v1.0

SaaS Alerts 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)

SAAS ALERTS CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AC.L2-3.1.1[a]	KASEYA provisions the initial CUSTOMER admin account using the email address supplied during onboarding. This account is designated as a backup and excluded from regular operational use. All other user accounts must be created via the CUSTOMER's identity source using KASEYA's SSO capability.	CUSTOMER manages user identities via their own identity source and provisions accounts through the PROVIDER's SSO capability. The initial admin account, created from the onboarding email, is retained solely for backup and not used for regular access.	Enable SSO with KaseyaOne
AC.L2-3.1.1[b]	KASEYA ensures all actions within the system are attributed to authenticated SSO user identities, captured in audit logs.	CUSTOMER ensures users authenticate via SSO; process attribution is handled by the PRODUCT.	Enable SSO with KaseyaOne
AC.L2-3.1.1[c]	KASEYA enables the PRODUCT dashboard to support CUSTOMER-initiated connections to specific SaaS systems.	CUSTOMER selects and authorizes which SaaS systems (e.g., Google Workspace, Office 365, Salesforce) should connect to the PRODUCT via the dashboard.	
AC.L2-3.1.1[d]	KASEYA enforces access control via SSO integration and role-based permissions.	CUSTOMER controls identity source and ensures only authorized users are provisioned and granted access via SSO.	Enable SSO with KaseyaOne
AC.L2-3.1.1[e]	KASEYA ensures all system actions are tied to authenticated user sessions via SSO.	CUSTOMER ensures proper identity governance; enforcement is handled by the PRODUCT.	Enable SSO with KaseyaOne
AC.L2-3.1.1[f]	KASEYA enforces access control by validating that only CUSTOMER-approved SaaS systems connected via the dashboard can transmit alerts.	CUSTOMER uses the PRODUCT dashboard to initiate and manage connections only for approved SaaS systems.	
AC.L2-3.1.2[a]	KASEYA defines default roles (MSP Admin, MSP User) with scoped permissions.	CUSTOMER may define additional roles and assign users based on operational needs.	
AC.L2-3.1.2[b]	KASEYA enforces role-based access control aligned with defined role permissions.	CUSTOMER assigns roles appropriately; PRODUCT enforces access based on role configuration.	

SAAS ALERTS CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AC.L2-3.1.5[a]	KASEYA identifies the initial privileged account as the CUSTOMER admin user account during environment provisioning.	CUSTOMER identifies any additional privileged accounts beyond the initial admin account and determines who will be assigned.	-
AC.L2-3.1.5[b]	KASEYA enforces role-based access controls within the PRODUCT to support least privilege; CUSTOMER must assign roles appropriately.	CUSTOMER assigns users to privileged accounts based on operational need, ensuring alignment with least privilege principles.	Role Based Access Control
AC.L2-3.1.5[c]	KASEYA designates general use of the PRODUCT—including account management and configuration—as a security function.	CUSTOMER recognizes that use of the PRODUCT constitutes access to security functions and governs access accordingly.	-
AC.L2-3.1.5[d]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER uses account management and role-based access control to ensure only authorized users can access security functions.	-
AC.L2-3.1.8[a]	KASEYA supplies single sign-on (SSO) capability, which can support integration with CUSTOMER identity sources.	CUSTOMER defines logon attempt limitations (e.g., lockout thresholds, retry intervals) within its identity source.	Enable SSO with KaseyaOne
AC.L2-3.1.8[b]	KASEYA does not implement or enforce logon attempt limitations; this is outside their operational scope.	CUSTOMER enforces these limitations through configuration of its identity provider integrated with the SSO.	-
AC.L2-3.1.11[a]	KASEYA defines session termination conditions (e.g., inactivity timeout) within the PRODUCT portal configuration.	Not applicable — CUSTOMER does not define or manage session termination conditions.	-
AC.L2-3.1.11[b]	KASEYA enforces automatic session termination and reauthentication after the defined inactivity period.	Not applicable — CUSTOMER does not control session enforcement mechanisms.	-

