# Security Self-Assessment (CAIQ – Lite)

The framework 'CAIQ-Lite' for cloud vendor assessment is prepared by Cloud Security Alliance consisting of 71 Questions and 16 Control Domains. More info can be found here.

## Application & Interface Security

| Control Heading | Original ID, Question Text | Answer | Notes |
|---|---|---|---|
| Application Security | **AIS-01.2** Do you use an automated source code analysis tool to detect security defects in code prior to production? | Yes | The Snyk service is used for automatic detection of vulnerabilities in code and in the dependencies. In addition, an Atlassian Marketplace process scans all listed apps as given here. |
| Application Security | **AIS-01.5** (SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production? | Yes | The dev team checks against top 10 OWASP common vulnerabilities including XSS, XSRF, query injection, and others automatically identified by Snyk app. |
| Customer Access Requirements | **AIS-02.1** Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems? | Yes | The app serves Atlassian customers that install the app through the Atlassian marketplace. To proceed with installation customers agree with Performance Objectives app's Privacy Policy, SLA and EULA listed on our website. |
| Data Integrity | **AIS-03.1** Does your data management policies and procedures require audits to verify data input and output integrity routines? | Yes | The app has large amount of end-to-end automation testing covering all major functions. The input and output of the app is verified manually with each new code and then automated if it is not done already. The app is subscribed for BugBounty program at BugCrowd where external security engineers scan for issues including data input and output. |

## Audit Assurance & Compliance

| Control Heading | Original ID, Question Text | Answer | Notes |
|---|---|---|---|
| Independent Audits | **AAC-02.1** Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports? | Yes | We don’t have SOC2/ISO 27001 or similar third-party audit. We use Heroku managed infrastructure and their reports can be seen here. We do not share penetration testing reports. Additional info can be provided on client request. |
| Independent Audits | **AAC-02.2** Do you conduct network penetration tests of your cloud service infrastructure at least annually? | Not Applicable | The app uses Heroku managed infrastructure. More details can be found here: Security and Isolation and Security. |
| Independent Audits | **AAC-02.3** Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance? | Yes | Considering the minimum surface of the app based entirely on standard Atlassian components, authorization and API, the testing is handled internally by our engineers. The Heroku Dyno’s application penetration testing can be found here.<br>In addition, we are in enrolled for continuous BugBounty program at BugCrowd.  More details of the Atlassian BugBounty program can be found here. We don’t have formal external penetration testing. |
| Information System Regulatory Mapping | **AAC-03.1** Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements? | Yes | We review regulatory landscape (including GDPR, CCPA) on quarterly bases and adapt our Privacy Policy, EULA and Security Policy when needed. The app does not store customer data and the regulatory requirements rarely impact us. |

## Business Continuity Management & Operational Resilience

| Control Heading | Original ID, Question Text | Answer | Notes |
|---|---|---|---|
| Business Continuity Testing | **BCR-02.1** Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness? | Yes | The business continuity plans are reviewed on annual bases and updated to reflect any significant changes. |
| Policy | **BCR-10.1** Are policies and procedures established and made available for all personnel to adequately support services operations’ roles? | Yes | |
| Retention Policy | **BCR-11.1** Do you have technical capabilities to enforce tenant data retention policies? | Yes | The app stores only license information and no customer data outside clients’ instances. There is a manual data retention process that allows us to wipe license details on request for inactive clients. |
| Retention Policy | **BCR-11.3** Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements? | Yes | There are automated data backups maintained by Heroku service and as redundant backup storage we use the company Google Drive account. |
| Retention Policy | **BCR-11.7** Do you test your backup or redundancy mechanisms at least annually? | Yes | The backup restore process is tested annually to assure our capability to react in case of an incident. |

## Change Control & Configuration Management

| Control Heading | Original ID, Question Text | Answer | Notes |
|---|---|---|---|
| Unauthorized Software Installations | **CCC-04.1** Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems? | Yes | It’s not possible to install arbitrary code into this PAAS environment. GitHub repo stores infrastructure installation instructions and that’s the only route to publish production changes. Heroku instances download the code from GitHub using Heroku built-in function and that is |

| | | | |
|---|---|---|---|
| | | | triggered manually by authorized personnel. Then new releases on the Atlassian Marketplace portal need to be published again by authorized personnel. All DevAcrobats users in these 3 systems (GitHub, Heroku and Atlassian Marketplace) are using MFA authentication. Heroku and Atlassian Marketplace keep logs for each deployment and Atlassian auto notifies on published changes. The security policy is applied on local PCs. Local PCs are assured with Microsoft Intune (MS Endpoint Manager) & MS Defender for Endpoint products and installed software is monitored against approved white list of softwares that can be used by the employees. |

