v1.0

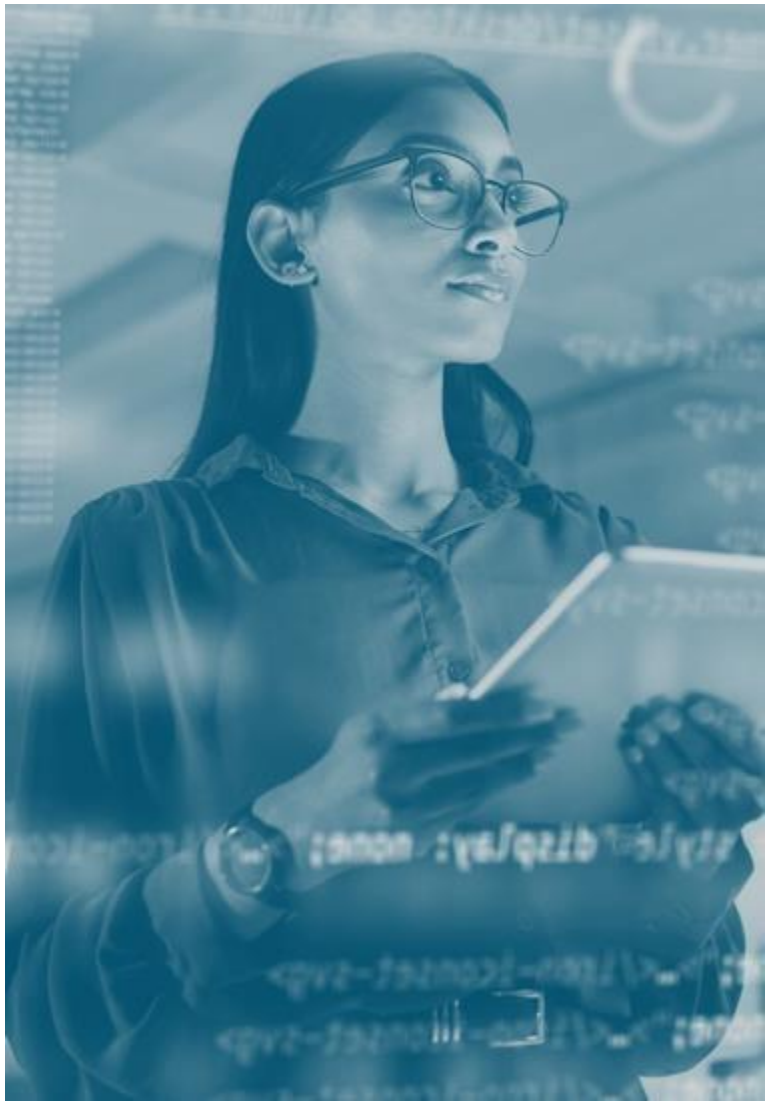
COMPLIANCE MANAGER GRC CUSTOMER RESPONSIBILITY MATRIX

Powered by ControlCase (C3PAO) and KASEYA

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

NIST 800-171 Rev 2

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)

