU.L2-3.3.1[c]		CUSTOMER provides evidence of audit log generation	Reports and Alerting
AU.L2-3.3.1[d]		CUSTOMER determines if audit logs contain defined content	
AU.L2-3.3.1[e]	PROVIDER retains audit logs for the active subscription period (typically 90 days)	CUSTOMER determines audit log export for long-term retention (i.e., 1 year)	
AU.L2-3.3.1[f]	PROVIDER provides audit records retention	CUSTOMER provides audit records as defined	
AU.L2-3.3.2[a]	PROVIDER provides who performed the action, what action occurred, timestamps and target system/device	CUSTOMER provides the defined content	User Activity Log
AU.L2-3.3.2[b]		CUSTOMER to determine if audit record(s) includes the defined content.	

DATTO BCDR CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AU.L2-3.3.3[a]		CUSTOMER to define process for determining when to review logged events	User Activity Log
AU.L2-3.3.3[b]		CUSTOMER to perform reviews of logs in accordance with the defined review process	
AU.L2-3.3.3[c]		CUSTOMER to determine if event types are (or need to be) updated	
AU.L2-3.3.8[a]	PROVIDER provides tamper-resistant cloud-stored logs and Role-restricted access to logs		
AU.L2-3.3.8[b]		CUSTOMER to determine if audit information is protected from unauthorized modification	
AU.L2-3.3.8[c]		CUSTOMER to determine if audit information is protected from unauthorized deletion	

DATTO BCDR CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AU.L2-3.3.8[d]		CUSTOMER to determine if audit information is protected from unauthorized access	
AU.L2-3.3.8[e]		CUSTOMER to determine if audit tool is protected from unauthorized access	
AU.L2-3.3.8[f]		CUSTOMER to determine if audit tool is protected from unauthorized deletion	
CM.L2-3.4.1[a]	PROVIDER provides configurations such as Backup schedules Retention policies, device registration, RBAC (roles/permissions), security settings (MFA, encryption, network restrictions)	CUSTOMER defines and documents the baseline configuration for systems and backups, then applies the baseline across all devices and agents	Device Management
CM.L2-3.4.1[b]	PROVIDER (once configured) provides a baseline, reporting hardware (model/specs), software (agent version, features, assigned policies) and firmware (appliance OS/firmware version)	CUSTOMER determines if the baseline configuration includes hardware, software and firmware	

DATTO BCDR CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
CM.L2-3.4.1[c]	PROVIDER provides baseline configuration functionality	CUSTOMER determines if baseline is maintained throughout system lifecycle	
CM.L2-3.4.1[d]	PROVIDER provides an inventory (i.e., device hostname and type, OS and version, agent version and configuration, appliance/cloud reporting, logging and alerts)	CUSTOMER determines and establishes inventory	
CM.L2-3.4.1[e]	PROVIDER provides a system inventory (hostname, type (server, laptop, VM), hardware specs (CPU, memory, storage), OS, installed agent version, installed applications and endpoint BIOS/UEFI firmware)	CUSTOMER determines if system inventory includes hardware, software and firmware documentation	
CM.L2-3.4.1[f]	PROVIDER provides a system inventory (HW, SW, Firmware)	CUSTOMER determines if the inventory is maintained through system lifecycle	
CM.L2-3.4.4[a]	PROVIDER provides backup verification, Test restores and Virtualization testing		
IA.L2-3.5.1[a]	PROVIDER provides named user accounts and MFA for portal access	CUSTOMER determines if provided users are identified	Managing Employee Roles

DATTO BCDR CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
IA.L2-3.5.2[a]	PROVIDER determines if each user is authenticated before granting system access	CUSTOMER to verify unique authenticators are used to verify user identities	Portal Login
IA.L2-3.5.2[b]		CUSTOMER to define which processes (i.e., service accounts) are allowed to run on endpoints	
IA.L2-3.5.2[c]	PROVIDER determines if a device is authenticated before it can access or connect to the system (agent installed and registered)	CUSTOMER responsible for defining and controlling which devices are authorized to access the system	
IR.L2-3.6.1[a]	PROVIDER provides supports recovery, and enables recovery from ransomware or outages	CUSTOMER establishes operational incident-handling capability	Reports and Alerting
IR.L2-3.6.1[b]		CUSTOMER determines if the operational incident-handling capability includes preparation	
IR.L2-3.6.1[c]		CUSTOMER determines if the operational incident-handling capability includes detection.	

