Cloud Security Alliance
CAIQ v4.1 Self-Assessment

JSM LaunchPad

Atlassian Forge Application

Let's Talk Solutions Ltd

February 2026

Summary

283 controls across 17 security domains

185 Yes | 98 NA (Atlassian-managed) | 0 No

140 CSC-owned | 95 CSP-owned | 48 Shared

CSC = Let's Talk Solutions Ltd (app vendor)

CSP = Atlassian (cloud platform)

JSM LaunchPad runs entirely within Atlassian Cloud infrastructure. No external servers, no customer data outside Atlassian, AES-256 at rest, TLS 1.2+ in transit.

Audit & Assurance

A&A-01.1 | Yes | CSC-owned

Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?

JSM LaunchPad maintains security policies documented in our internal security framework. As a Forge app, we operate within Atlassian's security infrastructure while maintaining app-level security controls for code quality, data handling, and access management.

A&A-01.2 | Yes | CSC-owned

Are audit and assurance policies, procedures, and standards reviewed and updated at least annually, or upon significant changes?

Security policies are reviewed annually and upon significant changes to the application, Forge platform updates, or regulatory requirements.

A&A-02.1 | NA | CSP-owned

Are independent audit and assurance assessments conducted according to relevant standards at least annually?

As a Forge marketplace app, independent third-party audits are conducted at the Atlassian platform level. Atlassian maintains SOC 2 Type II and ISO 27001 certifications covering the Forge infrastructure. The app undergoes Atlassian's marketplace security review process.

A&A-03.1 | NA | CSP-owned

Are independent audit and assurance assessments performed according to risk-based plans and policies, and in response to significant changes or emerging risks?

Risk-based audit planning is managed at the Atlassian platform level. The app is subject to Atlassian Marketplace security reviews and Forge platform security assessments.

A&A-04.1 | Yes | Shared

Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?

The app complies with Atlassian Marketplace Partner Agreement, Forge platform security requirements, GDPR, and UK Data Protection Act 2018. Platform-level compliance (SOC 2, ISO 27001) is maintained by Atlassian.

A&A-05.1 | NA | CSP-owned

Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence and aligned with relevant auditing standards?

Audit management processes are handled at the Atlassian platform level. The app participates in Atlassian's marketplace review process.

A&A-06.1 | Yes | CSC-owned

Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?

Findings from Atlassian marketplace reviews, security scans, and internal code reviews are tracked and remediated through a structured process using Jira for issue tracking.

A&A-06.2 | Yes | CSC-owned

Is the remediation status of audit findings regularly reviewed and reported to relevant stakeholders?

Remediation status is tracked in Jira and reviewed as part of the development cycle. Critical findings are prioritized for immediate resolution.

Application & Interface Security

AIS-01.1 | Yes | CSC-owned

Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?

Application security policies and procedures are established covering secure development practices, code review requirements, dependency management, and Forge-specific security guidelines.

AIS-01.2 | Yes | CSC-owned

Are application security policies and procedures reviewed and updated at least annually, or upon any significant changes?

Application security policies are reviewed annually and updated when Forge platform changes, new security requirements, or significant application changes occur.

AIS-02.1 | Yes | CSC-owned

Are baseline requirements to secure applications established, documented, and maintained?

Baseline security requirements include: input validation, output encoding, secure API usage, least-privilege Forge permissions, dependency vulnerability

scanning, and adherence to Atlassian Forge security best practices.

AIS-03.1 | Yes | CSC-owned

Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?

Application metrics tracked include: dependency vulnerability counts, code review completion rates, automated test coverage, and Forge security scan results.

AIS-04.1 | Yes | CSC-owned

Is a secure SDLC process defined and implemented for application requirements analysis, planning, design, development, testing, deployment, and operation per organizationally designed security requirements?

A secure SDLC is implemented using Git version control, branch protection, code reviews, automated testing, dependency scanning (npm audit/Snyk), and staged deployment through Forge CLI. All code changes require review before merge to main branch.

AIS-05.1 | Yes | CSC-owned

Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and meeting organizational delivery goals?

Testing strategy includes unit tests, integration tests, and manual testing against Forge sandbox environments. Acceptance criteria include passing all automated tests, security scan clearance, and successful deployment to staging environment.

AIS-05.2 | Yes | CSC-owned

Is testing automated when applicable and possible?

Automated testing is implemented via CI/CD pipeline including unit tests, linting, dependency vulnerability checks, and Forge-specific validations.

AIS-06.1 | Yes | CSC-owned

Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?

Application code is deployed through Atlassian Forge CLI using a standardized deployment process: development > staging > production. Forge handles runtime isolation, sandboxing, and infrastructure security.

AIS-06.2 | Yes | CSC-owned

Is the deployment and integration of application code automated where possible?

Deployment is automated through Forge CLI integrated with CI/CD pipeline. Manual approval gates exist for production deployments.

AIS-07.1 | Yes | CSC-owned

Are application security vulnerabilities remediated following defined processes?

Application vulnerabilities are identified through automated dependency scanning, code reviews, and Atlassian marketplace security reviews. Remediation follows severity-based SLAs: Critical (24hrs), High (72hrs), Medium (2 weeks), Low (next release).

AIS-07.2 | Yes | CSC-owned

Is the remediation of application security vulnerabilities automated when possible?

Dependency updates and vulnerability remediation are partially automated through Dependabot/Snyk alerts and automated PR creation for dependency updates.

AIS-08.1 | Yes | Shared

Are processes, procedures, and technical measures defined and implemented to secure APIs?

The app uses Forge platform APIs exclusively, which are secured by Atlassian's authentication and authorization framework. App-level API interactions follow Forge security model with scoped permissions and OAuth 2.0.

AIS-08.2 | Yes | Shared

Are reviews and updates for any improvements conducted at least annually, or upon significant changes?

API security practices are reviewed when Forge platform updates occur and at least annually. Forge permission scopes are reviewed to maintain least-privilege access.

Business Continuity Management and Operational Resilience

BCR-01.1 | Yes | Shared
Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?

Business continuity for the Forge app relies primarily on Atlassian's platform infrastructure. App-level continuity measures include: source code in version control (Git), documented build/deploy procedures, and ability to rapidly redeploy via Forge CLI.

BCR-01.2 | Yes | CSC-owned
Are the policies and procedures reviewed and updated at least annually, or upon significant changes?

App-level continuity procedures are reviewed annually.

BCR-02.1 | NA | CSP-owned
Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?

Business continuity risk assessment and impact analysis for infrastructure is managed by Atlassian. The Forge platform provides built-in resilience and redundancy.

BCR-02.2 | NA | CSP-owned
Are the risk assessment and impact analysis reviewed and updated at least annually or upon significant changes?

Infrastructure-level risk assessments are managed by Atlassian.

BCR-03.1 | NA | CSP-owned
Are strategies being established to reduce the impact of business disruptions, and are resiliency and recovery from business disruptions being improved?

Infrastructure resilience and recovery capabilities are provided by the Atlassian Forge platform, including automatic scaling, redundancy, and disaster recovery.

BCR-04.1 | NA | CSP-owned
Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?

Operational resilience strategies at the infrastructure level are managed by Atlassian.

BCR-05.1 | Yes | Shared
Is relevant documentation developed, identified, and acquired both internally and from external parties, to support business continuity and operational resilience plans?