COMPLIANCE MANAGER GRC CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AC.L2-3.1.1[a]	KASEYA is responsible for creating the CUSTOMER admin account during the provisioning of the CUSTOMER environment and sending an email with a setup link to the CUSTOMER. This ensures the CUSTOMER has secure access to the PRODUCT.	CUSTOMER is responsible for completing the password reset process to establish a password for the CUSTOMER admin account. Additionally, the CUSTOMER must manage the CUSTOMER admin account and identify any additional authorized users.	Enable SSO Login with KaseyaOne
AC.L2-3.1.1[b]	KASEYA enables functionality that allows the CUSTOMER to configure and manage scan jobs, ensuring the system supports CUSTOMER-defined operational workflows.	CUSTOMER is responsible for managing scan jobs based on its internal processes, including any required approval or change management procedures that must be completed before configuring or modifying scan jobs.	Configure Devices with Benchmarks
AC.L2-3.1.1[c]	KASEYA provides a agent that can be downloaded from KASEYA's portal, ensuring the CUSTOMER has the necessary software to deploy within its system.	CUSTOMER is responsible for identifying the system(s) to which the agent will be installed, ensuring compatibility and adherence to internal security and operational requirements.	Enable Compliance Scans for Discovery Agents
AC.L2-3.1.1[d]	KASEYA requires authentication through a username and password for the CUSTOMER admin account, ensuring secure initial access to the system. Additionally, KASEYA offers a single sign-on PRODUCT to facilitate integration with the CUSTOMER's identity KASEYA.	CUSTOMER is responsible for using the admin account only for initial access and not for daily system management. CUSTOMER must also implement single sign-on via its own identity source, leveraging KASEYA's single sign-on product to ensure secure and controlled user access.	Users and Global Access Roles
AC.L2-3.1.1[e]	KASEYA enables functionality that allows the CUSTOMER to configure and manage scan jobs, ensuring that system access for automated processes aligns with CUSTOMER-defined operational workflows.	CUSTOMER is responsible for configuring scan jobs that have been approved through its internal processes, ensuring adherence to required approval and security measures before implementation.	Configure Devices with Benchmarks
AC.L2-3.1.1[f]	KASEYA supplies a agent that the CUSTOMER can deploy, ensuring compatibility with authorized systems and maintaining secure access controls.	CUSTOMER is responsible for installing the agent on its system(s).	Users and Global Access Roles

COMPLIANCE MANAGER GRC CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AC.L2-3.1.2[b]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER is responsible for assigning user accounts to the appropriate roles based on required permissions, ensuring that authorized users have access to the necessary transactions and functions within the system.	
AC.L2-3.1.5[a]	See KASEYA responsibility for AC.L2-3.1.1[a].	See CUSTOMER responsibility for AC.L2-3.1.1[a].	Manage Users (Global Level)
AC.L2-3.1.5[b]	KASEYA holds no responsibility in meeting this objective.	See CUSTOMER responsibility for AC.L2-3.1.2[b].	
AC.L2-3.1.5[c]	KASEYA incorporates the following security functions within the PRODUCT: - Account Management – Supports the management of the CUSTOMER admin account and additional user accounts. - Configuration Management – Enables PRODUCT configuration to implement single sign-on via the CUSTOMER's own identity KASEYA, leveraging KASEYA's single sign-on PRODUCT to ensure secure and controlled user access. - Vulnerability Management – Facilitates the use of the PRODUCT to identify vulnerabilities within the CUSTOMER's environment.	CUSTOMER holds no responsibility in achieving this objective.	MFA and Portal Users
AC.L2-3.1.5[d]	KASEYA holds no responsibility in meeting this objective.	See CUSTOMER responsibility for AC.L2-3.1.2[b].	
AC.L2-3.1.7[a]	See KASEYA responsibility for AC.L2-3.1.2[a].	CUSTOMER holds no responsibility in achieving this objective.	Users and Global Access Roles

COMPLIANCE MANAGER GRC CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AC.L2-3.1.8[a]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER is responsible for establishing measures to limit unsuccessful logon attempts. This includes implementing security controls, such as account lockout policies, multi-factor authentication, or other methods, to prevent unauthorized access and maintain system integrity.	
AC.L2-3.1.8[b]	KASEYA offers a single sign-on PRODUCT to facilitate integration with the CUSTOMER's identity source, enabling secure authentication mechanisms.	CUSTOMER is responsible for implementing single sign-on through its own identity source, utilizing KASEYA's single sign-on product to enforce secure and controlled access, including measures to limit unsuccessful logon attempts.	Enable SSO Log In with KaseyaOne
AC.L2-3.1.11[a]	KASEYA establishes and enforces session termination policies within the PRODUCT, which requires all user sessions be automatically terminated after 7 hours of inactivity.	CUSTOMER holds no responsibility in achieving this objective.	
AC.L2-3.1.11[b]	KASEYA configures the PRODUCT to enforce automatic session termination based on defined conditions, ensuring that user sessions are ended after 7 hours of inactivity.	CUSTOMER holds no responsibility in achieving this objective.	
AT.L2-3.2.2[a]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER is responsible for defining information security-related duties, roles, and responsibilities associated with the management and use of the product.	
AT.L2-3.2.2[b]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER is responsible for assigning designated personnel to fulfill the defined information security-related duties, roles, and responsibilities associated with the management and use of the product.	

