CAIQ Lite CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE LITE v4.0.3

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	No		Independent audit and assurance assessments are not currently conducted for the Application or Alteris Edge. FieldSync (the "Application") is hosted on Atlassian Forge, and Alteris Edge relies on Atlassian's platform-level security and compliance controls where applicable.		A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Independent Assessments	Audit & Assurance
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	No		Alteris Edge does not currently perform independent audit and assurance assessments based on formal risk-based audit plans and policies. The Application is hosted on Atlassian Forge.		A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	Risk Based Planning Assessment	
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	No		Alteris Edge does not currently conduct formal compliance verification audits against all applicable standards, regulations, legal, contractual, and statutory requirements. Compliance responsibilities for the underlying Atlassian Forge platform are managed by Atlassian.		A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	Requirements Compliance	
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	No		Alteris Edge does not maintain a formal risk-based corrective action program for audit findings because independent audits are not currently performed.		A&A-06	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.	Remediation	
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	No		Alteris Edge does not formally review and report remediation status for audit findings because independent audits are not currently performed.					
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	No		Alteris Edge does not maintain documented baseline security requirements for applications. The Application is developed and hosted on Atlassian Forge, which provides platform-level security controls.		AIS-02	Establish, document and maintain baseline requirements for securing different applications.	Application Security Baseline Requirements	Application & Interface Security
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	No		Alteris Edge does not maintain a formally defined and documented Secure Software Development Lifecycle (SDLC) process. Development and deployment activities follow Atlassian Forge platform requirements and security practices.		AIS-04	Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	Secure Application Design and Development	
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	No		Alteris Edge does not maintain formally documented strategies and capabilities for secure, standardized, and compliant application code deployment. Deployments are performed through Atlassian Forge deployment mechanisms.		AIS-06	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Automated Secure Application Deployment	
AIS-06.2	Is the deployment and integration of application code automated where possible?	Yes		Application deployment and integration are performed using Atlassian Forge's automated deployment capabilities.					
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	No		Alteris Edge does not maintain a formal documented process for remediation of application security vulnerabilities. Security issues identified during development are addressed as needed.		AIS-07	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.	Application Vulnerability Remediation	
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	No		Alteris Edge does not use automated vulnerability remediation processes for application security vulnerabilities.					
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	NA		The Application and Alteris Edge do not maintain independent business continuity or operational resilience policies. These are managed by Atlassian Forge for the hosting environment.		BCR-01	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually.	Business Continuity Management Policy and Procedures	
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	NA		The Application and Alteris Edge do not maintain independent business continuity policies or procedures. Business continuity for the application is handled by Atlassian Forge.					
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	NA		The Application and Alteris Edge do not develop independent business continuity or resiliency strategies. Atlassian Forge ensures resiliency for its platform.		BCR-02	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.	Risk Assessment and Impact Analysis	
BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	NA		The Application does not implement independent business continuity strategies. Atlassian Forge provides strategies to ensure platform resiliency.		BCR-03	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.	Business Continuity Strategy	