SAAS ALERTS CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AT.L2-3.2.2[a]	KASEYA does not define CUSTOMER-specific security roles or responsibilities.	CUSTOMER defines roles and responsibilities based on organizational structure and regulatory requirements.	-
AT.L2-3.2.2[b]	KASEYA does not assign CUSTOMER personnel to roles.	CUSTOMER assigns personnel to defined roles and ensures accountability.	-
AT.L2-3.2.2[c]	KASEYA develops training materials related to the use of the PRODUCT, which may support CUSTOMER training.	CUSTOMER ensures personnel receive appropriate training, potentially incorporating PROVIDER materials.	SaaS Alerts KB Home Page
AU.L2-3.3.1[a]	KASEYA defines event types captured in the PRODUCT portal.	CUSTOMER has no responsibility for audit logging functionality. Their only role is to connect SaaS systems to the PRODUCT, which triggers alert generation.	-
AU.L2-3.3.1[b]	KASEYA specifies the fields included in audit records (e.g., timestamp, user ID, action).	CUSTOMER has no responsibility for audit logging functionality. Their only role is to connect SaaS systems to the PRODUCT, which triggers alert generation.	-
AU.L2-3.3.1[c]	KASEYA ensures audit records are automatically generated based on system activity and alert ingestion.	CUSTOMER has no responsibility for audit logging functionality. Their only role is to connect SaaS systems to the PRODUCT, which triggers alert generation.	-
AU.L2-3.3.1[d]	KASEYA validates that audit records include all required fields to support traceability and analysis.	CUSTOMER has no responsibility for audit logging functionality. Their only role is to connect SaaS systems to the PRODUCT, which triggers alert generation.	-
AU.L2-3.3.1[e]	KASEYA defines a 400-day retention policy for audit logs stored within the PRODUCT.	CUSTOMER has no responsibility for audit logging functionality. Their only role is to connect SaaS systems to the PRODUCT, which triggers alert generation.	Log Retention

SAAS ALERTS CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AU.L2-3.3.1[f]	KASEYA enforces the 400-day retention period within the PRODUCT.	CUSTOMER has no responsibility for audit logging functionality. Their only role is to connect SaaS systems to the PRODUCT, which triggers alert generation.	Log Retention
AU.L2-3.3.2[a]	KASEYA confirms that audit records consistently include user attribution.	CUSTOMER has no responsibility for audit logging functionality. Their only role is to connect SaaS systems to the PRODUCT, which triggers alert generation.	-
AU.L2-3.3.2[b]	KASEYA defines an internal review process for evaluating logged event types.	CUSTOMER has no responsibility for audit logging functionality. Their only role is to connect SaaS systems to the PRODUCT, which triggers alert generation.	-
AU.L2-3.3.3[a]	KASEYA defines an internal process to review event types captured in the PRODUCT on an annual basis	CUSTOMER has no responsibility for audit logging functionality. Their only role is to connect SaaS systems to the PRODUCT, which triggers alert generation.	-
AU.L2-3.3.3[b]	KASEYA conducts an annual review of logged event types (e.g., failed logins, unauthorized activity, log clearing)	CUSTOMER has no responsibility for audit logging functionality. Their only role is to connect SaaS systems to the PRODUCT, which triggers alert generation.	-
AU.L2-3.3.3[c]	KASEYA updates the event types in the PRODUCT as needed based on findings from the annual review	CUSTOMER has no responsibility for audit logging functionality. Their only role is to connect SaaS systems to the PRODUCT, which triggers alert generation.	
AU.L2-3.3.8[a]	KASEYA enforces role-based access controls (RBAC) and encryption for PRODUCT logs	CUSTOMER has no responsibility for audit logging functionality. Their only role is to connect SaaS systems to the PRODUCT, which triggers alert generation.	

SAAS ALERTS CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AU.L2-3.3.8[b]	KASEYA applies write-once storage policies and integrity checks to prevent tampering	CUSTOMER has no responsibility for audit logging functionality. Their only role is to connect SaaS systems to the PRODUCT, which triggers alert generation.	
AU.L2-3.3.8[c]	KASEYA enforces retention policies and privileged access restrictions to prevent deletion	CUSTOMER has no responsibility for audit logging functionality. Their only role is to connect SaaS systems to the PRODUCT, which triggers alert generation.	
AU.L2-3.3.8[d]	KASEYA restricts access to logging infrastructure via network segmentation and authentication controls	CUSTOMER has no responsibility for audit logging functionality. Their only role is to connect SaaS systems to the PRODUCT, which triggers alert generation.	
AU.L2-3.3.8[e]	KASEYA uses configuration management and change control processes to prevent unauthorized changes	CUSTOMER has no responsibility for audit logging functionality. Their only role is to connect SaaS systems to the PRODUCT, which triggers alert generation.	
AU.L2-3.3.8[f]	KASEYA applies system hardening and privileged access restrictions to prevent deletion of logging tools	CUSTOMER has no responsibility for audit logging functionality. Their only role is to connect SaaS systems to the PRODUCT, which triggers alert generation.	
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.	
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.	
IA.L2-3.5.1[a]	KASEYA does not identify CUSTOMER users; user identity is managed via CUSTOMER's identity source.	CUSTOMER identifies all system users via its identity source.	