App-level continuity documentation includes: deployment procedures, rollback processes, source code repository access, and Forge CLI deployment guides. Infrastructure continuity documentation is maintained by Atlassian.

BCR-05.2 | Yes | Shared
Is business continuity and operational resilience documentation available to authorized stakeholders?

Documentation is accessible to the development team and authorized stakeholders.

BCR-05.3 | Yes | CSC-owned
Is business continuity and operational resilience documentation reviewed at least annually or upon significant changes?

App-level continuity documentation is reviewed annually and upon significant application changes.

BCR-06.1 | NA | CSP-owned

Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?

Business continuity plan testing at infrastructure level is conducted by Atlassian. App-level recovery is validated through routine deployment and rollback procedures.

BCR-07.1 | Yes | Shared

Are communication channels with all relevant stakeholders established and maintained during business continuity and resilience procedures?

Communication channels are maintained through Atlassian's status page for platform incidents, and direct communication channels for app-specific issues via Atlassian Marketplace support.

BCR-08.1 | NA | CSP-owned

Are backups performed periodically?

Data backups are managed by Atlassian's Forge platform infrastructure. App source code is backed up through Git version control with remote repositories.

BCR-08.2 | NA | CSP-owned

Is the confidentiality, integrity, and availability of the backup ensured?

Backup confidentiality, integrity, and availability is managed by Atlassian at the platform level.

BCR-08.3 | NA | CSP-owned

Can backups be restored appropriately for resiliency?

Backup restoration capabilities are managed by Atlassian.

BCR-09.1 | NA | CSP-owned

Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?

Disaster response planning for infrastructure is managed by Atlassian.

BCR-09.2 | NA | CSP-owned

Is the disaster response plan updated at least annually, and when significant changes occur?

Disaster response plan updates are managed by Atlassian.

BCR-10.1 | NA | CSP-owned

Is the disaster response plan exercised annually or when significant changes occur?

Disaster response exercises are managed by Atlassian.

BCR-10.2 | NA | CSP-owned

Are local emergency authorities included, if possible, in the exercise?

Emergency authority coordination is managed by Atlassian at the datacenter level.

BCR-11.1 | NA | CSP-owned

Are business-critical equipment supplemented with both locally redundant and geographically dispersed equipment located at a reasonable minimum distance, in accordance with applicable industry standards?

Equipment redundancy and geographic distribution is managed by Atlassian's cloud infrastructure.

Change Control and Configuration Management

CCC-01.1 | Yes | CSC-owned
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?

Change management policies are established for the application covering code changes, dependency updates, configuration changes, and Forge manifest modifications. All changes follow Git-based workflow with branch protection and code review requirements.

CCC-01.2 | Yes | CSC-owned
Are the policies and procedures reviewed and updated at least annually, or upon significant changes?

Change management policies are reviewed annually and updated upon significant changes.

CCC-02.1 | Yes | CSC-owned
Is a defined quality change control, approval and testing process, incorporating baselines, testing, and release standards, established, maintained and implemented?

Quality change control includes: Git branching strategy, pull request reviews, automated CI/CD testing, staging environment validation, and production deployment approval gates via Forge CLI.

CCC-03.1 | Yes | CSC-owned
Is a change management procedure implemented to manage the risks associated with applying changes to assets, owned, controlled or used by the organization?

Change management procedure implemented through Git workflow: feature branches, pull requests with mandatory review, automated testing pipeline, staged deployment (dev > staging > production).

CCC-04.1 | Yes | Shared
Is a procedure to authorize the addition, removal, update, and management of assets owned, controlled, or used by the organization, implemented and enforced?

Asset management for the app includes: source code repository management, Forge manifest permission scoping, dependency tracking, and npm package management. Infrastructure assets are managed by Atlassian.

CCC-05.1 | Yes | Shared
Are provisions to limit changes directly impacting service customer-owned environments (tenants) to explicitly authorized requests included within service level agreements?

The Forge platform enforces tenant isolation. App changes are deployed through Atlassian's controlled Forge deployment process which manages tenant-level impacts. App permissions are explicitly declared in the Forge manifest.

CCC-06.1 | Yes | CSC-owned
Are change management and configuration baselines established, documented and implemented for all relevant authorized changes on organizational assets?

Configuration baselines are maintained through: Forge manifest (permissions, modules), package.json (dependencies), environment configuration, and documented deployment procedures.

CCC-06.2 | Yes | CSC-owned
Are the baselines reviewed and updated at least annually or upon significant changes?

Configuration baselines reviewed annually and upon significant changes.

CCC-07.1 | Yes | Shared
Are detection measures implemented with proactive notification if changes deviate from established baselines?

Forge platform monitors app behaviour against declared permissions. Git-level detection through branch protection rules and CI/CD pipeline checks for unauthorized changes.

CCC-08.1 | Yes | CSC-owned

Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?

Emergency change procedures are defined for critical security patches and production hotfixes, allowing expedited review and deployment while maintaining audit trail.

CCC-08.2 | Yes | CSC-owned

Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?

Emergency change exceptions follow the governance exception process with documented justification and post-implementation review.

CCC-09.1 | Yes | CSC-owned

Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?

Rollback capability is built into the deployment process via Forge CLI version management. Previous app versions can be redeployed rapidly. Git version history provides complete code rollback capability.

Cryptography, Encryption & Key Management

CEK-01.1 | Yes | Shared

Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?

Encryption at the infrastructure level (data at rest, in transit) is managed by Atlassian's Forge platform. The app follows Atlassian's cryptographic standards and does not implement custom encryption. All data transmission uses HTTPS/TLS enforced by the Forge platform.

CEK-01.2 | Yes | Shared

Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually, upon significant changes?

Cryptographic practices are reviewed when Forge platform updates occur and at least annually.

CEK-02.1 | NA | CSP-owned

Are cryptography, encryption, and key management roles and responsibilities defined and implemented?

Cryptographic roles and responsibilities at the infrastructure level are managed by Atlassian. The app does not manage encryption keys or cryptographic infrastructure directly.

CEK-03.1 | Yes | CSP-owned

Are data protection at-rest and in-transit, and where applicable in use, provided using cryptographic libraries certified to approved standards?

Data protection at rest and in transit is provided by Atlassian's Forge platform using industry-standard cryptographic libraries. All Forge app data stored in Atlassian infrastructure is encrypted at rest (AES-256) and in transit (TLS 1.2+).

CEK-04.1 | Yes | CSP-owned

Are encryption algorithms following industry standards utilized for protecting data, based on the data classification and associated risks?

Encryption algorithms are managed by Atlassian at the platform level (AES-256 at rest, TLS 1.2+ in transit). The app does not implement custom encryption algorithms.

CEK-05.1 | NA | CSP-owned

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?

Key management is entirely handled by Atlassian's Forge platform infrastructure. The app does not generate, store, rotate, or manage cryptographic keys. All encryption key lifecycle management is the responsibility of Atlassian as the CSP.

CEK-06.1 | NA | CSP-owned

Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?

Key management is entirely handled by Atlassian's Forge platform infrastructure. The app does not generate, store, rotate, or manage cryptographic keys. All encryption key lifecycle management is the responsibility of Atlassian as the CSP.

CEK-07.1 | NA | CSP-owned

Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?