BCR-08.1	Is cloud data periodically backed up?	Yes	Data and application assets supporting the Application are stored on managed platforms that perform backup and recovery activities, including Atlassian Forge and GitHub.	BCR-08	Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.	Backup	Business Continuity Management and Operational Resilience
BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	Yes	Backup confidentiality, integrity, and availability controls are provided by the managed platforms used to operate and develop the Application, including Atlassian Forge and GitHub.				
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	Backup restoration capabilities are provided by the managed platforms supporting the Application, including Atlassian Forge and GitHub.				
BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	No	The Application and Alteris Edge do not maintain independent disaster response plans. Atlassian Forge manages disaster recovery for the hosting platform.	BCR-09	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.	Disaster Response Plan	
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	NA	The Application and Alteris Edge do not maintain disaster response plans. Atlassian Forge ensures the Forge platform's disaster recovery plans are reviewed and updated as needed.				
CCC-01.1	Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)?	NA	The Application and Alteris Edge do not maintain independent risk management policies. These policies are established and maintained by Atlassian for the Forge platform, ensuring compliance with industry standards.	CCC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.	Change Management Policy and Procedures	Change Control and Configuration Management
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	NA	Policies and procedures for organizational changes are reviewed and updated by Atlassian Forge as part of their platform management. The Application relies on this framework for compliance.				
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	No	Alteris Edge does not maintain a formally defined and documented quality change control, approval, and testing process with established baselines, testing, and release standards. Changes are tested and deployed through Atlassian Forge development and deployment workflows.	CCC-02	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.	Quality Testing	
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	No	Alteris Edge does not maintain a formal process restricting unauthorized addition, removal, update, and management of organizational assets. Access to Atlassian Forge, GitHub, and other services is protected through account authentication and access controls.	CCC-04	Restrict the unauthorized addition, removal, update, and management of organization assets.	Unauthorized Change Protection	
CCC-05.1	Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs?	NA	The Application does not maintain independent SLAs. Change provisions and authorization requests are managed by Atlassian Forge within their established platform agreements.	CCC-05	Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.	Change Agreements	
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	No	Alteris Edge does not maintain formally documented change management baselines for authorized changes to organizational assets.	CCC-06	Establish change management baselines for all relevant authorized changes on organization assets.	Change Management Baseline	
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	No	Alteris Edge does not implement automated detection and proactive notification processes for deviations from established change management baselines.	CCC-07	Implement detection measures with proactive notification in case of changes deviating from the established baseline.	Detection of Baseline Deviation	
CCC-09.1	Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?	Yes	Source code for the Application is maintained in GitHub with version control and revision history. Changes can be reverted and prior known-good versions can be redeployed if errors or security concerns are identified. Further, the Application relies on Atlassian Forge's rollback mechanisms, which allow customer iinstallations to revert to a known 'good state' in case of errors or security concerns.	CCC-09	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.	Change Restoration	

CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	NA	Cryptography, encryption, and key management policies for The Application are managed by Atlassian Forge, ensuring compliance with approved standards and regulatory requirements.	CEK-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually.	Encryption and Key Management Policy and Procedures	Cryptography, Encryption & Key Management
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	NA	Atlassian Forge is responsible for reviewing and updating cryptography, encryption, and key management policies annually, ensuring they align with current standards.				
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	NA	Roles and responsibilities related to cryptography, encryption, and key management are defined and implemented by Atlassian Forge. The Application inherits these practices.	CEK-02	Define and implement cryptographic, encryption and key management roles and responsibilities.	CEK Roles and Responsibilities	
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes	Data transmitted to and from the Application is protected using HTTPS/TLS. Data stored within Atlassian Forge is protected using Atlassian-managed encryption controls.	CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.	Data Encryption	
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Yes	The Application relies on Atlassian Forge encryption controls and cryptographic implementations for protection of data at rest and in transit.	CEK-04	Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.	Encryption Algorithm	
CEK-05.1	Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	NA	Cryptography, encryption, and key management changes for The Application are managed by Atlassian Forge under their established change management procedures.	CEK-05	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.	Encryption Change Management	
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	NA	Cryptographic key generation and management for the Application's hosting environment are performed by Atlassian as part of the Atlassian Forge platform.	CEK-10	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	Key Generation	
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Yes	Atlassian Forge enforces key rotation based on cryptoperiods that comply with information disclosure risks and legal requirements, ensuring secure key management for The Application.	CEK-12	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.	Key Rotation	
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?	Yes	Cryptographic keys are revoked and removed by Atlassian Forge per their established processes when a key is compromised or no longer needed, ensuring compliance with legal and regulatory requirements.	CEK-13	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.	Key Revocation	
CEK-14.1	Are processes, procedures and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions?	Yes	Atlassian Forge implements processes and procedures for key destruction, including those stored in hardware security modules (HSMs), aligning with secure practices and regulatory provisions.	CEK-14	Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements.	Key Destruction	
DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	NA	The Application and Alteris Edge do not maintain physical offices or facilities for hosting or operations. These responsibilities are managed by Atlassian for their data centers and cloud infrastructure.	DCS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually.	Secure Area Policy and Procedures	Datacenter Security
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	NA	The Application and Alteris Edge do not operate physical offices or facilities. Atlassian is responsible for reviewing and updating security policies for their data centers and cloud environments.				
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	NA	The Application and Alteris edge do not manage physical or logical assets independently. Asset management and risk classification are handled by Atlassian for their infrastructure supporting the Forge platform.	DCS-05	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.	Assets Classification	
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	NA	Physical and logical asset tracking for The Application is managed by Atlassian, which catalogs and tracks all relevant assets within their secured systems for the Forge platform.	DCS-06	Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.	Assets Cataloguing and Tracking	

DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	NA	The Application does not independently manage data lifecycle policies. These responsibilities are handled by Atlassian Forge, which enforces compliance with applicable laws and standards.	DSP-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.	Security and Privacy Policy and Procedures	
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	NA	Data security and privacy policies are reviewed and updated by Atlassian Forge. The Application relies on these platform-level policies.				
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	No	Alteris Edge does not maintain a formal data inventory for sensitive and personal information processed by the Application.	DSP-03	Create and maintain a data inventory, at least for any sensitive data and personal data.	Data Inventory	
DSP-04.1	Is data classified according to type and sensitivity levels?	No	Alteris Edge does not maintain a formal data classification program that classifies data according to type and sensitivity levels.	DSP-04	Classify data according to its type and sensitivity level.	Data Classification	
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	No	Alteris Edge does not maintain formal data flow documentation identifying what data is processed and where it is stored or transmitted.	DSP-05	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.	Data Flow Documentation	
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	NA	Formal data flow documentation is not maintained by Alteris Edge.				
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	No	Alteris Edge does not maintain formal documentation assigning ownership and stewardship responsibilities for personal and sensitive data.	DSP-06	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.	Data Ownership and Stewardship	Data Security and Privacy Lifecycle Management
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	NA	Alteris Edge does not maintain formal data ownership and stewardship documentation.				
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	No	Alteris Edge does not maintain a formal security-by-design program or documented process. The Application is developed on Atlassian Forge, which incorporates platform security controls.	DSP-07	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.	Data Protection by Design and Default	
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	No	Alteris Edge does not maintain a formal privacy-by-design program or documented process.	DSP-08	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	Data Privacy by Design and Default	
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	NA	The Application does not provide configurable privacy settings that are managed by Alteris Edge.				
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	No	Alteris Edge does not maintain formal documented processes, procedures, and technical measures governing the transfer of personal or sensitive data.	DSP-10	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Sensitive Data Transfer	
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	No	Alteris Edge does not maintain formal processes and procedures to support data subject requests for access, modification, or deletion of personal data. The Application is not intended to collect or store personal data requiring such requests.	DSP-11	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.	Personal Data Access, Reversal, Rectification and Deletion	

DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?	No	Alteris Edge does not maintain formal documented processes to ensure personal data is processed according to applicable laws, regulations, and declared purposes. The Application is not designed to collect or process personal data beyond information required for operation within Atlassian Cloud.	DSP-12	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	Limitation of Purpose in Personal Data Processing	
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	No	Alteris Edge does not maintain formal documented processes governing the transfer and sub-processing of personal data. The Application processes data within Atlassian Cloud using Atlassian Forge and is not designed to transfer customer Jira data outside Atlassian-managed services.	DSP-13	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	Personal Data Sub-processing	
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	No	Alteris Edge does not maintain formal documented procedures for disclosing sub-processor access to personal or sensitive data. Information regarding Atlassian sub-processors is provided through Atlassian documentation and agreements.	DSP-14	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.	Disclosure of Data Sub-processors	
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	No	Alteris Edge does not maintain formal documented data retention, archiving, and deletion policies. Data retention and storage for the Application are primarily governed by Atlassian platform capabilities and customer-controlled Jira data management practices.	DSP-16	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	Data Retention and Deletion	
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	No	Alteris Edge does not maintain formal documented processes and procedures for protecting sensitive data throughout its lifecycle. The Application relies on Atlassian Forge security controls and encrypted communications.	DSP-17	Define and implement, processes, procedures and technical measures to protect sensitive data throughout it's lifecycle.	Sensitive Data Protection	
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	NA	Alteris Edge does not independently specify or document physical data processing or backup locations. Data location information for Atlassian-hosted services is provided by Atlassian.	DSP-19	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.	Data Location	
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	No	Alteris Edge does not maintain a formal information governance program with documented policies and procedures.	GRC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.	Governance Program Policy and Procedures	
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	NA	Alteris Edge does not maintain formal information governance policies and procedures.				
GRC-02.1	Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?	No	Alteris Edge does not maintain a formal, documented, leadership-sponsored enterprise risk management program.	GRC-02	Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.	Risk Management Program	Governance, Risk and Compliance
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	No	Alteris Edge does not maintain documented governance program roles and responsibilities.	GRC-06	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	Governance Responsibility Model	
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	No	Alteris Edge does not maintain formal documentation identifying and mapping all applicable standards, regulations, legal, contractual, and statutory requirements.	GRC-07	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.	Information System Regulatory Mapping	
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	No	Alteris Edge does not maintain formal documented clean desk or unattended workspace policies. Developer devices are protected through device authentication and automatic screen locking.	HRS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually.	Clean Desk Policy and Procedures	
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	NA	Alteris Edge does not maintain formal documented clean desk or unattended workspace policies.				
HRS-04.1	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?	No	Alteris Edge does not maintain formal documented policies and procedures for protecting information accessed, processed, or stored at remote locations. Security controls include authenticated devices, automatic screen locking, endpoint protection, operating system updates, and MFA where supported.	HRS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually.	Remote and Home Working	Human Resources

HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	NA	Alteris Edge does not maintain formal documented remote work policies and procedures.	HRS-04		Policy and Procedures	
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	No	Alteris Edge does not currently have an independent security awareness training program. Atlassian Forge ensures secure operations at the platform level.	HRS-11	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.	Security Awareness Training	
HRS-11.2	Are regular security awareness training updates provided?	No	Alteris Edge does not provide regular security awareness training updates. Security practices and awareness for the platform are managed by Atlassian Forge.				
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	No	Alteris Edge does not maintain formal documented identity and access management policies and procedures. Access to development and business systems is controlled through account authentication and MFA where supported.	IAM-01	Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually.	Identity and Access Management Policy and Procedures	
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	N/A	Alteris Edge does not maintain formal documented identity and access management policies and procedures.				
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes	System identities and access levels for the Application are managed through Atlassian Cloud and Atlassian Forge access controls. Access to Alteris Edge-managed systems is controlled through individual authenticated accounts.	IAM-03	Manage, store, and review the information of system identities, and level of access.	Identity Inventory	
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	No	Alteris Edge does not maintain a formal separation-of-duties program. As a one-person organization, separation of duties is generally not applicable.	IAM-04	Employ the separation of duties principle when implementing information system access.	Separation of Duties	
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes	Access to systems used by Alteris Edge is limited to authorized accounts. The Application also relies on Atlassian Cloud and Atlassian Forge access control mechanisms that restrict access based on assigned permissions.	IAM-05	Employ the least privilege principle when implementing information system access.	Least Privilege	
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	No	Alteris Edge does not maintain a formal documented user access provisioning process.	IAM-06	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	User Access Provisioning	Identity & Access Management
IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	No	Alteris Edge does not maintain a formal documented process for modifying or revoking user access following role or identity changes.	IAM-07	De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.	User Access Changes and Revocation	
IAM-08.1	Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?	No	Alteris Edge does not perform formal documented access reviews or revalidation activities at defined intervals.	IAM-08	Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.	User Access Review	
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	Yes	Atlassian Forge defines and enforces segregation of privileged access roles, ensuring distinct administrative data access, encryption, key management, and logging capabilities for The Application.	IAM-09	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated.	Segregation of Privileged Access Roles	
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Yes	Privileged access roles in Atlassian Forge are granted for limited periods as part of their access management protocols, ensuring security for hosted applications.	IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.	Management of Privileged Access Roles	
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	Yes	Atlassian Forge prevents the culmination of segregated privileged access through enforced access control policies and monitoring practices.				