DATTO BCDR CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
IR.L2-3.6.1[d]		CUSTOMER determines if the operational incident-handling capability includes analysis.	
IR.L2-3.6.1[e]		CUSTOMER determines if the operational incident-handling capability includes containment.	
IR.L2-3.6.1[f]		CUSTOMER determines if the operational incident-handling capability includes recovery.	
IR.L2-3.6.1[g]		CUSTOMER determines if the operational incident-handling capability includes user response activities.	
IR.L2-3.6.2[a]	PROVIDER tracks alerts, failed backups, failed restores, missed schedules, corrupt images	CUSTOMER responds to incidents	Reports and Alerting
IR.L2-3.6.2[b]	PROVIDER provides event logs, alerts, and system activity records	CUSTOMER to determine which events are security incidents, investigates and classifies incidents and produces formal incident reports for compliance or audits	Integrations

DATTO BCDR CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
IR.L2-3.6.2[c]		CUSTOMER to determine who to notify, such as internal management, regulatory bodies, or law enforcement	
IR.L2-3.6.2[d]		CUSTOMER to determine who to notify, such as internal management, regulatory bodies, or law enforcement	
IR.L2-3.6.2[e]		CUSTOMER to determine if internal management, regulatory bodies, or law enforcement are (have been) notified	
IR.L2-3.6.2[f]		CUSTOMER to determine if internal management, regulatory bodies, or law enforcement are (have been) notified	
MA.L2-3.7.2[a]	PROVIDER provides maintenance operations enforcing RBAC to restrict maintenance tasks to authorized personnel, logging all maintenance actions for audit and review, securing software and firmware updates to prevent unauthorized tool installation, and relies on customer oversight to assign roles and review	CUSTOMER assign roles and permissions according to the principle of least privilege, authorized personnel can perform system maintenance (backup restores, agent updates, appliance configuration). Create, modify, or disable accounts for users as personnel change and enforce MFA	Device Access
MA.L2-3.7.2[b]	PROVIDER techniques are the maintenance tasks (backups, restores, updates) executed through endpoints or server agents.	CUSTOMER authorizes users who approve patches, creates or run scripts and authorizes computer restarts	

DATTO BCDR CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
MA.L2-3.7.2[c]	PROVIDER provides mechanisms such as patch management, script automation, software deployment, monitoring, alerting and remote control	CUSTOMER assigns Role-Based Access Control (RBAC) to ensure only authorized users can execute tasks	
MA.L2-3.7.2[d]	PROVIDER enforces that only authorized users can log in and perform maintenance (e.g., Role-Based Access Control (RBAC), Admin, Technician, Operators)	CUSTOMER establishes policies and procedures for system maintenance and assign, review, and manage personnel access	
MA.L2-3.7.4[a]	PROVIDER checks media for malicious code automatically	CUSTOMER establishes policies and procedures for system maintenance	Backup Verification
MA.L2-3.7.5[a]	PROVIDER mandates MFA to Partner Portal Home (website)	CUSTOMER establishes policies and procedures for system maintenance	Introduction to Screenshot Verification
RA.L2-3.11.1[a]		CUSTOMER defines frequency to assess organizational risks	
RA.L2-3.11.1[b]	PROVIDER performs data Backups, indicates success/failure data and data restoration results	CUSTOMER establishes policies and procedures for system maintenance	

