



# MYGLUE CUSTOMER RESPONSIBILITY MATRIX

Powered by ControlCase (C3PAO) and KASEYA

Mark Cline | SVP, Sales  
404.307.7235  
[mcline@controlcase.com](mailto: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)

# MYGLUE 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 user 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 user account. Additionally, the CUSTOMER must manage the CUSTOMER admin user account and identify any additional authorized users.	<a href="#">Enable SSO Login With MyGlue</a>
AC.L2-3.1.1[d]	KASEYA requires authentication through a username and password for the CUSTOMER admin user account, ensuring secure initial access to the system. Additionally, KASEYA offers a single sign-on PRODUCT to facilitate integration with the CUSTOMER's identity source.	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.	<a href="#">User and Global Access Roles</a>
AC.L2-3.1.2[a]	KASEYA defines roles (Administrator, Manager, Editor, Creator, Read-Only, Lite), each with a distinct set of permissions, ensuring a structured approach to user access control within the system. Additional roles can be created at the discretion of the CUSTOMER.	CUSTOMER defines roles, each with a distinct set of permissions, ensuring a structured approach to user access control within the system.	<a href="#">Account Settings for Managers &amp; Admins</a>
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 (default roles or customer-defined 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]	KASEYA is responsible for creating the CUSTOMER admin user 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 user account. Additionally, the CUSTOMER must manage the CUSTOMER admin user account and identify any additional authorized users.	<a href="#">Enable SSO Login With MyGlue</a>
AC.L2-3.1.5[b]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER is responsible for assigning user accounts to the appropriate roles (default roles or customer-defined roles) based on required permissions, ensuring that authorized users have access to the necessary transactions and functions within the system.	

# MYGLUE 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	<a href="#">Managing Employee Roles</a>
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)	<a href="#">Reports and Alerting</a>
AU.L2-3.3.1[b]		CUSTOMER defines, provides evidence of audit log content	<a href="#">Reports and Alerting</a>

# MYGLUE CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AC.L2-3.1.5[c]	<p>KASEYA incorporates the following security functions within the PRODUCT:</p> <ul style="list-style-type: none"> <li>- User Account Management – Supports the management of the CUSTOMER admin account and additional user accounts.</li> <li>- Configuration Management – Enables PRODUCT configuration to implement single sign-on via the CUSTOMER's own identity source, leveraging KASEYA's single sign-on Kaseya to ensure secure and controlled user access.</li> </ul>	CUSTOMER holds no responsibility in achieving this objective.	<a href="#">User and Global Access Roles</a>
AC.L2-3.1.5[d]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER is responsible for assigning user accounts to the appropriate roles (default roles or customer-defined roles) based on required permissions, ensuring that authorized users have access to the necessary transactions and functions within the system.	
AC.L2-3.1.6[a]	KASEYA makes a distinction between privileged and nonsecurity functions through role-based design. Nonsecurity functions are implicitly those available to non-privileged roles and exclude account management and configuration management.	CUSTOMER holds no responsibility in achieving this objective.	<a href="#">Enable SSO Login With MyGlue</a>
AC.L2-3.1.6[b]	KASEYA holds no responsibility in meeting this objective.	The CUSTOMER assigns users to roles appropriately, ensuring that individuals accessing nonsecurity functions do so using non-privileged accounts based on their responsibilities.	<a href="#">Enable SSO Login With MyGlue</a>
AC.L2-3.1.7[a]	KASEYA defines privileged functions within the PRODUCT as those related to user account management and configuration management, including the ability to configure single sign-on integration.	CUSTOMER interprets boundaries when assigning users to roles with or without access to account and configuration management.	<a href="#">User and Global Access Roles</a>
AC.L2-3.1.7[b]	KASEYA establishes that non-privileged users are those who do not have access to privileged functions within the PRODUCT.	CUSTOMER holds no responsibility in achieving this objective.	<a href="#">User and Global Access Roles</a>

# MYGLUE CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AC.L2-3.1.7[c]	KASEYA holds no responsibility in meeting this objective.	The CUSTOMER maintains role assignments to enforce access control, ensuring non-privileged users are not granted elevated privileges unless required.	
AC.L2-3.1.7[d]	KASEYA captures account management and configuration management activity in basic activity tracking audit logs. Some audit data may not be directly visible to the CUSTOMER, but the logging mechanisms exist to support accountability and forensic analysis.	CUSTOMER holds no responsibility in achieving this objective.	<a href="#">Enable SSO Login With MyGlue</a>
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.	<a href="#">Enable SSO Login With MyGlue</a>
AC.L2-3.1.11[a]	KASEYA, as part of the underlying SaaS security model, enables functionality within the PRODUCT that supports session termination based on inactivity. While the KASEYA does not define the period itself, it provides the configurable mechanism through which the CUSTOMER can define and enforce session timeout conditions.	The CUSTOMER is responsible for defining the period of inactivity that should trigger session termination. This is done by configuring the setting via the PRODUCT's portal.	
AC.L2-3.1.11[b]	The KASEYA ensures the PRODUCT enforces the configured session termination logic. Once the CUSTOMER defines the condition (e.g., inactivity timeout), the PRODUCT is responsible for automatically terminating the session accordingly.	The CUSTOMER ensures the defined session termination settings are properly configured and active within the PRODUCT's portal to support enforcement of the condition.	