COMPLIANCE MANAGER GRC CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AT.L2-3.2.2[c]	KASEYA provides user manuals and other PRODUCT literature to support the CUSTOMER in understanding and utilizing the PRODUCT effectively.	CUSTOMER is responsible for ensuring that personnel assigned to information security-related duties, roles, and responsibilities receive adequate training. This includes leveraging KASEYA's documentation and implementing additional training as needed to ensure personnel can effectively manage and secure the product.	Compliance Manager GRC KB Home
AU.L2-3.3.1[a]	KASEYA defines and implements the audit logging framework within the PRODUCT, determining which event types are captured for monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. The following event types are captured: Scan Completed, Scan Started, and Scan Created.	CUSTOMER holds no responsibility in achieving this objective.	
AU.L2-3.3.1[b]	KASEYA defines and implements the content structure of audit records within the PRODUCT to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. Each audit record is configured to capture essential information, including Date, Site, User, Message, and Detail.	CUSTOMER holds no responsibility in achieving this objective.	
AU.L2-3.3.1[c]	See KASEYA responsibility for AU.L2-3.3.1[a] and AU.L2-3.3.1[b].	CUSTOMER holds no responsibility in achieving this objective.	
AU.L2-3.3.1[d]	See KASEYA responsibility for AU.L2-3.3.1[a] and AU.L2-3.3.1[b].	CUSTOMER holds no responsibility in achieving this objective.	
AU.L2-3.3.1[e]	KASEYA establishes and enforces retention requirements for the PRODUCT's audit records, ensuring that logs are maintained for 6 months to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	CUSTOMER holds no responsibility in achieving this objective.	

COMPLIANCE MANAGER GRC CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AU.L2-3.3.1[f]	KASEYA configures the PRODUCT to retain audit records for the defined retention period, ensuring compliance with security and regulatory requirements. This retention policy supports monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity	CUSTOMER holds no responsibility in achieving this objective.	
AU.L2-3.3.2[a]	See KASEYA responsibility for AU.L2-3.3.1[b].	CUSTOMER holds no responsibility in achieving this objective.	
AU.L2-3.3.2[b]	See KASEYA responsibility for AU.L2-3.3.1[b].	CUSTOMER holds no responsibility in achieving this objective.	
AU.L2-3.3.3[a]	KASEYA establishes a structured process that mandates an annual review of logged events.	CUSTOMER holds no responsibility in achieving this objective.	
AU.L2-3.3.3[b]	KASEYA conducts an annual assessment of the event types being logged within the PRODUCT. Findings from the review inform any necessary adjustments to enhance the PPRODUCT's logging capabilities.	CUSTOMER holds no responsibility in achieving this objective.	
AU.L2-3.3.3[c]	Based on the annual review, KASEYA updates the audit log configuration where necessary.	CUSTOMER holds no responsibility in achieving this objective.	

