CLEARLANE

CAIQ-Lite v4.1.0 — Security self-assessment

Clearlane apps for Jira and Confluence Cloud (Atlassian Forge, Runs on Atlassian) · Completed 4 November 2026 · Self-assessment, not audited

Scope. All Clearlane Marketplace apps. They run on Atlassian's Forge platform: code and stored data stay inside the customer's Atlassian site; Clearlane operates no servers and keeps no copy of customer content. Publisher: Maxime Ragionieri EI (brand: Clearlane Apps), a sole proprietorship registered in France, run by its founder, Maxime Ragionieri; development uses an AI coding assistant under his supervision.
How to read it. "Yes" means the part of the control is in place, "No" that it is not (yet), "NA" that it does not apply to this service. Ownership follows the CSA Shared Security Responsibility Model: "3rd-party" is Atlassian, which hosts the apps; "CSC" is the customer.
Full questionnaire. The same answers, with the other questions of the full CAIQ v4.1, are published in the CSA STAR Registry (STAR Level 1, self-assessment): https://cloudsecurityalliance.org/star/registry/clearlane-apps/services/clearlane-apps-for-jira-and-confluence
Answers. Yes 97 | No 38 | NA 3 of 138 questions.

ID	Question	Answer · Owner	How Clearlane meets it
Audit & Assurance			
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	**No** CSP-owned	Maxime Ragionieri EI (brand: Clearlane Apps), a sole proprietorship, has had no independent audit or certification of its own (no SOC 2 or ISO 27001). The apps run on Atlassian Forge (Runs on Atlassian); Atlassian holds its own independent audits for its cloud platform, and customers can obtain the reports and their scope from Atlassian.
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies, and in response to significant changes or emerging risks?	**No** CSP-owned	No independent assessment of Clearlane itself so far (see A&A-02.1). Each release is reviewed internally before production: automated tests, dependency audit and a separate automated security code review, repeated until no high or medium finding remains.
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	**No** CSP-owned	No audit is performed (see A&A-02.1). Before each release, the release protocol runs forge lint, a dependency audit, an access test with an account without rights and a security code review.
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	**Yes** CSP-owned	Findings from internal security reviews, automated dependency audits and the weekly check are recorded in a security register with a severity and a deadline taken from Atlassian's Security Bug Fix Policy, and tracked until fixed in production.
A&A-06.2	Is the remediation status of audit findings regularly reviewed and reported to relevant stakeholders?	**Yes** CSP-owned	Open findings are checked every week, with the dependency audit and Atlassian's security tickets, against the security register. Customers affected by a confirmed issue are informed; fixes are listed in the release notes.
Application & Interface Security			
AIS-02.1	Are baseline requirements to secure applications established, documented, and maintained?	**Yes** CSP-owned	Security baseline published in the security policy (least-privilege permissions, actions taken with the user's own permissions, no network call outside Atlassian, nothing sensitive in logs, signing passwords hashed) and enforced for every app by the documented release protocol (blocking quality checks, forge lint, dependency audit, access test with an account without rights, security code review).
AIS-04.1	Is a secure SDLC process defined and implemented for application requirements analysis, planning, design, development, testing, deployment, and operation per organizationally designed security requirements?	**Yes** CSP-owned	Documented release protocol: automated tests (including Forge limits, simultaneous users and large volumes), blocking quality checks, forge lint, dependency audit, test on a real Atlassian development site, access test with an account without rights, and a separate automated security code review, repeated until no high or medium finding remains; production deployment needs the founder's written approval. Code is written with AI coding assistance under the founder's supervision.
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	**Yes** CSP-owned	Code is deployed only through the Forge CLI to Atlassian's platform, from a versioned source archive, after the release checklist. Atlassian controls how versions reach customer sites (minor versions cannot add permissions).
AIS-06.2	Is the deployment and integration of application code automated where possible?	**Yes** Shared CSP and 3rd-party	Build, tests, linting and deployment run through scripted commands (Forge CLI, npm). Production deployments need the founder's written approval.
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	**Yes** CSP-owned	Vulnerabilities are fixed within the deadlines of Atlassian's Security Bug Fix Policy for Marketplace apps (critical 10 days, high 4 weeks, medium 12 weeks, low 25 weeks), tracked in the security register.