Key management is entirely handled by Atlassian's Forge platform infrastructure. The app does not generate, store, rotate, or manage cryptographic keys. All encryption key lifecycle management is the responsibility of Atlassian as the CSP.

CEK-08.1 | NA | CSP-owned

Are service providers providing service customers with the capacity to manage their own data encryption keys?

Key management is entirely handled by Atlassian's Forge platform infrastructure. The app does not generate, store, rotate, or manage cryptographic keys. All encryption key lifecycle management is the responsibility of Atlassian as the CSP.

CEK-09.1 | NA | CSP-owned

Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event?

Key management is entirely handled by Atlassian's Forge platform infrastructure. The app does not generate, store, rotate, or manage cryptographic keys. All encryption key lifecycle management is the responsibility of Atlassian as the CSP.

CEK-09.2 | NA | CSP-owned

Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?

Key management is entirely handled by Atlassian's Forge platform infrastructure. The app does not generate, store, rotate, or manage cryptographic keys. All encryption key lifecycle management is the responsibility of Atlassian as the CSP.

CEK-10.1 | NA | CSP-owned

Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?

Key management is entirely handled by Atlassian's Forge platform infrastructure. The app does not generate, store, rotate, or manage cryptographic keys. All encryption key lifecycle management is the responsibility of Atlassian as the CSP.

CEK-11.1 | NA | CSP-owned

Are private keys provisioned for a unique purpose managed, and is cryptography secret?

Key management is entirely handled by Atlassian's Forge platform infrastructure. The app does not generate, store, rotate, or manage cryptographic keys. All encryption key lifecycle management is the responsibility of Atlassian as the CSP.

CEK-12.1 | NA | CSP-owned

Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?

Key management is entirely handled by Atlassian's Forge platform infrastructure. The app does not generate, store, rotate, or manage cryptographic keys. All encryption key lifecycle management is the responsibility of Atlassian as the CSP.

CEK-13.1 | NA | CSP-owned

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?

Key management is entirely handled by Atlassian's Forge platform infrastructure. The app does not generate, store, rotate, or manage cryptographic keys. All encryption key lifecycle management is the responsibility of Atlassian as the CSP.

CEK-14.1 | NA | CSP-owned

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?

Key management is entirely handled by Atlassian's Forge platform infrastructure. The app does not generate, store, rotate, or manage cryptographic keys. All encryption key lifecycle management is the responsibility of Atlassian as the CSP.

CEK-15.1 | NA | CSP-owned

Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?

Key management is entirely handled by Atlassian's Forge platform infrastructure. The app does not generate, store, rotate, or manage cryptographic keys. All encryption key lifecycle management is the responsibility of Atlassian as the CSP.

CEK-16.1 | NA | CSP-owned

Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?

Key management is entirely handled by Atlassian's Forge platform infrastructure. The app does not generate, store, rotate, or manage cryptographic keys. All encryption key lifecycle management is the responsibility of Atlassian as the CSP.

CEK-17.1 | NA | CSP-owned

Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?

Key management is entirely handled by Atlassian's Forge platform infrastructure. The app does not generate, store, rotate, or manage cryptographic keys. All encryption key lifecycle management is the responsibility of Atlassian as the CSP.

CEK-18.1 | NA | CSP-owned

Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?

Key management is entirely handled by Atlassian's Forge platform infrastructure. The app does not generate, store, rotate, or manage cryptographic keys. All encryption key lifecycle management is the responsibility of Atlassian as the CSP.

CEK-19.1 | NA | CSP-owned

Are processes, procedures, and technical measures to use compromised keys to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) defined, implemented, and evaluated to include legal and regulatory requirement provisions?

Key management is entirely handled by Atlassian's Forge platform infrastructure. The app does not generate, store, rotate, or manage cryptographic keys. All encryption key lifecycle management is the responsibility of Atlassian as the CSP.

CEK-20.1 | NA | CSP-owned

Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?

Key management is entirely handled by Atlassian's Forge platform infrastructure. The app does not generate, store, rotate, or manage cryptographic keys. All encryption key lifecycle management is the responsibility of Atlassian as the CSP.

CEK-21.1 | NA | CSP-owned

Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions?

Key management is entirely handled by Atlassian's Forge platform infrastructure. The app does not generate, store, rotate, or manage cryptographic keys. All encryption key lifecycle management is the responsibility of Atlassian as the CSP.

Datacenter Security

DCS-01.1 | NA | CSP-owned

Are policies and procedures for physical and environmental security established, documented, approved, communicated, applied, evaluated, and maintained?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-01.2 | NA | CSP-owned

Are policies and procedures for physical and environmental security reviewed and updated at least annually, or upon significant changes?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-02.1 | NA | CSP-owned

Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-02.2 | NA | CSP-owned

Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-02.3 | NA | CSP-owned

Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually or upon significant changes?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-03.1 | NA | CSP-owned

Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-03.2 | NA | CSP-owned

Does a relocation or transfer request require written or cryptographically verifiable authorization?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-03.3 | NA | CSP-owned

Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually, or upon significant changes?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-04.1 | NA | CSP-owned

Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-04.2 | NA | CSP-owned

Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually, or upon significant changes?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-05.1 | NA | CSP-owned

Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-05.2 | NA | CSP-owned

Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually, or upon significant changes?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-06.1 | NA | CSP-owned

Is the classification and documentation of physical and logical assets based on the organizational business risk?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-06.2 | NA | CSP-owned

Are assets' classifications reviewed and updated at least annually or upon significant changes?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-07.1 | NA | CSP-owned

Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-07.2 | NA | CSP-owned

Is the catalogue reviewed and updated at least annually or upon significant changes?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-08.1 | NA | CSP-owned

Are physical security perimeters designed and implemented to safeguard personnel, data, and information systems?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-09.1 | NA | CSP-owned

Is equipment identification used as a method for connection authentication?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-10.1 | NA | CSP-owned

Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-10.2 | NA | CSP-owned

Are access control records retained periodically, as deemed appropriate by the organization?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-11.1 | NA | CSP-owned

Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-12.1 | NA | CSP-owned

Are datacenter personnel trained to safely manage adverse events, including but not limited to unauthorized ingress and egress attempts?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-13.1 | NA | CSP-owned

Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-14.1 | NA | CSP-owned

Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-15.1 | NA | CSP-owned

Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-16.1 | NA | CSP-owned

Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-17.1 | NA | CSP-owned

Are datacenter security metrics established, monitored, and reported to secure data center assets and services?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

DCS-18.1 | NA | CSP-owned

Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure continuous operations?

Datacenter security is entirely managed by Atlassian. As a Forge app, JSM LaunchPad runs on Atlassian's cloud infrastructure (AWS). All physical security, environmental controls, and datacenter operations are Atlassian's responsibility. Refer to Atlassian's Trust Center (https://www.atlassian.com/trust) for datacenter security documentation.

Data Security and Privacy Lifecycle Management

DSP-01.1 | Yes | CSC-owned

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?

Data security and privacy policies are established covering: data handling within JSM Assets/CMDB context, tenant data isolation (enforced by Forge), GDPR compliance, and data minimization principles. The app processes CMDB schema configuration data only - no personal data is collected or stored beyond what exists in the customer's JSM instance.

DSP-01.2 | Yes | CSC-owned

Are data security and privacy policies and procedures reviewed and updated at least annually, or upon significant changes?

Data security and privacy policies reviewed annually and upon significant changes.