DATTO BCDR CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
CA.L2-3.12.1[a]	PROVIDER periodically performs internal audits and vulnerability assessments of its appliances, cloud services, and agent software quarterly or semi-annually for formal internal audits	CUSTOMER establishes policies, procedures and defined frequency for security assessment reviews	
CA.L2-3.12.1[b]	PROVIDER performs ongoing control evaluation continuously enforcing controls and releases updates, while internal formal reviews are conducted periodically	CUSTOMER provides evidence that controls are effective in their application	
SC.L2-3.13.1[a]		CUSTOMER to define, identify and control external boundaries	
SC.L2-3.13.1[b]		CUSTOMER to define, identify and control internal boundaries	
SC.L2-3.13.1[c]	PROVIDER provides logs include who connected, when, from where, and what actions were taken	CUSTOMER to determine if communications at external boundary are monitored.	
SC.L2-3.13.1[d]	PROVIDER tracks network interfaces, IP addresses, and connectivity of endpoints	CUSTOMER to define, identify and monitor internal boundaries	

DATTO BCDR CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
SC.L2-3.13.1[e]	PROVIDER provides enforcement over which device(s) can communicate with specific systems (i.e., a registered agent)	CUSTOMER to determine authorized devices, users and managed endpoints and apply policies as applicable. CUSTOMER to review logs and show external communications were initiated by controlled agents or users.	
SC.L2-3.13.1[f]	PROVIDER provides capability to assign endpoints to logical groups (e.g., Finance PCs, Production Servers) where patching, software restrictions, and remote access can be applied per group	CUSTOMER to determine critical internal systems such as Financial systems vs general user workstations, servers storing Controlled Unclassified Information (CUI) vs other servers, development environments vs production environments	
SC.L2-3.13.1[g]	PROVIDER provides TLS-encrypted channels for all agent-to-console and technician-to-endpoint communications and logs record who accessed what and when	CUSTOMER to determine if information transmitted across the external boundary is confidential and authenticated (Encryption, TLS/SSL, VPN)	
SC.L2-3.13.1[h]		CUSTOMER provides review of session logs to verify all cross-boundary remote management communications are encrypted.	
SC.L2-3.13.8[a]	PROVIDER encrypts data in transit and data at rest		
SC.L2-3.13.8[b]		CUSTOMER provides/identifies alternative physical safeguards	

DATTO BCDR CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
SC.L2-3.13.8[c]	PROVIDER encrypts data in transit and data at rest	CUSTOMER provides/identifies alternative physical safeguards	
SC.L2-3.13.16[a]	PROVIDER protects data with AES-256 encryption at rest (Backup images, Snapshot data)		
SI.L2-3.14.1[a]	PROVIDER provide alerting and monitoring capabilities	CUSTOMER determines in policy, the time (i.e., when) to identify system flaws	
SI.L2-3.14.1[b]		CUSTOMER determines if system flaws are identified within specified timeframe(s)	
SI.L2-3.14.1[c]		CUSTOMER specifies in policy, the time to report system flaws	
SI.L2-3.14.1[d]		CUSTOMER determines if system flaws are (have been) reported within the specified timeframe	

DATTO BCDR CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
SI.L2-3.14.1[e]		CUSTOMER specifies in policy, the time to correct system flaws Example: Critical vulnerabilities, corrected within 7 days, High vulnerabilities corrected within 14 days	
SI.L2-3.14.1[f]	PROVIDER updates are deployed in a Continuous Deployment model, with infrastructure patches occurring regularly. Agent updates are automatically rolled out across the fleet using a staged rollout process.	CUSTOMER to review reporting for when the vulnerability, missing patch, or misconfiguration was first flagged, then compare against established timeframes.	
SI.L2-3.14.6[a]	PROVIDER provides monitoring signals related to attacks within the backup environment	CUSTOMER responsible for enterprise-wide attack detection	Reports and Alerting
SI.L2-3.14.6[b]	PROVIDER monitors agent-to-appliance connectivity, backup job traffic health (success/failure, integrity) and anomalous data patterns within backup streams	CUSTOMER responsible for monitoring inbound network communications traffic through perimeter security controls	Reports and Alerting
SI.L2-3.14.6[c]		CUSTOMER responsible for monitoring outbound communications traffic to detect attacks and indicators of potential attacks.	

CONTACT US



404.307.7235



mcline@controlcase.com



Corporate Headquarters
3975 FAIR RIDGE DR STE T25S-D
FAIRFAX, VA 22033