ID	Question	Answer · Owner	How Clearlane meets it
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	**No** CSP-owned	Detection is automated (npm audit before each release and in a weekly scheduled check). Fixes are applied under the founder's supervision and verified by the automated release checks.
AIS-08.1	Are processes, procedures, and technical measures defined and implemented to secure APIs?	**Yes** Shared CSP and 3rd-party	The apps expose no public API of their own. Calls between an app's screens and its server functions go through Forge, which authenticates the user. Most calls to Jira and Confluence are made with the user's own permissions; the few made with the app's own access are listed in the security policy.
AIS-08.2	Are reviews and updates for any improvements conducted at least annually, or upon significant changes?	**Yes** CSP-owned	API use is reviewed in the security code review of every release that changes it.
Business Continuity Management and Operational Resilience			
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	**No** Shared CSP and 3rd-party	No formal business continuity policy yet. In place: the apps run on Atlassian's Forge platform and do not depend on any Clearlane server; source code and release archives are backed up to a private Bitbucket repository after each work step, with a restore script; customers are told at least 90 days in advance if an app is ever withdrawn.
BCR-01.2	Are the policies and procedures reviewed and updated at least annually, or upon significant changes?	**No** CSP-owned	No formal policy to review yet (see BCR-01.1).
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	**No** CSP-owned	No formal business impact analysis. The main risks for a one-person publisher (loss of the workstation, loss of account access, unavailability of the founder) are limited by design: the apps never depend on Clearlane servers and customer records stay in the customer's site.
BCR-02.2	Are the risk assessment and impact analysis reviewed and updated at least annually or upon significant changes?	**No** CSP-owned	See BCR-02.1.
BCR-03.1	Are strategies being established to reduce the impact of business disruptions, and are resiliency and recovery from business disruptions being improved?	**Yes** CSP-owned	Off-site backup of all source code and release archives with a restore script, and evidence exports (PDF, CSV) in the quality and cyber apps so customers keep their records independently of Clearlane.
BCR-08.1	Are backups performed periodically?	**Yes** Shared CSP and 3rd-party	Clearlane backs up all source code and release archives to a private Bitbucket repository after each work step. Data the apps keep sits in Atlassian's Forge storage, under Atlassian's own arrangements; Clearlane holds no copy of it. Customers can keep their own copies of records through the PDF and CSV evidence exports of the quality and cyber apps.
BCR-08.2	Is the confidentiality, integrity, and availability of the backup ensured?	**Yes** CSP-owned	Clearlane's code backups are kept in a private Bitbucket repository reachable only by the founder's account, protected by two-step verification, and its access key; release archives are checked every week against their recorded fingerprints.
BCR-08.3	Can backups be restored appropriately for resiliency?	**Yes** CSP-owned	Code and release archives are restored from the Bitbucket backup with a restore script. Clearlane cannot restore app data in Forge storage, which is Atlassian's.
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** Shared CSP and 3rd-party	No formal disaster response plan. Disasters affecting hosting are handled by Atlassian for its platform. For Clearlane's own part, code and release archives can be restored from the off-site Bitbucket backup with a restore script (BCR-08.3).
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	**No** CSP-owned	See BCR-09.1.
Change Control and Configuration Management			
CCC-01.1	Are policies and procedures for managing the risks associated with applying changes to assets owned, controlled, or used by the organization established, documented, approved, communicated, applied, evaluated, and maintained?	**Yes** CSP-owned	Documented change management for the apps: every change follows the release checklist (tests, review, development site, production approval) and is announced in the release notes.
CCC-01.2	Are the policies and procedures reviewed and updated at least annually, or upon significant changes?	**Yes** CSP-owned	Updated upon significant changes (for example, the validation impact line added to release notes on 28 October 2026). No yearly review has fallen due yet.