DSP-02.1 | NA | CSP-owned

Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?

Secure data disposal from storage media is managed by Atlassian at the infrastructure level.

DSP-03.1 | Yes | CSC-owned

Is a data inventory created and maintained for sensitive, regulated and personal information (at a minimum)?

Data inventory maintained for the app: the app processes JSM Assets object type schemas, attribute definitions, and reference type configurations. No personal or sensitive data is collected beyond standard Atlassian user context (user ID for audit purposes).

DSP-03.2 | Yes | CSC-owned

Is the inventory reviewed and updated at least annually or upon significant changes?

Data inventory is reviewed annually and upon significant application changes.

DSP-04.1 | Yes | Shared

Is data classified according to type and sensitivity levels?

Data processed by the app is classified as: CMDB configuration data (object type schemas, attributes, relationships). This is operational configuration data, not personal or sensitive data. Data classification at the infrastructure level is managed by Atlassian.

DSP-05.1 | Yes | CSC-owned

Is data flow documentation created to identify what data is processed and where it is stored and transmitted?

Data flow documentation exists showing: User initiates schema deployment > App reads schema template > App calls JSM Assets API to create object types/attributes/references > Data stored in customer's JSM Assets instance. All data flows use Forge-secured API channels.

DSP-05.2 | Yes | CSC-owned

Is data flow documentation reviewed at defined intervals, at least annually, or upon significant changes?

Data flow documentation reviewed annually and upon significant application changes.

DSP-06.1 | Yes | Shared

Is the ownership and stewardship of all relevant personal and sensitive data documented?

Data ownership is clear: CMDB schema data created by the app belongs to the service customer. The app acts as a deployment tool - it creates configurations in the customer's own JSM Assets instance. Let's Talk Solutions Ltd is the data processor for any transient data handled during schema deployment.

DSP-06.2 | Yes | CSC-owned

Is data ownership and stewardship documentation reviewed at least annually?

Data ownership documentation reviewed annually.

DSP-07.1 | Yes | CSC-owned

Are systems, products, and business practices based on security principles by design and per industry best practices?

The app is designed with security by design principles: least-privilege Forge permissions, no unnecessary data collection, tenant isolation via Forge platform, input validation, and secure API usage patterns.

DSP-08.1 | Yes | CSC-owned

Are systems, products, and business practices based on privacy principles by design and according to industry best practices?

Privacy by design implemented: the app minimizes data collection, does not store personal data, respects tenant boundaries enforced by Forge, and defaults to the most privacy-preserving configuration.

DSP-08.2 | Yes | Shared

Are systems' privacy settings configured by default and according to all applicable laws and regulations?

Privacy settings default to most restrictive. Forge platform enforces tenant-level data isolation. The app does not expose configuration options that could weaken privacy protections.

DSP-09.1 | NA | CSC-owned

Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations and industry best practices?

A DPIA is not required as the app does not process personal data. The app deploys CMDB schema configurations (object types, attributes, relationships) which are operational metadata, not personal data.

DSP-10.1 | Yes | Shared

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)?

All data processing occurs within the Atlassian Forge platform (AWS regions). No personal data is transferred outside the platform. Forge enforces data residency requirements at the platform level.

DSP-11.1 | NA | CSP-owned

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)?

Data subject access requests would be handled through Atlassian's platform as the app does not independently store personal data. Any CMDB schema data is stored in the customer's own JSM instance.

DSP-12.1 | Yes | Shared

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)?

The app processes data only for its stated purpose: deploying CMDB schemas into JSM Assets. No data is used for secondary purposes. Forge platform enforces scope limitations.

DSP-13.1 | NA | CSC-owned

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 sub-processing occurs. The app operates entirely within the Forge platform without transferring data to third parties.

DSP-14.1 | Yes | CSC-owned

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?

Data handling practices are disclosed through the Atlassian Marketplace listing, privacy policy, and this CAIQ self-assessment. The app's Forge manifest declares all required permissions.

DSP-15.1 | NA | CSC-owned

Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?

The app does not replicate or use production data for testing. Development and testing use synthetic CMDB schema data.

DSP-16.1 | Yes | Shared

Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?

The app does not independently retain data. All CMDB schema data created by the app resides in the customer's JSM Assets instance and is subject to their retention policies. Forge platform storage follows Atlassian's data retention practices.

DSP-17.1 | Yes | Shared

Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?

Sensitive data protection throughout lifecycle is managed through Forge platform controls (encryption, access controls, tenant isolation) combined with app-level data minimization practices.

DSP-18.1 | Yes | Shared

Does the service provider ensure that a procedure is in place and communicated to service customers for managing and responding to requests by law enforcement authorities for the disclosure of personal data, in accordance with applicable laws and regulations?

Data breach procedures follow Atlassian's platform-level incident response for infrastructure events. For app-specific security issues, Let's Talk Solutions maintains incident response procedures and will notify affected customers through Atlassian Marketplace channels.

DSP-19.1 | Yes | CSP-owned

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?

Physical data location is managed by Atlassian's infrastructure. Forge apps run on Atlassian's AWS infrastructure with data residency options configured at the Atlassian platform level.

Governance, Risk and Compliance

GRC-01.1 | Yes | CSC-owned

Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?

Information governance policies are established for Let's Talk Solutions Ltd, covering data handling, security practices, and compliance requirements applicable to Forge app development and marketplace distribution.

GRC-01.2 | Yes | CSC-owned

Are the policies and procedures reviewed and updated at least annually, or upon significant changes?

Governance policies reviewed annually.

GRC-02.1 | Yes | CSC-owned

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?

A risk management approach is maintained proportional to the organization's size and the app's risk profile. Key risks identified include: dependency vulnerabilities, Forge platform changes, data handling errors, and marketplace compliance.

GRC-03.1 | Yes | CSC-owned
Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?

Organizational policies reviewed annually and upon substantial changes.

GRC-04.1 | Yes | CSC-owned
Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?

An exception process exists for documented deviations from established policies, requiring justification and approval.

GRC-05.1 | Yes | CSC-owned
Has an information security program (including programs of all relevant CCM domains) been developed and implemented?

An information security program appropriate to the organization's size is implemented, covering: secure development, access management, incident response, and compliance with Atlassian marketplace requirements.

GRC-06.1 | Yes | CSC-owned
Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?

Roles and responsibilities for governance are defined. As a small vendor (sole proprietor), the owner/developer maintains responsibility for all security governance functions.

GRC-07.1 | Yes | CSC-owned
Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?

Applicable requirements identified: Atlassian Marketplace Partner Agreement, Forge Security Requirements, GDPR, UK Data Protection Act 2018, UK Companies Act requirements for Let's Talk Solutions Ltd.

GRC-07.2 | Yes | CSC-owned
Are the identified requirements reviewed at least annually or upon significant changes?

Requirements reviewed annually.

GRC-08.1 | Yes | CSC-owned
Is contact established and maintained with related special interest groups and other relevant entities?

Engagement maintained with Atlassian Developer Community, Atlassian Partner network (Valiantys), and relevant security information sharing forums.

Human Resources

HRS-01.1 | NA | CSC-owned
Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) established, documented, approved, communicated, applied, evaluated, and maintained?

As a sole proprietor/single-developer operation (Let's Talk Solutions Ltd), traditional HR background verification for new employees is not applicable. The sole developer/owner maintains all security responsibilities.