COMPLIANCE MANAGER GRC CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AU.L2-3.3.8[a]	KASEYA ensures that audit information within the PRODUCT's audit logs is safeguarded against unauthorized access, modification, or deletion, maintaining data integrity and compliance.	CUSTOMER ensures that authorized users can access audit information within the PRODUCT's audit logs, in compliance with AC.L2-3.1.2[b].	Compliance Manager GRC Assign Site Roles
AU.L2-3.3.8[b]	See KASEYA responsbility for AU.L2-3.8.8[a].	CUSTOMER holds no responsibility in achieving this objective.	Compliance Manager GRC Assign Site Roles
AU.L2-3.3.8[c]	See KASEYA responsbility for AU.L2-3.8.8[a].	CUSTOMER holds no responsibility in achieving this objective.	Compliance Manager GRC Assign Site Roles
AU.L2-3.3.8[d]	KASEYA implements security controls to protect audit logging tools within the PRODUCT, preventing unauthorized access, modification, or removal to ensure continuous logging functionality.	CUSTOMER holds no responsibility in achieving this objective.	Compliance Manager GRC Assign Site Roles
AU.L2-3.3.8[e]	See KASEYA responsbility for AU.L2-3.8.8[d].	CUSTOMER holds no responsibility in achieving this objective.	Compliance Manager GRC Assign Site Roles
AU.L2-3.3.8[f]	See KASEYA responsbility for AU.L2-3.8.8[d].	CUSTOMER holds no responsibility in achieving this objective.	Compliance Manager GRC Assign Site Roles

COMPLIANCE MANAGER GRC CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
CM.L2-3.4.2[a]	KASEYA develops the PRODUCT and enables certain settings to be configurable by the CUSTOMER, allowing customization within defined parameters. KASEYA does not manage or enforce the CUSTOMER's chosen configurations.	CUSTOMER determines and establishes security configurations within the available configurable settings of the PRODUCT, ensuring alignment with organizational security requirements.	Quick Start Guide To Perform Your First Assessment
CM.L2-3.4.2[b]	While KASEYA does not manage CUSTOMER configurations, it ensures that mechanisms within the PRODUCT support enforcement of configurable security settings according to industry best practices.	CUSTOMER is responsible for managing and enforcing security configurations within the PRODUCT, ensuring compliance with policies and operational needs.	Quick Start Guide To Perform Your First Assessment
IA.L2-3.5.1[a]	See KASEYA responsibility for AC.L2-3.1.1[a].	See CUSTOMER responsibility for AC.L2-3.1.1[a].	Manage Users and Access
IA.L2-3.5.1[b]	See KASEYA responsibility for AC.L2-3.1.1[b].	See CUSTOMER responsibility for AC.L2-3.1.1[b].	Conducting Compliance Assessments
IA.L2-3.5.1[c]	See KASEYA responsibility for AC.L2-3.1.1[c].	See CUSTOMER responsibility for AC.L2-3.1.1[c].	
IA.L2-3.5.2[a]	See KASEYA responsibility for AC.L2-3.1.1[d].	See CUSTOMER responsibility for AC.L2-3.1.1[d].	Users and Global Access Roles

COMPLIANCE MANAGER GRC CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
IA.L2-3.5.2[c]	See KASEYA responsibility for AC.L2-3.1.1[f].	See CUSTOMER responsibility for AC.L2-3.1.1[f].	
IA.L2-3.5.3[a]	See KASEYA responsibility for AC.L2-3.1.1[a].	See CUSTOMER responsibility for AC.L2-3.1.1[a].	Manage Users and Access
IA.L2-3.5.3[b]	See KASEYA responsibility for AC.L2-3.1.8[b].	CUSTOMER is responsible for implementing single sign-on through its own identity source, utilizing KASEYA's single sign-on product to enforce secure and controlled access, including implementing multifactor authentication for local access to privileged accounts.	Enable SSO Login with KaseyaOne
IA.L2-3.5.3[c]	See KASEYA responsibility for AC.L2-3.1.8[b].	CUSTOMER is responsible for implementing single sign-on through its own identity source, utilizing KASEYA's single sign-on product to enforce secure and controlled access, including implementing multifactor authentication for network access to privileged accounts.	Enable SSO Login with KaseyaOne
IA.L2-3.5.3[d]	See KASEYA responsibility for AC.L2-3.1.8[b].	CUSTOMER is responsible for implementing single sign-on through its own identity source, utilizing KASEYA's single sign-on product to enforce secure and controlled access, including implementing multifactor authentication for network access to non-privileged accounts.	Enable SSO Login with KaseyaOne
IA.L2-3.5.2[c]	See KASEYA responsibility for AC.L2-3.1.1[f].	See CUSTOMER responsibility for AC.L2-3.1.1[f].	