ID	Question	Answer · Owner	How Clearlane meets it
CCC-02.1	Is a defined quality change control, approval and testing process, incorporating baselines, testing, and release standards, established, maintained and implemented?	**Yes** CSP-owned	Quality change control: automated test suites, blocking quality checks, real test on a development site, a separate automated security code review, repeated until no high or medium finding remains, and release notes. For the quality and cyber apps, release notes state the validation impact, and functional changes to signed records, signatures or approval workflows are announced at least 30 days in advance.
CCC-04.1	Is a procedure to authorize the addition, removal, update, and management of assets owned, controlled, or used by the organization, implemented and enforced?	**Yes** CSP-owned	Only the founder's accounts can add, change or remove apps, versions, permissions and accounts; production changes need his written approval. Atlassian requires the customer's administrator to approve any version that adds a permission.
CCC-05.1	Are provisions to limit changes directly impacting service customer-owned environments (tenants) to explicitly authorized requests included within service level agreements?	**No** Shared CSP and CSC	Clearlane offers no SLA. Atlassian applies minor versions automatically; a version that adds a permission or an outside connection waits for the customer administrator's approval. Changes to signed records, signatures or approval workflows are announced at least 30 days in advance, and the apps change customer data only through features a user triggers or the scheduled tasks listed in the security policy.
CCC-06.1	Are change management and configuration baselines established, documented and implemented for all relevant authorized changes on organizational assets?	**Yes** CSP-owned	Each release has a manifest (permissions, modules), a software bill of materials (CycloneDX SBOM) and a versioned source archive that serve as the baseline.
CCC-06.2	Are the baselines reviewed and updated at least annually or upon significant changes?	**Yes** CSP-owned	Baselines are produced again for every release.
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	**Yes** CSP-owned	A weekly scheduled check compares every release archive with its recorded fingerprint, re-runs the quality checks on any archive that changed and reports any difference to the founder. Before each release, blocking quality checks, forge lint and a dependency audit run.
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** Shared CSP and 3rd-party	A previous version can be redeployed from its versioned archive. Atlassian's version rules apply on customer sites.
Cryptography, Encryption & Key Management			
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	**Yes** Shared CSP and 3rd-party	Encryption at rest and in transit is provided by Atlassian's platform (AES-256 at rest, TLS 1.2 or higher in transit). Clearlane's public security policy sets how signing passwords are kept: only as a salted scrypt hash in Atlassian's secret storage. Clearlane's deployment keys are listed with their expiry dates in its internal security register, stored on the founder's encrypted workstation, loaded only into the temporary session that runs a deployment, and never displayed.
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually, upon significant changes?	**Yes** CSP-owned	Updated upon significant changes (security policy last updated 3 November 2026, privacy policy 29 October 2026). No yearly review has fallen due yet.
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	**Yes** Shared CSP and 3rd-party	Atlassian manages platform encryption keys. The founder is responsible for Clearlane's deployment keys.
CEK-03.1	Are data protection at-rest and in-transit, and where applicable in use, provided using cryptographic libraries certified to approved standards?	**No** Shared CSP and 3rd-party	Encryption at rest and in transit is provided by Atlassian's platform (AES-256 at rest, TLS 1.2 or higher in transit); see Atlassian's documentation for its cryptographic modules. Clearlane's own hashing (scrypt for signing passwords) uses the Node.js built-in crypto module, which Clearlane has not verified as certified (for example FIPS 140) in the Forge runtime.
CEK-04.1	Are encryption algorithms following industry standards utilized for protecting data, based on the data classification and associated risks?	**Yes** Shared CSP and 3rd-party	Industry-standard algorithms protect customer data: AES-256 and TLS by Atlassian; scrypt for signing passwords in the apps.
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?	**Yes** CSP-owned	Any change to how the apps use cryptography goes through the release protocol and its security code review, and is stated in the release notes.