HRS-01.2 | NA | CSC-owned
Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?

Not applicable - single-developer operation.

HRS-01.3 | NA | CSC-owned
Are background verification policies and procedures reviewed and updated at least annually, or upon significant changes?

Not applicable - single-developer operation.

HRS-02.1 | Yes | CSC-owned
Are policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained?

Acceptable use policies for development equipment and tools are established, including secure handling of development credentials, API keys, and access to production Forge environments.

HRS-02.2 | Yes | CSC-owned
Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually, or upon significant changes?

Acceptable use policies reviewed annually.

HRS-03.1 | Yes | CSC-owned
Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?

Screen lock and workspace security measures are implemented: automatic screen lock on development workstations, encrypted storage, and secure handling of any displayed confidential information.

HRS-03.2 | Yes | CSC-owned
Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually, or upon significant changes?

Workspace security policies reviewed annually.

HRS-04.1 | Yes | CSC-owned
Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?

Remote working security policies are in place covering: VPN usage, encrypted communications, secure development environment configuration, and secure access to code repositories and Forge deployment tools.

HRS-04.2 | Yes | CSC-owned
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?

Remote working policies reviewed annually.

HRS-05.1 | NA | CSC-owned
Are return procedures of organizationally-owned assets by terminated employees established and documented?

Not applicable - single-developer operation. Access credentials and Forge API keys are controlled by the sole owner/developer.

HRS-06.1 | NA | CSC-owned
Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all relevant personnel?

Not applicable - single-developer operation.

HRS-07.1 | NA | CSC-owned
Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?

Not applicable - single-developer operation. No employees to onboard.

HRS-08.1 | NA | CSC-owned
Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?

Not applicable - single-developer operation.

HRS-09.1 | Yes | CSC-owned
Are employee roles and responsibilities relating to information assets' security and privacy, established, documented and communicated?

As sole developer/owner, roles and responsibilities for information asset security are self-documented and maintained as part of the security framework.

HRS-10.1 | NA | CSC-owned
Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?

Not applicable - single-developer operation. No employees requiring NDAs. Contractor/consultant NDAs would be implemented if the team expands.

HRS-11.1 | NA | CSC-owned
Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?

Not applicable - single-developer operation. The owner/developer maintains current security awareness through professional development, Atlassian security updates, and industry best practices.

HRS-11.2 | NA | CSC-owned
Are regular security awareness training updates provided?

Not applicable - single-developer operation.

HRS-12.1 | NA | CSC-owned
Are employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?

Not applicable - single-developer operation.

HRS-12.2 | NA | CSC-owned
Are employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?

Not applicable - single-developer operation.

HRS-13.1 | NA | CSC-owned
Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?

Not applicable - single-developer operation.

Identity & Access Management

IAM-01.1 | Yes | Shared

Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?

Identity and access management for the app operates at two levels: (1) Atlassian platform handles user authentication and authorization for JSM Assets access; (2) App-level access is controlled through Forge permission scopes declared in the manifest.

IAM-01.2 | Yes | CSC-owned

Are identity and access management policies and procedures reviewed and updated at least annually, or upon significant changes?

IAM policies reviewed annually.

IAM-02.1 | Yes | CSC-owned

Are policies and procedures for the management of authentication credentials, including passwords, established, documented, approved, communicated, implemented, applied, evaluated, and maintained?

Authentication credential management: Forge API tokens stored securely, Git credentials managed through SSH keys, no hardcoded credentials in source code. CI/CD pipeline credentials managed through secure environment variables.

IAM-02.2 | Yes | CSC-owned

Are policies and procedures reviewed and updated at least annually, or upon significant changes?

Credential management procedures reviewed annually.

IAM-03.1 | Yes | Shared

Is the inventory of identities managed, stored, and regularly reviewed, and is their level of access monitored?

Identity inventory: App users are managed entirely through Atlassian's identity platform. The app does not maintain a separate identity store. Forge platform provides the identity context for each app invocation.

IAM-04.1 | Yes | Shared

Is the separation of duties principle employed when implementing information system access?

Separation of duties: Development and production Forge environments are separate. Code deployments require explicit action through Forge CLI. Atlassian platform enforces role-based access within customer JSM instances.

IAM-05.1 | Yes | Shared

Is the least privilege principle employed when implementing information system access?

Least privilege: The Forge manifest declares only the minimum required permission scopes. The app requests only JSM Assets API permissions necessary for schema deployment. No broad administrative permissions are requested.

IAM-06.1 | Yes | CSP-owned

Is an identity access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?

User access provisioning is managed through Atlassian's platform. App installation grants access based on Forge manifest permissions. Individual user access within JSM is managed by the customer's Atlassian admin.

IAM-07.1 | Yes | CSP-owned

Is a process in place to de-provision or modify identity access in a timely manner?

De-provisioning is handled by Atlassian's platform. App uninstallation revokes all app permissions. User-level de-provisioning is managed by the customer's Atlassian admin.

IAM-08.1 | Yes | CSC-owned

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?

Access reviews: Forge permission scopes are reviewed with each release to ensure least-privilege. Development tool access is reviewed quarterly.

IAM-09.1 | Yes | Shared

Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated?

Privileged access: Forge deployment credentials and marketplace admin access are restricted to the sole owner/developer. Atlassian platform manages privileged access within customer instances.

IAM-10.1 | Yes | CSC-owned

Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?

Privileged access (Forge deployment, marketplace admin) is limited to the sole developer/owner and is used only when required for deployments or marketplace management.

IAM-10.2 | Yes | CSC-owned

Are procedures implemented to prevent the accumulation of segregated privileged access?

As a single-developer operation, segregated privileged access accumulation is managed through role awareness and regular access review.

IAM-11.1 | Yes | CSP-owned

Are processes and procedures for service customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?

Service customer participation in access management is facilitated through Atlassian's admin console, where customers can manage app installations and user access.

IAM-12.1 | Yes | Shared

Are processes, procedures, and technical measures that ensure identities' activities are identifiable through uniquely associated IDs defined, implemented, and evaluated?

Identity traceability: Forge platform provides user context for each app invocation. All app actions are associated with the authenticated Atlassian user identity. Development activities are tracked through Git commit history.

IAM-13.1 | Yes | CSP-owned

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?

Authentication is managed entirely by Atlassian's platform using their identity services. The app inherits Atlassian's authentication framework including MFA support.

IAM-13.2 | Yes | CSP-owned

Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?

Digital certificate management for authentication is handled by Atlassian.

IAM-14.1 | Yes | CSC-owned

Are processes, procedures, and technical measures for the secure management of authentication credentials, including passwords, defined, implemented, and evaluated?

Secure credential management for development tools: SSH keys for Git, Forge CLI authentication tokens, marketplace admin credentials - all stored securely and rotated periodically.

IAM-15.1 | Yes | Shared
Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?

Authorization verification: Forge platform verifies that the app has appropriate permissions before allowing API calls. App-level authorization respects the customer's JSM permission scheme.

Interoperability & Portability

IPY-01.1 | Yes | Shared
Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application interfaces (e.g., APIs)?

Communication channel security is managed through Forge's secure platform. All API communications use TLS-encrypted channels provided by Atlassian.

IPY-01.2 | Yes | CSC-owned
Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?