# MYGLUE CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
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.	
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 (i.e., knowledge base articles, guides, and self-service resources).	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.	<a href="#">MyGlue KB Home</a>
AU.L2-3.3.1[a]	KASEYA defines and implements the audit logging framework within the PRODUCT. The following event types are captured: User Activities (User logins, access, record creation, edits, deletions and permission changes - activity logs).	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 User logins, access, record creation, edits, deletions and permission changes information.	CUSTOMER holds no responsibility in achieving this objective.	

# MYGLUE CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
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]	CUSTOMER holds no responsibility in achieving this objective.	CUSTOMER is responsible for defining retention requirements.	
AU.L2-3.3.1[f]	CUSTOMER holds no responsibility in achieving this objective.	CUSTOMER is responsible for determining if audit records are retained for the defined period.	
AU.L2-3.3.2[a]		CUSTOMER is responsible for determining if the content of the audit records support the ability to uniquely trace users to their actions	
AU.L2-3.3.2[b]		CUSTOMER is responsible for determining if audit records, once created, contain the defined content	

# MYGLUE CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AU.L2-3.3.3[a]	KASEYA establishes a structured process that mandates an annual review of logged events.	CUSTOMER is responsible for determining when to review audit records has been defined.	
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 is responsible for determining if audit records are reviewed per the defined schedule.	
AU.L2-3.3.3[c]	Based on an annual review, KASEYA updates the PRODUCT audit log configuration where necessary.	CUSTOMER is responsible for determining if event types need to be updated based on review.	
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].	<a href="#">Assigning User-Based GlueConnect Permissions</a>
AU.L2-3.3.8[b]	KASEYA ensures that audit information within the backend of PRODUCT's audit logs is safeguarded against unauthorized access, modification, or deletion, maintaining data integrity and compliance.	CUSTOMER holds no responsibility in achieving this objective.	<a href="#">Assigning User-Based GlueConnect Permissions</a>
AU.L2-3.3.8[c]	KASEYA ensures that audit information within the backend of PRODUCT's audit logs is safeguarded against unauthorized access, modification, or deletion, maintaining data integrity and compliance.	CUSTOMER holds no responsibility in achieving this objective.	<a href="#">Assigning User-Based GlueConnect Permissions</a>

# MYGLUE CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AU.L2-3.3.8[d]	KASEYA implements security controls to protect audit logging tools within the backend of the PRODUCT, preventing unauthorized access, modification, or removal to ensure continuous logging functionality.	CUSTOMER holds no responsibility in achieving this objective.	<a href="#">Assigning User-Based GlueConnect Permissions</a>
AU.L2-3.3.8[e]	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.	
AU.L2-3.3.8[f]	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.	
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]	See KASEYA responsibility for AC.L2-3.1.1[a].	See CUSTOMER responsibility for AC.L2-3.1.1[a].	

# MYGLUE CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
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].	<a href="#">User and Global Access Roles</a>
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].	<a href="#">User and Global Access Roles</a>
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.	<a href="#">Enable SSO Login With MyGlue</a>
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.	<a href="#">Enable SSO Login With MyGlue</a>
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.	
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.	

# MYGLUE CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
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.	
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.	
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.	
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.	
IA.L2-3.5.7[a]		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 change of character requirements. Then, password complexity is entirely enforced by identity provider (e.g., Azure AD, Okta)	
IA.L2-3.5.7[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 defining password change of character requirements.	

# MYGLUE 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.	
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.	
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.	
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.	
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.	
IA.L2-3.5.10[a]	Passwords (both user account credentials and stored secrets) are cryptographically protected at rest, consistent with standard SaaS security practices.	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.	

# MYGLUE CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
IA.L2-3.5.10[b]	Passwords and all other sensitive data are encrypted during transmission using standard HTTPS/TLS protocols.	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.	
IA.L2-3.5.11[a]	Authentication information (like usernames and passwords) is protected during the authentication process, mainly via encryption in transit.	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.	<a href="#">Enable SSO Login With MyGlue</a>
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.	<a href="#">Security &amp; Encryption</a>

# CONTACT US



404.307.7235



[mcline@controlcase.com](mailto:mcline@controlcase.com)



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