ID	Question	Answer · Owner	How Clearlane meets it
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	**Yes** Shared CSP and 3rd-party	Platform keys are generated by Atlassian; Clearlane's deployment keys are generated by the issuing services (Atlassian, Bitbucket, Cloudflare). Signing-password hashing uses the Node.js built-in crypto module.
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	**No** Shared CSP and 3rd-party	Platform keys are rotated by Atlassian. No cryptoperiod has been formally calculated for Clearlane's own keys: the Atlassian and Bitbucket deployment keys expire within one year and will be replaced before expiry; the website publishing key has no expiry date and can only publish the website.
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** CSP-owned	A compromised deployment key would be revoked in the issuing service and replaced, as part of the containment step of the incident plan.
CEK-14.1	Are processes, procedures and technical measures to securely destroy cryptographic keys when they are no longer needed, defined, implemented, and evaluated, and include provisions for legal and regulatory requirements?	**Yes** Shared CSP and 3rd-party	Atlassian destroys platform keys. When a deployment key is replaced, the old one is revoked in the issuing service and its file is deleted.
Datacenter Security			
DCS-04.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	**No** CSP-owned	Clearlane has no offices or data centres; the founder works from a private home office, and no customer data from the apps is held there. No formal written workspace policy.
DCS-04.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually, or upon significant changes?	**No** CSP-owned	See DCS-04.1.
DCS-06.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	**No** CSP-owned	No formal classification of assets by business risk. Assets are few: the apps and their release archives (fingerprints recorded), the website, deployment keys (listed with their expiry dates in the internal security register), the workstation and the accounts listed in STA-08.1.
DCS-06.2	Are assets' classifications reviewed and updated at least annually or upon significant changes?	**No** CSP-owned	See DCS-06.1.
DCS-07.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	**Yes** CSP-owned	Clearlane has no sites of its own. Its deployment keys, with their expiry dates, are listed in its internal security register, and its release archives with their recorded fingerprints. Physical hosting assets belong to Atlassian.
DCS-07.2	Is the catalogue reviewed and updated at least annually or upon significant changes?	**Yes** CSP-owned	Release archives are checked every week against their recorded fingerprints; the rest of the list is updated upon changes.
Data Security and Privacy Lifecycle Management			
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the preparation, classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	**Yes** CSP-owned	Public privacy policy and security policy, and a Data Processing Agreement, describe what data each app keeps and where. Customer content stays in the customer's Atlassian site.
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually, or upon significant changes?	**Yes** CSP-owned	Updated upon significant changes (security policy last updated 3 November 2026, privacy policy 29 October 2026). No yearly review has fallen due yet.
DSP-03.1	Is a data inventory created and maintained for sensitive, regulated and personal information (at a minimum)?	**Yes** CSP-owned	The privacy policy lists, app by app, the personal data kept (mainly Atlassian account IDs and the names shown at signing). Clearlane keeps a record of processing activities.
DSP-03.2	Is the inventory reviewed and updated at least annually or upon significant changes?	**Yes** CSP-owned	Updated with every release that changes the data kept.

ID	Question	Answer · Owner	How Clearlane meets it
DSP-04.1	Is data classified according to type and sensitivity levels?	**Yes** Shared CSP and CSC	The privacy and security policies distinguish customer content (stays in the customer's site), personal data (account IDs, names at signing) and secrets (signing password hashes). Customers classify their own content in Jira and Confluence.
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	**Yes** CSP-owned	Data flows are documented in the trust center, privacy policy and each app's Marketplace Privacy and security tab: data is processed and stored only within Atlassian; the apps make no call outside Atlassian.
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, or upon significant changes?	**Yes** CSP-owned	Reviewed with every release that changes the data kept or where it flows.
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	**Yes** Shared CSP and CSC	The customer owns its content and is the controller; Clearlane acts as processor for the little personal data the apps keep, as set out in the Data Processing Agreement.
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	**Yes** CSP-owned	Updated upon significant changes (security policy last updated 3 November 2026, privacy policy 29 October 2026). No yearly review has fallen due yet.
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	**Yes** CSP-owned	Security by design: Forge only, no Clearlane servers, least-privilege permissions, actions taken with the user's own permissions, no outside network calls, signing passwords hashed.
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	**Yes** CSP-owned	Privacy by design: only what a record needs is kept; content never leaves the customer's site; the apps send no analytics or tracking data outside Atlassian.
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	**Yes** CSP-owned	Actions that create or share data happen only when a person asks or under the scheduled tasks listed in the security policy. Nothing is sent outside Atlassian.
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)?	**Yes** Shared CSP and 3rd-party	The apps transfer no data outside Atlassian, by design (no outside network connection declared). Transfers within Atlassian's platform are encrypted (TLS 1.2 or higher) and governed by Atlassian.
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)?	**Yes** Shared CSP and CSC	Requests are handled through the customer (controller) and Clearlane's help center. The apps report the accounts they store to Atlassian's personal data reporting API, and data linked to closed accounts is erased automatically.
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)?	**Yes** CSP-owned	Personal data is used only to run the feature it belongs to (for example who signed a record), as declared in the privacy policy.
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)?	**Yes** CSP-owned	The only sub-processor for customer data is Atlassian, which already hosts the customer's site; it is listed in the Data Processing Agreement and the public sub-processor list.
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?	**Yes** CSP-owned	The sub-processor list is public; under the Data Processing Agreement, Clearlane informs customers at least 30 days before adding or replacing a sub-processor.
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	**Yes** Shared CSP and CSC	Records are kept in the customer's site as long as the customer keeps them; data linked to closed accounts is erased automatically; on uninstall, Atlassian deletes the app's stored data under its retention rules.
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	**Yes** Shared CSP and 3rd-party	Sensitive data stays in Forge storage encrypted by Atlassian; signing passwords are only stored as hashes; nothing sensitive is written to logs.