Interoperability policies reviewed annually.

IPY-01.3 | Yes | CSC-owned
Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?

Application programming interfaces follow Forge platform standards and Atlassian REST API conventions.

IPY-01.4 | Yes | Shared
Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?

Information processing interoperability maintained through standard Forge APIs and JSM Assets API formats.

IPY-01.5 | Yes | CSC-owned
Are interoperability and portability policies and procedures reviewed and updated at least annually, or upon significant changes?

Interoperability and portability policies reviewed annually.

IPY-02.1 | Yes | Shared
Are service customers able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?

Service customers can access their CMDB data through standard JSM Assets APIs. The app creates standard JSM Assets configurations that remain fully accessible through Atlassian's native interfaces and APIs after deployment.

IPY-03.1 | Yes | CSP-owned
Are cryptographically secure network protocols implemented for the management, import, and export of data in accordance with industry standards?

Cryptographically secure network protocols are enforced by the Forge platform (TLS 1.2+).

IPY-04.1 | Yes | Shared
Do agreements include provisions specifying service customers' data access upon contract termination, and have the following?
a. Data format
b. Duration data will be stored
c. Scope of the data retained and made available to the service customers
d. Data deletion policy

Upon contract termination (app uninstallation), all CMDB schemas and data created by the app remain in the customer's JSM Assets instance. The app does not hold customer data hostage - all configurations are standard JSM Assets objects.

Infrastructure Security

I&S-01.1 | NA | CSP-owned
Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?

Infrastructure and virtualization security is managed by Atlassian's Forge platform. The app runs in Forge's sandboxed execution environment.

I&S-01.2 | NA | CSP-owned
Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually, or upon significant changes?

Infrastructure security policies are managed by Atlassian.

I&S-02.1 | NA | CSP-owned
Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?

Resource availability and capacity planning is managed by Atlassian's Forge platform with automatic scaling.

I&S-03.1 | Yes | CSP-owned
Are communications between environments, services, and applications monitored?

Communications between the app and Atlassian services are monitored by the Forge platform.

I&S-03.2 | Yes | CSP-owned
Are communications between environments, services, and applications encrypted?

All communications are encrypted by the Forge platform (TLS 1.2+).

I&S-03.3 | Yes | CSP-owned
Are communications between environments, services, and applications restricted to only authenticated and authorized connections, as justified by the business?

Communications restricted to authenticated and authorized connections by the Forge platform.

I&S-03.4 | NA | CSP-owned
Are network configurations reviewed at least annually?

Network configuration reviews at the infrastructure level are managed by Atlassian.

I&S-03.5 | NA | CSP-owned
Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?

Network configuration documentation is managed by Atlassian.

I&S-04.1 | NA | CSP-owned
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?

OS and infrastructure hardening is managed by Atlassian's Forge platform.

I&S-05.1 | Yes | Shared
Are the environments separated into production and non production environments to reduce the risk of sensitive production data being used in non-production environments?

Environment separation: Forge provides separate development and production environments. The app maintains separate staging/production deployment targets.

I&S-05.2 | Yes | CSC-owned
Is production data sanitized or protected before being used for any authorized non-production purpose?

Production data is not used in development/testing. All testing uses synthetic CMDB schema data.

I&S-06.1 | Yes | CSP-owned
Are applications and infrastructures designed, developed, deployed, and configured such that service customer (tenant) access is appropriately segmented, segregated, monitored, and restricted?

Multi-tenant isolation is enforced by the Forge platform. Each customer's data is isolated at the Atlassian platform level.

I&S-07.1 | NA | CSP-owned
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?

Server/service migration communications are managed by Atlassian.

I&S-08.1 | Yes | Shared
Are high-risk environments identified and documented based on data sensitivity, threat exposure, and business impact?

The app environment risk is assessed based on: the data sensitivity (CMDB configuration data - operational, not personal), Forge platform security posture, and marketplace distribution scope.

I&S-09.1 | Yes | Shared
Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?

Defense-in-depth: Forge platform provides network-level security, sandboxed execution, permission enforcement. App-level measures include input validation, least-privilege permissions, and secure coding practices.

Logging and Monitoring

LOG-01.1 | Yes | Shared
Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?

Logging at the infrastructure level is managed by Atlassian's Forge platform. App-level logging follows Forge logging practices with structured log output for operational and security events.

LOG-01.2 | Yes | CSC-owned
Are policies and procedures reviewed and updated at least annually, or upon significant changes?

Logging policies reviewed annually.

LOG-02.1 | Yes | CSP-owned
Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?

Audit log security and retention is managed by Atlassian's platform. Forge provides logging infrastructure with appropriate access controls.

LOG-03.1 | Yes | Shared
Are security-related events identified and monitored within applications and the underlying infrastructure?

Security-related events are monitored through: Forge platform monitoring, application error tracking, dependency vulnerability alerts, and Git activity monitoring.

LOG-03.2 | Yes | Shared
Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?

Alerting configured for: dependency vulnerability notifications (Dependabot/Snyk), Forge deployment failures, and application error spikes.

LOG-04.1 | Yes | CSP-owned
Is audit log access restricted to authorized identities, and are records of that access maintained?

Audit log access control is managed by Atlassian's platform.

LOG-05.1 | NA | CSP-owned
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?

Security audit log correlation and monitoring is managed by Atlassian at the platform level.

LOG-05.2 | NA | CSP-owned
Is a process established and followed to review and take appropriate and timely actions on detected anomalies?

Anomaly detection and response at the infrastructure level is managed by Atlassian.

LOG-06.1 | NA | CSP-owned
Is a reliable time source being used across all relevant information processing systems?

Time source reliability is managed by Atlassian's infrastructure.

LOG-07.1 | Yes | Shared
Are logging requirements for information meta/data system events established, documented, and implemented?

App-level logging captures: schema deployment events, API call outcomes, error conditions, and user-initiated actions. Infrastructure-level logging is managed by Atlassian.

LOG-07.2 | Yes | CSC-owned
Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment and as per relevant regulatory requirements?

Logging scope reviewed annually.

LOG-08.1 | NA | CSP-owned
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?

Log data scrubbing and tokenization capabilities for service customers are managed at the Atlassian platform level.

LOG-09.1 | Yes | Shared
Are audit records generated, and do they contain relevant security information?

App-level audit records include: schema deployment operations, configuration changes, and error events with relevant context (user, timestamp, action, outcome).

LOG-10.1 | Yes | CSP-owned
Are audit records protected from unauthorized access, modification, and deletion?

Audit record protection is managed by Atlassian's Forge platform infrastructure.

LOG-11.1 | NA | CSP-owned
Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?

Cryptographic operations monitoring is managed by Atlassian.

LOG-12.1 | NA | CSP-owned

Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?

Key lifecycle logging is managed by Atlassian.

LOG-13.1 | NA | CSP-owned

Is physical access logged and monitored using an auditable access control system?

Physical access logging is managed by Atlassian.

LOG-14.1 | Yes | Shared

Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?

Monitoring system anomalies are reported through Forge platform monitoring and app-level error tracking.

LOG-14.2 | Yes | CSC-owned

Are accountable parties immediately notified about anomalies and failures?

Immediate notification of critical anomalies through automated alerting (deployment failures, critical errors, security scan failures).

Security Incident Management, E-Discovery, & Cloud Forensics

SEF-01.1 | Yes | Shared

Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?