COMPLIANCE MANAGER GRC CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
IA.L2-3.5.4[a]	See KASEYA responsibility for AC.L2-3.1.8[b].	CUSTOMER is responsible for implementing single sign-on through its own identity source, utilizing KASEYA's single sign-on product to enforce secure and controlled access, including employing replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	Enable SSO Login with KaseyaOne
IA.L2-3.5.5[a]	See KASEYA responsibility for AC.L2-3.1.8[b].	CUSTOMER is responsible for implementing single sign-on through its own identity source, utilizing KASEYA's single sign-on product to enforce secure and controlled access, including defining a period within which identifiers cannot be reused.	Enable SSO Login with KaseyaOne
IA.L2-3.5.5[b]	See KASEYA responsibility for AC.L2-3.1.8[b].	CUSTOMER is responsible for implementing single sign-on through its own identity source, utilizing KASEYA's single sign-on product to enforce secure and controlled access, including preventing the reuse of identifiers within the defined period.	Enable SSO Login with KaseyaOne
IA.L2-3.5.6[a]	See KASEYA responsibility for AC.L2-3.1.8[b].	CUSTOMER is responsible for implementing single sign-on through its own identity source, utilizing KASEYA's single sign-on product to enforce secure and controlled access, including defining a period of inactivity after which an identifier is disabled.	Enable SSO Login with KaseyaOne
IA.L2-3.5.6[b]	See KASEYA responsibility for AC.L2-3.1.8[b].	CUSTOMER is responsible for implementing single sign-on through its own identity source, utilizing KASEYA's single sign-on product to enforce secure and controlled access, including disabling identifiers after the defined period of inactivity.	Enable SSO Login with KaseyaOne
IA.L2-3.5.7[a]	See KASEYA responsibility for AC.L2-3.1.8[b].	CUSTOMER is responsible for implementing single sign-on through its own identity source, utilizing KASEYA's single sign-on product to enforce secure and controlled access, including defining password complexity requirements.	Enable SSO Login with KaseyaOne

COMPLIANCE MANAGER GRC CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
IA.L2-3.5.7[c]	See KASEYA responsibility for AC.L2-3.1.8[b].	CUSTOMER is responsible for implementing single sign-on through its own identity source, utilizing KASEYA's single sign-on product to enforce secure and controlled access, including enforcing minimum password complexity requirements as defined when new passwords are created.	Enable SSO Login with KaseyaOne
IA.L2-3.5.7[d]	See KASEYA responsibility for AC.L2-3.1.8[b].	CUSTOMER is responsible for implementing single sign-on through its own identity source, utilizing KASEYA's single sign-on product to enforce secure and controlled access, including enforcing minimum password change of character requirements as defined when new passwords are created.	Enable SSO Login with KaseyaOne
IA.L2-3.5.8[a]	See KASEYA responsibility for AC.L2-3.1.8[b].	CUSTOMER is responsible for implementing single sign-on through its own identity source, utilizing KASEYA's single sign-on product to enforce secure and controlled access, including specifying the number of generations during which a password cannot be reused.	Enable SSO Login with KaseyaOne
IA.L2-3.5.8[b]	See KASEYA responsibility for AC.L2-3.1.8[b].	CUSTOMER is responsible for implementing single sign-on through its own identity source, utilizing KASEYA's single sign-on product to enforce secure and controlled access, including prohibiting the reuse of passwords during the specified number of generations.	Enable SSO Login with KaseyaOne
IA.L2-3.5.9[a]	See KASEYA responsibility for AC.L2-3.1.8[b].	CUSTOMER is responsible for using the admin account only for initial access and not for daily system management. CUSTOMER must also implement single sign-on via its own identity source, leveraging KASEYA's single sign-on product to ensure secure and controlled user access, which includes requiring an immediate change to a permanent password when a temporary password is used for system logon.	Enable SSO Login with KaseyaOne
IA.L2-3.5.10[a]	See KASEYA responsibility for AC.L2-3.1.8[b].	CUSTOMER is responsible for implementing single sign-on through its own identity source, utilizing KASEYA's single sign-on product to enforce secure and controlled access, including cryptographically protecting passwords in storage.	Enable SSO Login with KaseyaOne