ID	Question	Answer · Owner	How Clearlane meets it
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?	**Yes** Shared CSP and 3rd-party	Data is stored in Atlassian's Forge storage for the customer's site and follows the site's data residency (pinned to the same region when the site is pinned). Atlassian may occasionally process data outside that region; stored data stays pinned. Location details are in Atlassian's documentation.
Governance, Risk and Compliance			
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	**Yes** CSP-owned	Clearlane's security and privacy rules are written, approved and applied by the founder, who is the only person in the business; the public security policy, privacy policy and trust center summarise them.
GRC-01.2	Are the policies and procedures reviewed and updated at least annually, or upon significant changes?	**Yes** CSP-owned	Updated upon significant changes (security policy last updated 3 November 2026, privacy policy 29 October 2026). No yearly review has fallen due yet.
GRC-02.1	Is there an established and maintained formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of risks?	**No** CSP-owned	No formal enterprise risk management programme, which would be disproportionate for a one-person business. Security vulnerabilities are assessed and tracked in the security register.
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	**Yes** CSP-owned	The founder holds all roles: decisions, production approvals, incident reporting to Atlassian and authorities.
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	**Yes** CSP-owned	Applicable requirements are identified and documented: GDPR, the Atlassian Marketplace partner agreement and security requirements, Forge platform terms, and French law.
GRC-07.2	Are the identified requirements reviewed at least annually or upon significant changes?	**Yes** CSP-owned	Updated upon significant changes (security policy last updated 3 November 2026, privacy policy 29 October 2026). No yearly review has fallen due yet.
Human Resources			
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	**No** CSP-owned	One-person business working from a private home office; no written clean-desk policy. No customer data from the apps is held on the workstation.
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually, or upon significant changes?	**No** CSP-owned	See HRS-03.1.
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** CSP-owned	No written remote-work policy. In practice the founder works from his home office on one workstation with BitLocker disk encryption, Windows firewall and active antivirus, and supervises temporary sessions of the AI coding assistant; every business account uses two-step verification; deployment keys are never displayed. Automatic screen lock is not yet enabled (see UEM-06.1).
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, or upon significant changes?	**No** CSP-owned	See HRS-04.1.
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	**No** CSP-owned	No employees; no formal training programme. The founder follows Atlassian's security requirements and advisories for Marketplace partners.
HRS-11.2	Are regular security awareness training updates provided?	**No** CSP-owned	See HRS-11.1.
Identity & Access Management			