Security incident management policies established covering: app-specific security incidents (code vulnerabilities, data handling issues) and coordination with Atlassian for platform-level incidents.

SEF-01.2 | Yes | CSC-owned

Are policies and procedures reviewed and updated annually, or upon significant changes?

Incident management policies reviewed annually.

SEF-02.1 | Yes | CSC-owned

Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?

Incident management procedures include: identification, classification, containment (emergency Forge deployment rollback), investigation, remediation, and communication. Timelines defined based on severity.

SEF-02.2 | Yes | CSC-owned

Are policies and procedures for timely management of security incidents reviewed and updated at least annually, or upon significant changes?

Incident management procedures reviewed annually.

SEF-03.1 | Yes | CSC-owned

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?

Incident response plan includes communication strategy: notify Atlassian Marketplace team, notify affected customers through marketplace channels, and coordinate with Atlassian security team for platform-related incidents.

SEF-04.1 | Yes | CSC-owned
Is a structured approach followed to evaluate the effectiveness of incident response plans at planned intervals or upon significant changes?

Incident response effectiveness reviewed annually and after any significant incident.

SEF-05.1 | Yes | CSC-owned
Are information security incident metrics established, monitored and reported?

Incident metrics tracked: number of incidents, severity distribution, time to detection, time to resolution, and root cause categories.

SEF-06.1 | Yes | CSC-owned
Are processes, procedures, and technical measures supporting business processes
to triage security-related events defined, implemented, and evaluated?

Security event triage process defined: automated alerts evaluated, severity classified, response initiated based on classification.

SEF-07.1 | Yes | CSC-owned
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?

Incident response procedures include: immediate containment (Forge rollback capability), root cause analysis, remediation, and post-incident review.

SEF-07.2 | Yes | CSC-owned
Are these processes and procedures reviewed, updated, and tested at least annually?

Incident response processes reviewed annually and after significant incidents.

SEF-08.1 | Yes | Shared
Are processes, procedures, and technical measures for security breach notifications
defined and implemented?

Security breach notification procedures defined covering: notification to Atlassian (marketplace and security teams), notification to affected customers, and notification to relevant authorities as required by GDPR/UK DPA.

SEF-08.2 | Yes | Shared
Are material security breaches reported (including any relevant supply chain breaches)
as per applicable SLAs, laws, and regulations?

Material breaches reported as per Atlassian Marketplace Partner Agreement SLAs and within GDPR/UK DPA mandated timeframes (72 hours to supervisory authority where applicable).

SEF-09.1 | Yes | CSC-owned
Is a secure repository of security incident records established and maintained?

Security incident records maintained in a secure repository (Jira) with access restricted to authorized personnel.

SEF-09.2 | Yes | CSC-owned
Are incident records regularly reviewed to identify patterns, root causes, and systemic
vulnerabilities, and are relevant corrective measures implemented?

Incident records reviewed to identify patterns and root causes. Findings incorporated into security improvements.

SEF-10.1 | Yes | CSC-owned
Are points of contact maintained for applicable regulation authorities, national
and local law enforcement, and other legal jurisdictional authorities?

Points of contact maintained for: UK Information Commissioner's Office (ICO), Atlassian Security team, Atlassian Marketplace team.

SEF-10.2 | Yes | CSC-owned
Are points of contact reviewed and updated at least annually?

Contact information reviewed annually.

Supply Chain Management, Transparency, and Accountability

STA-01.1 | Yes | CSC-owned
Are policies and procedures for supply chain risk management established, documented, approved, communicated, applied, evaluated, and maintained?

Supply chain risk management policies address: open-source dependency management, Atlassian Forge platform dependency, and npm package ecosystem risks.

STA-01.2 | Yes | CSC-owned
Are policies and procedures for supply chain risk management reviewed and updated at least annually, or upon significant changes?

Supply chain policies reviewed annually.

STA-02.1 | Yes | CSC-owned
Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?

SSRM policies implemented: clear delineation between Atlassian (CSP) responsibilities (infrastructure, platform security) and Let's Talk Solutions (CSC) responsibilities (application security, code quality, dependency management).

STA-02.2 | Yes | CSC-owned
Are the policies and procedures that apply the SSRM reviewed and updated annually, or upon significant changes?

SSRM policies reviewed annually.

STA-03.1 | Yes | Shared
Is the SSRM applied, documented, implemented, and managed throughout the supply chain?

SSRM applied throughout the supply chain: Atlassian provides Forge platform > App uses Forge APIs > Customer deploys schemas to their JSM instance. Responsibilities clearly documented at each level.

STA-04.1 | Yes | CSC-owned
Is the service customer given SSRM guidance detailing information about SSRM applicability throughout the supply chain?

SSRM guidance provided to customers through: marketplace listing documentation, privacy policy, and this CAIQ self-assessment detailing shared responsibilities.

STA-05.1 | Yes | CSC-owned
Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM?

CSA CCM controls delineated per SSRM in this CAIQ self-assessment, clearly identifying CSP-owned (Atlassian), CSC-owned (Let's Talk Solutions), and shared controls.

STA-06.1 | Yes | CSC-owned
Is the SSRM documentation reviewed and validated?

SSRM documentation (this CAIQ) reviewed and validated as part of the marketplace submission and annually thereafter.

STA-07.1 | Yes | CSC-owned
Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?

CSC-owned portions of the SSRM are implemented and maintained as documented in this self-assessment.

STA-08.1 | Yes | CSC-owned
Is an inventory of all supply chain relationships developed and maintained?

Supply chain inventory maintained: Atlassian Forge platform (primary dependency), npm packages (tracked in package-lock.json), development tools and services.

STA-09.1 | Yes | CSC-owned
Is a process defined, implemented, and enforced for establishing a Bill of Material
for the service supply chain?

Software Bill of Materials (SBOM) maintained through package-lock.json for npm dependencies. Forge platform dependencies managed by Atlassian.

STA-09.2 | Yes | CSC-owned
Is the Bill of Material reviewed and updated at least annually or upon significant changes?

SBOM updated with each release and reviewed annually.

STA-10.1 | Yes | CSC-owned
Are risk factors associated with supply chain relationships periodically reviewed?

Supply chain risks reviewed periodically: dependency vulnerability scanning (automated), Forge platform update impact assessment, npm ecosystem security monitoring.

STA-11.1 | Yes | Shared
Do service agreements between service providers and service customers (tenants) incorporate at least the following mutually agreed upon provisions and/or terms?
* Scope, characteristics, and location of business relationship and services offered
* Information security requirements (including SSRM)
* Change management process
* Logging and monitoring capability
* Incident management and communication procedures
* Right to audit and third-party assessment
* Service termination
* Interoperability a

Service agreements: Atlassian Marketplace Partner Agreement governs the relationship between Let's Talk Solutions and Atlassian. End-user agreements governed through marketplace terms of service.

STA-12.1 | Yes | CSC-owned
Are supply chain agreements reviewed at least annually or upon significant changes?

Supply chain agreements reviewed annually.

STA-13.1 | Yes | CSC-owned
Is there a process for conducting internal assessments at least annually to
confirm the conformance and effectiveness of standards, policies, procedures,
and SLA activities?

Internal assessments conducted annually to confirm conformance with security policies and marketplace requirements.