SAAS ALERTS CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
IA.L2-3.5.1[b]	KASEYA does not define or manage CUSTOMER-side service accounts or automation.	CUSTOMER identifies and manages service accounts and automated processes.	-
IA.L2-3.5.1[c]	KASEYA does not identify CUSTOMER devices; access is gated by CUSTOMER agent deployment.	CUSTOMER tracks and manages device identities through endpoint management and identity integration.	-
IA.L2-3.5.2[a]	KASEYA enables single sign-on (SSO) integration; actual authentication is performed by CUSTOMER identity source.	CUSTOMER enforces user authentication via its identity source.	Enable SSO with KaseyaOne
IA.L2-3.5.2[b]	KASEYA does not authenticate CUSTOMER-side processes; attribution is based on authenticated user context.	CUSTOMER authenticates service accounts and associated processes.	-
IA.L2-3.5.2[c]	KASEYA does not authenticate CUSTOMER devices; access is scoped by agent installation.	CUSTOMER enforces device authentication through its identity and endpoint management systems.	-
IA.L2-3.5.3[a]	KASEYA provisions the initial CUSTOMER admin account; all other privileged accounts are CUSTOMER-defined.	CUSTOMER identifies privileged accounts within its identity source.	Onboarding Guide
IA.L2-3.5.3[b]	KASEYA does not enforce MFA for local access; CUSTOMER identity source governs this.	CUSTOMER enforces MFA for local privileged access.	-
IA.L2-3.5.3[c]	KASEYA does not enforce MFA for network access; CUSTOMER identity source governs this.	CUSTOMER enforces MFA for network privileged access.	-
IA.L2-3.5.3[d]	KASEYA does not enforce MFA for non-privileged accounts; CUSTOMER identity source governs this.	CUSTOMER enforces MFA for non-privileged network access.	-
IA.L2-3.5.4[a]	KASEYA does not implement replay resistance; CUSTOMER identity source governs this.	CUSTOMER implements replay-resistant protocols (e.g., Kerberos, FIDO2, TLS) via its identity source.	-

SAAS ALERTS CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
IA.L2-3.5.5[a]	KASEYA does not define identifier reuse periods; CUSTOMER identity source governs this.	CUSTOMER defines identifier reuse periods in identity policy.	
IA.L2-3.5.5[b]	KASEYA does not enforce identifier reuse restrictions.	CUSTOMER enforces identifier reuse restrictions.	
IA.L2-3.5.6[a]	KASEYA does not define inactivity thresholds for identifiers.	CUSTOMER defines inactivity thresholds for disabling identifiers.	
IA.L2-3.5.6[b]	KASEYA does not enforce identifier deactivation.	CUSTOMER enforces identifier deactivation policies.	
IA.L2-3.5.7[a]	KASEYA does not define password complexity; CUSTOMER identity source governs this.	CUSTOMER defines password complexity policies.	
IA.L2-3.5.7[b]	KASEYA does not define character change requirements.	CUSTOMER defines character change requirements for password updates.	
IA.L2-3.5.7[c]	KASEYA does not enforce password complexity.	CUSTOMER enforces password complexity during creation.	
IA.L2-3.5.7[d]	KASEYA does not enforce character change requirements.	CUSTOMER enforces character change requirements during password updates.	
IA.L2-3.5.8[a]	KASEYA does not define password history policies.	CUSTOMER defines password history retention policies.	
IA.L2-3.5.8[b]	KASEYA does not enforce password reuse restrictions.	CUSTOMER enforces password reuse restrictions.	

SAAS ALERTS CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
IA.L2-3.5.9[a]	KASEYA does not enforce temporary-to-permanent password transitions.	CUSTOMER enforces temporary-to-permanent password change policies.	
IA.L2-3.5.10[a]	KASEYA does not store CUSTOMER passwords; authentication is handled by CUSTOMER identity source.	CUSTOMER ensures password storage uses cryptographic protection (e.g., hashing, salting).	
IA.L2-3.5.10[b]	KASEYA does not transmit CUSTOMER passwords; authentication occurs via CUSTOMER identity source.	CUSTOMER enforces secure transmission protocols (e.g., TLS).	
IA.L2-3.5.11[a]	KASEYA does not control authentication UI or flows; CUSTOMER identity source governs this.	CUSTOMER ensures authentication inputs (e.g., passwords) are obscured during entry and transmission.	
SC.L2-3.13.15[a]	KASEYA ensures secure, authenticated communication between the PRODUCT agent and the PRODUCT portal, and between the CUSTOMER and the PRODUCT portal.	CUSTOMER relies on the PROVIDER's implementation for session authenticity. No direct responsibility unless integrating with third-party systems or proxies.	

CONTACT US

404.307.7235

mcline@controlcase.com

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

ControlCase Kaseya