ID	Question	Answer · Owner	How Clearlane meets it
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	**Yes** Shared CSP and CSC	End users are authenticated by Atlassian (customer SSO and two-step verification apply). Inside the apps, access follows Jira and Confluence permissions. Clearlane's own accounts are held only by the founder, each with two-step verification; AI development tools act only under his supervision.
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually, or upon significant changes?	**Yes** CSP-owned	Updated upon significant changes (security policy last updated 3 November 2026, privacy policy 29 October 2026). No yearly review has fallen due yet.
IAM-03.1	Is the inventory of identities managed, stored, and regularly reviewed, and is their level of access monitored?	**No** CSP-owned	Clearlane's identities are few: the founder's business accounts (STA-08.1) and deployment keys, listed in the security register (with expiry dates where they have one). No periodic review or access monitoring is scheduled yet. Customer identities are managed by Atlassian and the customer.
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	**No** CSP-owned	Not achievable in a one-person business: code is written with AI coding assistance under the founder's supervision and the founder authorises releases. Partly compensated by blocking automated checks, a separate automated security code review, repeated until no high or medium finding remains, and the customer administrator's approval of any version that adds a permission.
IAM-05.1	Is the least privilege principle employed when implementing information system access?	**Yes** CSP-owned	Each app requests only the Forge permissions its features use and acts with the user's own permissions, except the tasks listed in the security policy. The website publishing key is limited to publishing the website.
IAM-06.1	Is an identity access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	**Yes** Shared CSP and CSC	Customer access is provisioned by the customer in Atlassian. Clearlane's keys are created, recorded and revoked by the founder.
IAM-07.1	Is a process in place to de-provision or modify identity access in a timely manner?	**Yes** Shared CSP and CSC	Customers de-provision users in Atlassian; the apps follow at once. Clearlane revokes a key in the issuing service when it is no longer needed.
IAM-08.1	Are reviews and revalidation of identity access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance, and at least annually or upon significant changes?	**Yes** CSP-owned	Upon change: app permissions are reviewed in the security code review of every release. Clearlane's own accounts and keys are held by the founder alone; keys are listed in the security register (with expiry dates where they have one). No periodic access review is scheduled yet.
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated?	**Yes** Shared CSP and CSC	Where an app has administrative settings, they are limited to Jira or Confluence administrators or the managers they name (for example, only Jira administrators and the budget managers they name can create budgets in Clearlane Budget).
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	**No** CSP-owned	The founder, the only person in the business, holds permanent administrative access to Clearlane's accounts. The Atlassian and Bitbucket deployment keys expire within one year; the website publishing key has no expiry date but can only publish the website.
IAM-10.2	Are procedures implemented to prevent the accumulation of segregated privileged access?	**No** CSP-owned	All privileged access is held by the founder, the only person in the business, so it cannot be split between people (see IAM-04.1). Each deployment key is limited to one service.
IAM-13.1	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** Shared CSP and CSC	Users authenticate through Atlassian, with the customer's SSO and multi-factor rules. All Clearlane business accounts use two-step verification. Signing in the quality apps also requires a separate signing password.
IAM-13.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	**Yes** 3rd-party outsourced	App identities and calls between the apps and Atlassian's APIs are authenticated by the Forge platform.
Interoperability & Portability			
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application interfaces (e.g., APIs)?	**Yes** 3rd-party outsourced	Communications between the apps and Jira or Confluence use Atlassian's documented APIs through Forge.

ID	Question	Answer · Owner	How Clearlane meets it
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	**Yes** CSP-owned	Data stays in standard Jira and Confluence objects (work items, pages, properties, attachments) wherever possible.
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	**NA** CSP-owned	Customers use the apps as a service; they do not port the application code.
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	**Yes** CSP-owned	The quality and cyber apps export their records as PDF or CSV evidence files; data kept in Jira and Confluence objects remains available to the customer.
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually, or upon significant changes?	**Yes** CSP-owned	Updated upon significant changes (security policy last updated 3 November 2026, privacy policy 29 October 2026). No yearly review has fallen due yet.
Infrastructure Security			
I&S-03.1	Are communications between environments, services, and applications monitored?	**Yes** 3rd-party outsourced	Network monitoring of the platform is Atlassian's responsibility; Clearlane does not monitor traffic itself. The apps make no outbound calls outside Atlassian.
I&S-03.2	Are communications between environments, services, and applications encrypted?	**Yes** 3rd-party outsourced	All communications use TLS, provided by Atlassian's platform.
I&S-03.3	Are communications between environments, services, and applications restricted to only authenticated and authorized connections, as justified by the business?	**Yes** 3rd-party outsourced	Forge allows only authenticated calls from the app's own screens and to Atlassian's APIs; no outside network connection is declared.
I&S-03.4	Are network configurations reviewed at least annually?	**Yes** 3rd-party outsourced	Network configuration is Atlassian's. Clearlane reviews the apps' declared network access (none outside Atlassian) with every release.
I&S-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	**Yes** 3rd-party outsourced	Clearlane apps declare no outside services, protocols or ports. Platform network configuration is documented by Atlassian.
I&S-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** 3rd-party outsourced	Hosts, operating systems and control plane are Atlassian's and hardened by Atlassian. Clearlane operates no servers.
I&S-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that service customer (tenant) access is appropriately segmented, segregated, monitored, and restricted?	**Yes** 3rd-party outsourced	Forge isolates each customer site and app; app storage is per installation (per customer site).
I&S-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?	**NA** CSP-owned	Clearlane does not migrate customer servers, services or data to the cloud; the apps run inside the customer's Atlassian cloud site.
I&S-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** 3rd-party outsourced	Network attack protection of the platform is provided by Atlassian. Several apps add their own rate limits on their functions.
Logging and Monitoring			
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	**Yes** Shared CSP and 3rd-party	Documented rule: logs hold technical counters only (for example number of work items processed), never customer content or secrets. Logs are kept by Atlassian's Forge platform.
LOG-01.2	Are policies and procedures reviewed and updated at least annually, or upon significant changes?	**Yes** CSP-owned	Updated upon significant changes (security policy last updated 3 November 2026, privacy policy 29 October 2026). No yearly review has fallen due yet.