COMPLIANCE MANAGER GRC CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
IA.L2-3.5.10[b]	See KASEYA responsibility for AC.L2-3.1.8[b].	CUSTOMER is responsible for implementing single sign-on through its own identity source, utilizing KASEYA's single sign-on product to enforce secure and controlled access, including cryptographically protecting passwords in transit.	Enable SSO Login with KaseyaOne
IA.L2-3.5.11[a]	See KASEYA responsibility for AC.L2-3.1.8[b].	CUSTOMER is responsible for implementing single sign-on through its own identity source, utilizing KASEYA's single sign-on product to enforce secure and controlled access, including obscuring feedback of authentication information.	Enable SSO Login with KaseyaOne
MA.L2-3.7.1[a]	KASEYA manages the product life cycle, including the development of the agent. While KASEYA ensures updates are available, they do not automatically apply updates to agents installed in CUSTOMER environments unless the automatic update functionality is enabled. KASEYA releases updates to the agent as part of ongoing product maintenance, ensuring improvements in security, functionality, and compatibility.	The CUSTOMER is responsible for managing the maintenance of installed agents within their environment. If automatic updates are enabled (default setting), updates are applied automatically. If disabled, the CUSTOMER must manually push updates from the product portal. The CUSTOMER ensures that updates are implemented according to their chosen update configuration, either by allowing automatic updates or manually pushing updates via the product portal.	
SC.L2-3.13.15[a]	KASEYA ensures that security measures are in place to protect the authenticity of communication sessions between the PRODUCT and any CUSTOMER admin. This includes implementing encryption, authentication protocols, and secure session management to prevent unauthorized access, tampering, or interception, in alignment with NIST SP 800-171 requirements.	CUSTOMER holds no responsibility in achieving this objective.	Your IT Portal
SI.L2-3.14.1[a]	KASEYA establishes the timeframe for identifying system flaws within the agent as part of its product lifecycle management.	If the CUSTOMER has disabled automatic updates, they identify system flaws by accessing the product portal, which indicates when an update is available to address detected issues.	
SI.L2-3.14.1[b]	KASEYA conducts continuous monitoring and analysis of the agent to detect system flaws within the defined timeframe.	The CUSTOMER must check the product portal within their internally defined timeframe to ensure they are aware of available updates addressing system flaws.	

COMPLIANCE MANAGER GRC CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
SI.L2-3.14.1[d]	KASEYA ensures that detected flaws are reported within the established timeframe as part of its development process.	The CUSTOMER ensures identified flaws are reported within their internally defined timeframe when managing manual updates.	
SI.L2-3.14.1[e]	KASEYA defines the timeframe within which system flaws must be remediated in the agent to maintain security and functionality.	The CUSTOMER defines a timeframe for applying updates after KASEYA makes a corrected version available, ensuring flaws are addressed promptly.	
SI.L2-3.14.1[f]	KASEYA addresses system flaws within the defined remediation timeframe and releases updated versions of the agent. Updates are made available to CUSTOMER environments, either automatically if default settings are maintained or manually through the product portal if automatic updates are disabled.	The CUSTOMER is responsible for managing the update process for the agent within their environment. If automatic updates remain enabled (default setting), system flaw corrections are applied immediately. If manual updates are required, the CUSTOMER ensures that system flaws are corrected within their internally defined timeframe to maintain security and operational integrity.	

CONTACT US

404.307.7235

mcline@controlcase.com

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

ControlCase Kaseya