STA-14.1 | Yes | CSC-owned
Are policies that require all supply chain service providers to comply with information
security, confidentiality, access control, privacy, audit, personnel policy, and
service level requirements and standards implemented?

Supply chain service providers (Atlassian as platform provider) are evaluated for information security compliance. Atlassian maintains SOC 2 Type II and ISO 27001 certifications.

STA-15.1 | Yes | CSC-owned
Are the organization's service providers' IT governance policies and procedures reviewed
at least annually or upon significant changes?

Atlassian's IT governance policies reviewed through their Trust Center and compliance documentation, at least annually.

STA-16.1 | Yes | CSC-owned

Is a process defined and implemented for conducting risk-based security assessments of the supply chain?

Risk-based security assessments of the supply chain conducted focusing on: Forge platform security posture, dependency vulnerability landscape, and npm ecosystem risks.

Threat & Vulnerability Management

TVM-01.1 | Yes | Shared

Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities and threats to protect systems against vulnerability exploitation?

Threat and vulnerability management policies established covering: application-level vulnerability scanning, dependency management, and coordination with Atlassian's platform-level security.

TVM-01.2 | Yes | CSC-owned

Are threat and vulnerability management policies and procedures reviewed and updated at least annually, or upon significant changes?

TVM policies reviewed annually.

TVM-02.1 | Yes | Shared

Are policies and procedures to protect against malware and malicious instructions established, documented, approved, communicated, applied, evaluated, and maintained?

Malware protection at the infrastructure level managed by Atlassian. App-level measures include: dependency vulnerability scanning, code review for malicious patterns, and secure coding practices.

TVM-02.2 | Yes | CSC-owned

Are asset management and malware protection policies and procedures reviewed and updated at least annually, or upon significant changes?

Malware protection policies reviewed annually.

TVM-03.1 | Yes | CSC-owned

Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?

Vulnerability detection implemented through: automated dependency scanning (npm audit, Dependabot/Snyk), Atlassian marketplace security review, and manual code review. Scans run on every build and dependency update.

TVM-04.1 | Yes | CSC-owned

Are a threat analysis process and procedures defined, implemented, and evaluated to identify, assess, and review the threat landscape for cloud systems?

Threat analysis considers: OWASP Top 10 for web applications, Forge-specific attack vectors, supply chain attacks through npm dependencies, and social engineering risks.

TVM-04.2 | Yes | CSC-owned

Are threat models built according to industry best practices to inform the risk mitigation strategy?

Threat models informed by OWASP and Atlassian's Forge security documentation.

TVM-05.1 | Yes | CSC-owned

Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?

Detection tools and threat intelligence updated: dependency scanners automatically updated, vulnerability databases refreshed automatically, Atlassian security advisories monitored.

TVM-06.1 | Yes | CSC-owned

Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the organization's vulnerability management policy)?

Application and dependency updates identified through: automated alerts (Dependabot/Snyk), Forge platform update notifications, and npm security advisories.

TVM-07.1 | NA | CSC-owned

Are processes, procedures and technical measures defined, implemented and evaluated for the periodic performance of penetration testing by independent third parties?

Formal penetration testing is not conducted for this marketplace app due to the Forge sandboxed execution environment. Security testing is performed through automated scanning, code review, and Atlassian's marketplace security review process. Penetration testing would be implemented if the app scope expands significantly.

TVM-08.1 | Yes | Shared

Are processes, procedures and technical measures defined, implemented and evaluated based on identified risks to support scheduled and emergency responses to vulnerability identification?

Vulnerability management processes defined based on identified risks. Forge platform vulnerabilities managed by Atlassian. App-level vulnerability management through automated scanning and timely patching.

TVM-09.1 | Yes | CSC-owned

Is vulnerability remediation prioritized using a risk-based method from an industry-recognized framework?

Vulnerability remediation prioritized using CVSS scoring: Critical (9.0-10.0) - immediate, High (7.0-8.9) - within 72 hours, Medium (4.0-6.9) - within 2 weeks, Low (0.1-3.9) - next planned release.

TVM-10.1 | Yes | CSC-owned

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?

Threat prioritization and mitigation uses CVSS framework for vulnerability scoring and OWASP risk rating methodology for application-specific threats.

TVM-11.1 | Yes | CSC-owned

Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?

Vulnerability tracking through: Jira for remediation tracking, Git history for patch verification, dependency scanning dashboards for ongoing monitoring. Regular reporting of outstanding vulnerabilities.

TVM-12.1 | Yes | CSC-owned

Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?

Metrics tracked: total open vulnerabilities by severity, mean time to remediation, dependency update currency, security scan pass rate.

Universal Endpoint Management

UEM-01.1 | Yes | CSC-owned

Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?

Endpoint management policies established for development workstations used to develop and deploy the Forge app. Covers: OS updates, encryption, access controls, and secure development environment configuration.

UEM-01.2 | Yes | CSC-owned

Are universal endpoint management policies and procedures reviewed and updated at least annually, or upon significant changes?

Endpoint management policies reviewed annually.

UEM-02.1 | Yes | CSC-owned

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?

Approved software list maintained for development endpoints: approved IDEs, development tools, Forge CLI, Git clients, and security scanning tools.

UEM-03.1 | Yes | CSC-owned

Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?

Endpoint device compatibility validated: development machines run supported OS versions compatible with Forge CLI and required development tools.

UEM-04.1 | Yes | CSC-owned

Is an inventory of all endpoints used and maintained to store, access and process company data?

Inventory maintained for development endpoints used to access Forge deployment tools, code repositories, and marketplace admin console.

UEM-05.1 | Yes | CSC-owned

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?

Endpoint policies enforced: OS auto-updates enabled, disk encryption required, screen lock configured, antivirus/EDR active.

UEM-06.1 | Yes | CSC-owned

Are all relevant interactive-use endpoints configured to require an automatic lock screen?

Automatic screen lock configured on all development endpoints (5-minute idle timeout).

UEM-07.1 | Yes | CSC-owned

Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?

Endpoint OS and application updates managed through automatic updates and verified as part of development environment maintenance.

UEM-08.1 | Yes | CSC-owned

Is information protected from unauthorized disclosure on managed endpoints with storage encryption?

Full disk encryption enabled on all development endpoints (FileVault/BitLocker).

UEM-09.1 | Yes | CSC-owned

Are anti-malware detection and prevention technology services configured on managed endpoints?

Anti-malware protection active on all development endpoints with automatic definition updates.

UEM-10.1 | Yes | CSC-owned

Are software firewalls configured on managed endpoints?

Software firewall enabled and configured on all development endpoints.

UEM-11.1 | NA | CSC-owned

Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?

DLP technology not implemented on development endpoints - assessed as proportionate risk given single-developer operation and no customer data stored on endpoints.

UEM-12.1 | NA | CSC-owned

Are remote geo-location capabilities enabled for all managed mobile endpoints, in accordance with applicable laws and regulations?

Remote geo-location not applicable - development endpoints are managed personally by the sole developer/owner.

UEM-13.1 | Yes | CSC-owned

Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?

Remote wipe capability available on development endpoints through OS-level management (Find My Device/similar) for loss/theft scenarios.

UEM-14.1 | Yes | CSC-owned

Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?

Appropriate controls maintained for data on development endpoints: encrypted storage, secure credential management, no customer production data stored on endpoints.