ID	Question	Answer · Owner	How Clearlane meets it
LOG-04.1	Is audit log access restricted to authorized identities, and are records of that access maintained?	**Yes** Shared CSP and 3rd-party	App logs are visible only through the founder's Atlassian developer account, protected by two-step verification. Clearlane keeps no separate record of who viewed them.
LOG-05.1	Are capabilities implemented and maintained to correlate and monitor security audit logs for the detection of suspicious or anomalous activity that deviates from typical or expected patterns?	**No** Shared CSP and 3rd-party	Clearlane has no log correlation, automated anomaly detection or alerts. App logs hold technical counters only and are checked when an issue is reported; platform monitoring is Atlassian's.
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	**Yes** CSP-owned	Anomalies are handled under the incident plan (SEF-07.1).
LOG-08.1	Are technical measures defined, implemented, and evaluated to enable service customers to detect and scrub or tokenize sensitive data from logs, in order to prevent unauthorized exposure as per applicable laws and regulations?	**NA** CSP-owned	The apps write no sensitive data or customer content to logs, so there is nothing for customers to scrub.
Security Incident Management, E-Discovery, & Cloud Forensics			
SEF-03.1	Is a security incident response plan that includes a communication strategy for notifying relevant internal departments, impacted service customers, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	**Yes** CSP-owned	Documented incident response plan: qualification within hours, report to Atlassian within 24 hours, containment, fix within Atlassian's deadlines, affected customers, as controllers of their data, told without undue delay; the CNIL notified within 72 hours where Clearlane is the controller, and lessons learned.
SEF-04.1	Is a structured approach followed to evaluate the effectiveness of incident response plans at planned intervals or upon significant changes?	**No** CSP-owned	The plan is to be reviewed after any security event (none so far) and when rules change; no formal periodic exercise yet.
SEF-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for timely and effective response to security incidents in accordance with incident categories and severity levels?	**Yes** CSP-owned	Incidents are categorised by CVSS severity (critical, high, medium, low) with matching response and fix deadlines.
SEF-07.2	Are these processes and procedures reviewed, updated, and tested at least annually?	**No** CSP-owned	Reviewed and updated upon changes; not yet tested in a formal annual exercise.
SEF-08.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	**Yes** CSP-owned	Breach notification steps are part of the incident plan, covering Atlassian, affected customers and, where Clearlane is the controller, the CNIL.
SEF-08.2	Are material security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	**Yes** CSP-owned	Material breaches would be reported to Atlassian, affected customers and, where Clearlane is the controller, the CNIL, as required by the Marketplace rules and GDPR. None has occurred.
Supply Chain Management, Transparency, and Accountability			
STA-01.1	Are policies and procedures for supply chain risk management established, documented, approved, communicated, applied, evaluated, and maintained?	**No** CSP-owned	No formal supply chain risk management policy. Suppliers are few (STA-08.1) and only Atlassian handles the content of customers' sites; open-source dependencies come only from the npm registry, are audited before each release and every week, and are listed in a CycloneDX SBOM for each release.
STA-01.2	Are policies and procedures for supply chain risk management reviewed and updated at least annually, or upon significant changes?	**No** CSP-owned	See STA-01.1.
STA-03.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain?	**Yes** Shared CSP and 3rd-party	The split of responsibilities with Atlassian (platform) and with customers (their users, permissions and content) is documented in the trust center, security policy and this questionnaire.
STA-05.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM?	**Yes** CSP-owned	Ownership of each control is given in this questionnaire.