IAM-14.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?	Yes	Authentication processes, including multifactor authentication, are defined and implemented by Atlassian Forge to ensure secure access for least-privileged users and sensitive data.	IAM-14	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	Strong Authentication	
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Yes	Atlassian Forge adopts digital certificates or equivalent alternatives to achieve secure system identity management for applications like The Application.				
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	No	Alteris Edge does not maintain formal documented policies and procedures governing communications between application services or APIs. The Application communicates using Atlassian platform APIs and services.	IPY-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually.	Interoperability and Portability Policy and Procedures	Interoperability & Portability
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	No	Alteris Edge does not maintain formal documented policies and procedures for information processing interoperability.				
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	No	Alteris Edge does not maintain formal documented policies and procedures for application development portability.				
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	No	Alteris Edge does not maintain formal documented policies and procedures governing information and data exchange, usage, portability, integrity, and persistence.				
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	NA	Alteris Edge does not maintain formal interoperability and portability policies and procedures.				
IVS-03.1	Are communications between environments monitored?	Yes	Communications between environments are monitored by Atlassian Forge as part of their platform security practices.		Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.		

IVS-03.2	Are communications between environments encrypted?	Yes	Atlassian Forge encrypts communications between environments to ensure secure data transmission for applications like The Application.	IVS-03		Network Security	Infrastructure & Virtualization Security
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes	Communications between environments are restricted to authenticated and authorized connections, as enforced by Atlassian Forge's platform security protocols.				
IVS-03.4	Are network configurations reviewed at least annually?	Yes	Network configurations are reviewed and maintained by Atlassian Forge to ensure compliance with security and operational requirements.				
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Yes	Atlassian Forge justifies and documents all allowed services, protocols, ports, and compensating controls as part of its platform network configuration.				
IVS-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	Yes	Every host and guest OS, hypervisor, and infrastructure control plane is hardened and supported by Atlassian Forge's technical controls to maintain a security baseline.	IVS-04	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.	OS Hardening and Base Controls	
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	Yes	Atlassian Forge designs and configures its platform to ensure segmentation, segregation, monitoring, and restriction of tenant access, safeguarding applications like The Application.	IVS-06	Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants.	Segmentation and Segregation	
IVS-07.1	Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?	Yes	Atlassian Forge utilizes secure and encrypted communication channels with up-to-date approved protocols for migrating services and data in cloud environments.	IVS-07	Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.	Migration to Cloud Environments	
IVS-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?	Yes	Atlassian Forge implements defense-in-depth techniques and procedures for detecting and responding to network-based attacks, benefiting applications like The Application.	IVS-09	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.	Network Defense	
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Logging and monitoring policies are established, maintained, and managed by Atlassian Forge for hosted applications, including The Application.	LOG-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.	Logging and Monitoring Policy and Procedures	Logging and Monitoring
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes	Atlassian Forge reviews and updates logging and monitoring policies regularly to ensure compliance with industry standards.				
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes	Access to audit logs is restricted to authorized personnel, with records maintained to ensure accountability, as part of Atlassian Forge's managed services.	LOG-04	Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.	Audit Logs Access and Accountability	
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Yes	Security audit logs are monitored by Atlassian Forge to detect unusual activity and maintain security for hosted applications like The Application.	LOG-05	Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.	Audit Logs Monitoring and	

LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes	Atlassian Forge follows processes to review detected anomalies and take timely actions to mitigate potential security risks.	LOG-05		Response	
SEF-03.1	Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	No	Alteris Edge does not maintain a formal documented security incident response plan. Security incident response processes for the Atlassian Forge platform are managed by Atlassian.	SEF-03	'Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted.'	Incident Response Plans	Security Incident Management, E-Discovery, & Cloud Forensics
SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	NA	Alteris Edge does not maintain a formal documented security incident response plan.	SEF-04	Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.	Incident Response Testing	
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	No	Alteris Edge does not maintain formal documented security breach notification procedures. Security incident notification obligations related to the Atlassian Forge platform are managed by Atlassian.	SEF-07	Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.	Security Breach Notification	
SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	No	Alteris Edge does not maintain formal documented procedures governing security breach reporting.				
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	No	Alteris Edge does not maintain a documented Shared Responsibility Model (SSRM) governing its supply chain relationships.	STA-02	Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.	SSRM Supply Chain	Supply Chain Management, Transparency, and Accountability
STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	No	Alteris Edge does not maintain formal documentation mapping CSA CCM control ownership through a Shared Responsibility Model.	STA-04	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.	SSRM Control Ownership	
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	No	Alteris Edge does not maintain a formal inventory of all supply chain relationships.	STA-07	Develop and maintain an inventory of all supply chain relationships.	Supply Chain Inventory	
TVM-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Policies to protect against malware on managed assets are implemented and maintained by Atlassian Forge, ensuring secure hosting for The Application.	TVM-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually.	Malware Protection Policy and Procedures	Threat & Vulnerability Management
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Yes	Atlassian Forge regularly reviews and updates asset management and malware protection policies to comply with industry standards.				
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk)?	Yes	Processes for scheduled and emergency responses to vulnerabilities are defined and managed by Atlassian Forge, ensuring timely action.	TVM-03	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.	Vulnerability Remediation Schedule	
TVM-04.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	Yes	Detection tools and threat signatures are updated weekly (or more frequently) by Atlassian Forge as part of their robust security operations.	TVM-04	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.	Detection Updates	
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Yes	Atlassian Forge evaluates vulnerability detection processes monthly to ensure the security of managed assets.	TVM-07	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.	Vulnerability Identification	
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes	Atlassian Forge implements a process to track and report vulnerability identification and remediation, ensuring stakeholders are informed.	TVM-09	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.	Vulnerability Management Reporting	

UEM-02.1	Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?	No	Alteris Edge does not maintain a formal documented list of approved services, applications, and application sources for endpoint use.	UEM-02	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.	Application and Service Approval	Universal Endpoint Management
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	No	Alteris Edge does not maintain a formal inventory of all endpoints used to store and access company data.	UEM-04	Maintain an inventory of all endpoints used to store and access company data.	Endpoint Inventory	
UEM-05.1	Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?	No	Alteris Edge does not maintain formal documented endpoint management policies, procedures, and technical controls. Developer endpoints are protected through operating system security controls, endpoint protection, MFA where supported, and regular security updates.	UEM-05	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.	Endpoint Management	
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes	Alteris Edge requires password-protected access to developer endpoints and utilizes operating system security controls, including automatic screen locking after periods of inactivity. Access to development systems, source code repositories, and Atlassian administration interfaces requires authenticated user access.	UEM-06	Configure all relevant interactive-use endpoints to require an automatic lock screen.	Automatic Lock Screen	
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Yes	Alteris Edge utilizes endpoint protection technologies provided by the operating system platform, including anti-malware detection, threat protection, and automatic security updates. Developer endpoints are maintained with current security patches and protections appropriate to the operating environment.	UEM-09	Configure managed endpoints with anti-malware detection and prevention technology and services.	Anti-Malware Detection and Prevention	
UEM-10.1	Are software firewalls configured on managed endpoints?	Yes	Alteris Edge utilizes operating system firewall capabilities on developer endpoints to restrict unauthorized network access. Endpoint firewall protections are managed through native operating system security controls.	UEM-10	Configure managed endpoints with properly configured software firewalls.	Software Firewall	
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	No	Alteris Edge does not currently maintain a centralized device management platform capable of performing remote data deletion on managed endpoints. Company data is primarily stored on local managed endpoints, within managed cloud platforms, including Atlassian Forge, GitHub, and other hosted services that maintain their own access controls and data protection mechanisms.	UEM-13	Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.	Remote Wipe	

End of Standard

© Copyright 2024 Cloud Security Alliance - All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance "Consensus Assessments Initiative Questionnaire Lite (CAIQLite) Version 4.0.3" at http://www.cloudsecurityalliance.org subject to the following: (a) the Consensus Assessments Initiative Questionnaire Lite v4.0.3 may be used solely for your personal, informational, non-commercial use; (b) the Consensus Assessments Initiative Questionnaire Lite v4.0.3 may not be modified or altered in any way; (c) the Consensus Assessments Initiative Questionnaire Lite v4.0.3 may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Consensus Assessments Initiative Questionnaire Lite v4.0.3 as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance Consensus Assessments Initiative Questionnaire Lite Version 4.0.3. If you are interested in obtaining a license to this #material for other usages not addresses in the copyright notice, please contact info@cloudsecurityalliance.org.