## Data Security & Information Lifecycle Management

| Control Heading | Original ID, Question Text | Answer | Notes |
|---|---|---|---|
| E-commerce Transactions | **DSI-03.1** Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)? | Not Applicable | The app does not provide e-Commerce functions. |
| E-commerce Transactions | **DSI-03.2** Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)? | Not Applicable | The app does not provide e-Commerce functions. Https, SSH, SFTP is always enforced for any data transfer. |
| Nonproduction Data | **DSI-05.1** Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments? | Not Applicable | No replication mechanism of production data. The app does not store any clients' data. |
| Secure Disposal | **DSI-07.1** Do you support the secure deletion (e.g., | Yes | The app does not store any clients' data and no client |

| | | | |
|---|---|---|---|
| | degaussing/cryptographic wiping) of archived and backed-up data? | | data is downloaded locally. If such was sent to us during support process it is stored in our Atlassian service desk, Heroku PaaS or Google Drive and where deletion happens in cryptographically safe way. |
| Secure Disposal | **DSI-07.2** Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource? | Yes | The app does not store any clients' data. More details on retention of customer data received during support process can be found in our Privacy Policy and EULA. |

## Datacenter Security

| Control Heading | Original ID, Question Text | Answer | Notes |
|---|---|---|---|
| Asset Management | **DCS-01.2** Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership? | Yes | Up to date list with assets is kept in company's Google Drive. |
| Controlled Access Points | **DCS-02.1** Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems? | Not Applicable | All the data is on a secured cloud infrastructure. There are no physical assets to restrict or trusted networks. |
| User Access | **DCS-09.1** Do you restrict physical access to information assets and functions by users and support personnel? | Not Applicable | All the data is on a secured cloud infrastructure. There are no physical assets to restrict. The permissions are granted based on user and support functions. |

## Encryption & Key Management

| Control Heading | Original ID, Question Text | Answer | Notes |
|---|---|---|---|
| Key Generation | **EKM-02.1** Do you have a capability to allow creation of unique encryption keys per tenant? | Not Applicable | The app does not store tenant data. Only Performance Objectives license details are stored on Heroku instance per tenant. |
| Encryption | **EKM-03.1** Do you encrypt tenant data at rest (on disk/storage) within your environment? | Not Applicable | The app does not store tenant data. |

## Governance and Risk Management

| Control Heading | Original ID, Question Text | Answer | Notes |
|---|---|---|---|
| Baseline Requirements | **GRM-01.1** Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)? | Not Applicable | We use managed Heroku infrastructure. |
| Policy | **GRM-06.1** Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? | Yes | The Security policy is made available to impacted personnel and listed on our website here. |
| Policy Enforcement | **GRM-07.1** Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures? | Yes | Yes, it is part of employees obligations listed in their labor contracts. |
| Policy Reviews | **GRM-09.1** Do you notify your tenants when you make material changes to your information security and/or privacy policies? | Yes | |

| | | | |
|---|---|---|---|
| Policy Reviews | **GRM-09.2** Do you perform, at minimum, annual reviews to your privacy and security policies? | Yes | |

## Human Resources

| Control Heading | Original ID, Question Text | Answer | Notes |
|---|---|---|---|
| Asset Returns | **HRS-01.1** Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets? | Yes | |
| Background Screening | **HRS-02.1** Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification? | Yes | The employment, educational and clean criminal background are verified with each new employment. The candidates true identity is verified during the interview and hiring process as well. |
| Employment Agreements | **HRS-03.1** Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies? | Yes | |
| Employment Termination | **HRS-04.1** Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? | Yes | |
| Training / Awareness | **HRS-09.5** Are personnel trained and provided with awareness programs at least once a year? | Yes | |

## Identity & Access Management

| Control Heading | Original ID, Question Text | Answer | Notes |
|---|---|---|---|
| Audit Tools Access | **IAM-01.1** Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)? | Yes | Only authorized personnel may access Snyk and Microsoft Intune (MS Endpoint Manager) & MS Defender for Endpoint settings, and access is logged. The app uses Heroku managed infrastructure where hypervisors, firewalls, vulnerability scanners, network sniffers are not accessible even to our most privileged platform users. |
| Audit Tools Access | **IAM-01.2** Do you monitor and log privileged access (e.g., administrator level) to information security management systems? | Yes | |
| User Access Policy | **IAM-02.1** Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes? | Yes | |
| Policies and Procedures | **IAM-04.1** Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access? | Yes | |
| Source Code Access Restriction | **IAM-06.1** Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only? | Yes | The Performance Objectives app uses GitHub private repo and only authorized DevAcrobats personnel have access and all are with MFA enabled. |
| Source Code Access Restriction | **IAM-06.2** Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only? | Yes | |

| | | | |
|---|---|---|---|
| User Access Restriction / Authorization | **IAM-08.1** Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege? | Not Applicable | No customer credentials or any other customer data is stored or provisioned. |
| User Access Reviews | **IAM-10.1** Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function? | Yes | |
| User Access Revocation | **IAM-11.1** Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties? | Yes | |