ID	Question	Answer · Owner	How Clearlane meets it
STA-08.1	Is an inventory of all supply chain relationships developed and maintained?	**Yes** CSP-owned	Inventory: Atlassian (app hosting, Marketplace billing, help center, code backup on Bitbucket), Cloudflare (public website only), Apple iCloud (business e-mail), Brevo (newsletter and review-request e-mails), npm registry (open-source dependencies), and development tools including an AI coding assistant. Only Atlassian handles the content of customers' Jira and Confluence sites.
Threat & Vulnerability Management			
TVM-02.1	Are policies and procedures to protect against malware and malicious instructions established, documented, approved, communicated, applied, evaluated, and maintained?	**No** CSP-owned	No written malware-protection policy. In place: active antivirus and Windows firewall on the only workstation, whose disk is encrypted; code dependencies come only from the npm registry and are audited before each release and every week.
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually, or upon significant changes?	**No** CSP-owned	See TVM-02.1.
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	**Yes** CSP-owned	Dependencies of every app are checked for known vulnerabilities each week and before each release (npm audit).
TVM-05.1	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** Shared CSP and 3rd-party	The vulnerability database used by npm audit and the workstation's antivirus signatures update automatically.
TVM-08.1	Are processes, procedures and technical measures defined, implemented and evaluated based on identified risks to support scheduled and emergency responses to vulnerability identification?	**Yes** CSP-owned	Scheduled response through the weekly check; emergency response through the incident plan, with fixes deployed without delay for security issues.
TVM-10.1	Is a risk-based method used for the prioritization and mitigation of threats, leveraging an industry-recognized framework to guide threat decision-making and protection measures?	**Yes** CSP-owned	Severity is rated with CVSS and remediation deadlines follow Atlassian's Security Bug Fix Policy.
TVM-11.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	**Yes** CSP-owned	Vulnerabilities and their fixes are tracked in the security register; fixes are stated in release notes and affected customers are informed.
Universal Endpoint Management			
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** CSP-owned	No formal list of approved applications. Business data is handled on the founder's workstation, in temporary sessions of the AI coding assistant (source code only, no app data from customer sites), and in the business accounts listed in STA-08.1; code dependencies come only from the npm registry.
UEM-04.1	Is an inventory of all endpoints used and maintained to store, access and process company data?	**Yes** CSP-owned	One physical endpoint: the founder's workstation. Development and deployments also run in temporary sessions of the AI coding assistant, which receive the source code and, during a deployment, the deployment key.
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?	**Yes** CSP-owned	Disk encryption (BitLocker), antivirus, firewall and two-step verification on business accounts are in place; automatic screen lock is not yet enabled (UEM-06.1).
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	**No** CSP-owned	Automatic screen lock is not yet enforced on the workstation.
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	**Yes** CSP-owned	Antivirus active on the workstation.

ID	Question	Answer · Owner	How Clearlane meets it
UEM-10.1	Are software firewalls configured on managed endpoints?	**Yes** CSP-owned	Firewall active on the workstation.
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	**No** CSP-owned	No remote wipe capability. The disk is encrypted and no customer data from the apps is stored on the workstation.

Questions: Consensus Assessments Initiative Questionnaire Lite (CAIQ-Lite) v4.1.0, © 2026 Cloud Security Alliance, used under its terms of use.
Answers: Maxime Ragionieri EI (brand: Clearlane Apps), 4 November 2026; they are updated when Clearlane's practices change. More: clearlaneapps.com/trust · clearlaneapps.com/security · hello@clearlaneapps.com. The completed spreadsheet is available on request.