## Infrastructure & Virtualization Security

| Control Heading | Original ID, Question Text | Answer | Notes |
|---|---|---|---|
| Audit Logging / Intrusion Detection | **IVS-01.1** Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? | Not Applicable | The app uses managed Heroku infrastructure. More details can be found here. |
| Audit Logging / Intrusion Detection | **IVS-01.2** Is physical and logical user access to audit logs restricted to authorized personnel? | Yes | |

| | | | |
|---|---|---|---|
| Audit Logging / Intrusion Detection | **IVS-01.5** Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)? | Yes | We use Heroku managed infrastructure. More details can be found here. In addition, Papertrail service is used that sends automated alerts based on logs. |
| Clock Synchronization | **IVS-03.1** Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? | Yes | Heroku maintains clock synchronization. More details here. |
| OS Hardening and Base Controls | **IVS-07.1** Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template? | Yes | We use Google, Heroku PaaS infrastructure. |
| Production / Non-Production Environments | **IVS-08.1** For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes? | No | We don’t provide test instances to our customers. |
| Production / Non-Production Environments | **IVS-08.3** Do you logically and physically segregate production and non-production environments? | Yes | |
| Segmentation | **IVS-09.1** Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements? | Not Applicable | The app uses standard managed Heroku infrastructure with predefined firewall rules. |
| VMM Security – Hypervisor Hardening | **IVS-11.1** Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through | Yes | It is a must for the authorized DevAcrobats personnel to have MFA authentication enabled for their GitHub, Heroku and Atlassian marketplace systems. |

| | | | |
|---|---|---|---|
| | technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)? | | |
| Wireless Security | **IVS-12.1** Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic? | Not Applicable | We don’t use trusted WiFi or other networks. |
| Wireless Security | **IVS-12.2** Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)? | Not Applicable | We don’t use trusted WiFi or other networks. |
| Wireless Security | **IVS-12.3** Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network? | Not Applicable | We don’t use trusted WiFi or other networks. |

## Interoperability & Portability

| Control Heading | Original ID, Question Text | Answer | Notes |
|---|---|---|---|
| APIs | **IPY-01.1** Do you publish a list of all APIs available in the service and indicate which are standard and which are customized? | Not Applicable | The app does not host own data APIs. It uses Atlassian APIs. |

## Mobile Security

| Control Heading | Original ID, Question Text | Answer | Notes |
|---|---|---|---|
| Approved Applications | **MOS-03.1** Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device? | Not Applicable | We don’t provide company mobile devices. Precautions when using personal devices for work e-mail can be found in Security Policy. |

## Security Incident Management, E-Discovery, & Cloud Forensics

| Control Heading | Original ID, Question Text | Answer | Notes |
|---|---|---|---|
| Incident Management | **SEF-02.1** Do you have a documented security incident response plan? | Yes | |
| Incident Management | **SEF-02.4** Have you tested your security incident response plans in the last year? | Yes | |
| Incident Reporting | **SEF-03.1** Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner? | Yes | |
| Incident Reporting | **SEF-03.2** Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations? | Yes | Support Portal,<br>Email: security@devacrobats.com |
| Incident Response Legal Preparation | **SEF-04.4** Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas? | Yes | |

## Supply Chain Management, Transparency, and Accountability

| Control Heading | Original ID, Question Text | Answer | Notes |
|---|---|---|---|
| Incident Reporting | **STA-02.1** Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)? | Yes | Yes the incidents are reported on DevAcrobats Status Page and updated regularly.<br>Email: security@devacrobats.com. |
| Network / Infrastructure Services | **STA-03.1** Do you collect capacity and use data for all relevant components of your cloud service offering? | Yes | |
| Third Party Agreements | **STA-05.4** Do third-party agreements include provision for the security and protection of information and assets? | Yes | Our third-party providers are Atlassian, Google and Heroku, and it is listed in their terms of services and security policies. |
| Third Party Agreements | **STA-05.5** Do you have the capability to recover data for a specific customer in the case of a failure or data loss? | Yes | The app stores only license details and that's what it can recover. The app configurations are stored on the clients' Atlassian instances. |
| Supply Chain Metrics | **STA-07.4** Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance? | Yes | We provide metrics at DevAcrobats Status Page. |
| Third Party Audits | **STA-09.1** Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met? | Yes | Our third-party providers are Atlassian, Google and Heroku, and we review their policies as part of the annual review process. |

## Threat and Vulnerability Management

| Control Heading | Original ID, Question Text | Answer | Notes |
|---|---|---|---|
| Antivirus / Malicious Software | **TVM-01.1** Do you have anti-malware programs that support or connect to your | Not Applicable | Using Heroku managed web and DB nodes. More info here. |

| | | | |
|---|---|---|---|
| | cloud service offerings installed on all of your IT infrastructure network and systems components? | | Local PC are assured with Microsoft Intune (MS Endpoint Manager) & MS Defender for Endpoint. |
| Vulnerability / Patch Management | **TVM-02.5** Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems? | Yes | Heroku patches automatic web and DB nodes. More details here.<br>Local PC are assured with Microsoft Intune (MS Endpoint Manager) & MS Defender for Endpoint. |
| Mobile Code | **TVM-03.1** Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy? | Not Applicable | We don’t offer native applications for mobile devices. |