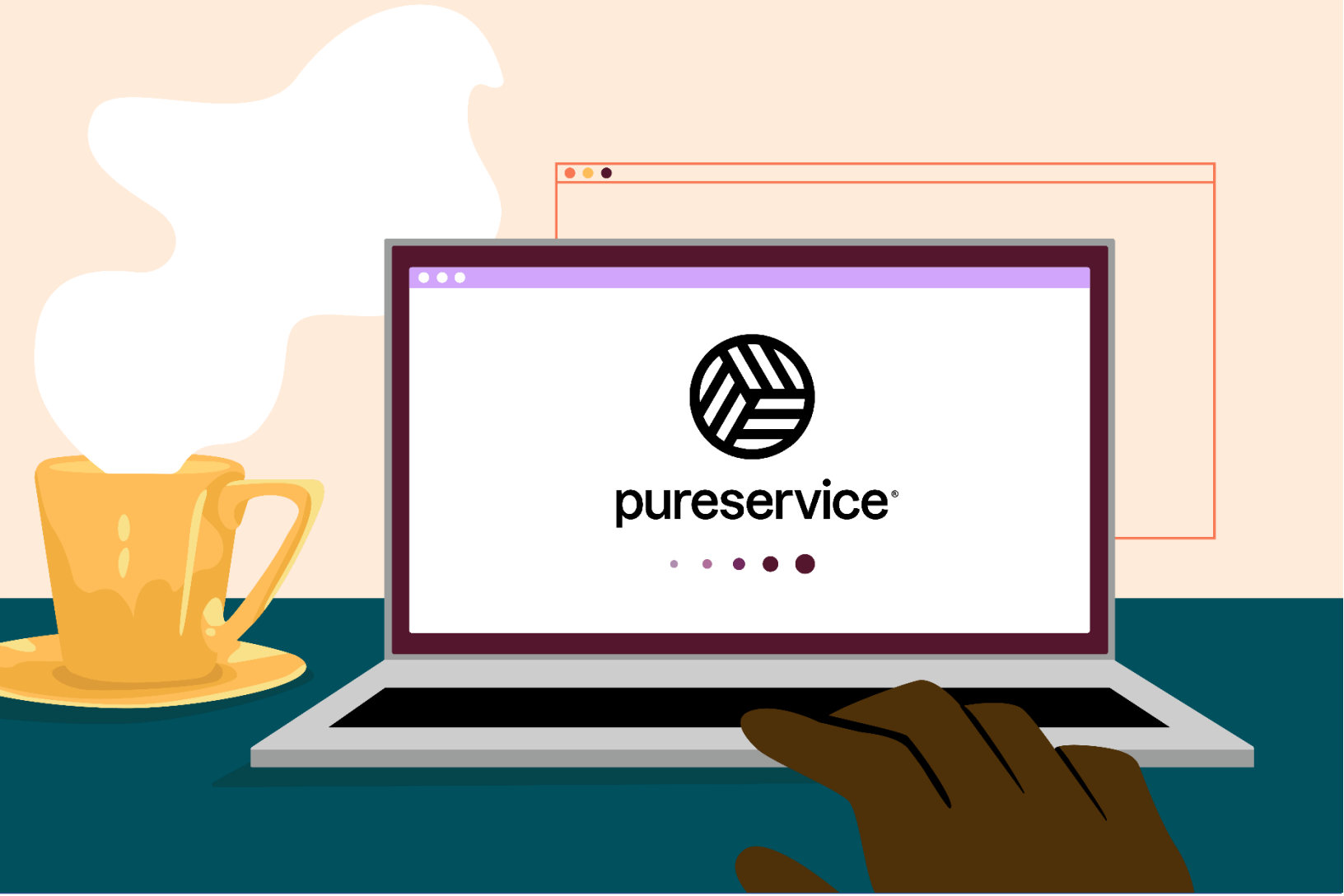
CSA CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE (CAIQ) – LITE V3.0.1



Notice

This information is provided for evaluation purposes only, so your organization may review Pureservice's security processes and controls to determine whether the products and services meet your needs. This questionnaire is not made part of any agreement you may sign with Pureservice AS, and does not constitute a representation or warranty on the part of Pureservice AS.

Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to "promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing".

Sections

- Application and Interface Security (AIS)
- Audit Assurance and Compliance (AAC)
- Business Continuity Management and Operational Resilience (BCR)
- Change Control and Configuration Management (CCC)
- Data Security and Information Lifecycle Management (DCI)
- Datacenter Security (DCS)
- Encryption and Key Management (EKM)
- Governance and Risk Management (GRM)
- Human Resources Security (HRS)
- Identity and Access Management (IAM)
- Infrastructure and Virtualization (IVS)
- Interoperability and Portability (IPY)
- Mobile Security (MOS)
- Security Incident Management, E-Disc & Cloud Forensics (SEF)
- Supply Chain Management, Transparency & Accountability (STA)
- Threat and Vulnerability Management (TVM)

The questionnaire has been completed using the current CSA CAIQ-Lite standard, v3.0.1.

ID	Question	Answer			Notes/Comment
		YES	NO	N/A	
AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?		X		We are currently working on enabling automated code analysis as a part of our deployment and release process. As a compensating action, the development team analyses and updates external third-party libraries at a regular basis.
AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X			Each code change that touches security features in the application is code reviewed by another senior peer and tested thoroughly in a staging environment before being deployed to production environments.
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?	X			The customer agreement, data processor agreement, security- and privacy policies provide this.
AIS-03.1	Does your data management policies and procedures require audits to verify data input and output integrity routines?	X			Data integrity is ensured via automated validation checks, input, and output sanitation in our APIs and both manual end-to-end and automated testing. All data is backed up with point-in-time restore to ensure minimal data loss in the event of an integrity error. Database schemas and migration scripts are machine-generated, and source controlled to minimize human errors.
AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	X			An independent third-party report related to audit and certification can be provided on demand. As we're a Microsoft Azure tenant, information about certifications in Microsoft Azure is available here: https://docs.microsoft.com/en-us/azure/compliance/
AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure at least annually?	X			External vulnerability threat assessments are conducted on an annual cadence by a third-party independent security firm. The

					development team follows the OWASP guidelines.
AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	X			Application penetration tests are conducted on an annual cadence by a third-party security firm. Identified vulnerabilities are remediated and re-tested by the third-party security firm.
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?	X			We review the regulatory landscape on a quarterly basis and make changes to our internal policies & documentation as needed.
BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X			The business continuity and disaster recovery plans are reviewed annually, and the disaster recovery plan is tested annually.
BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	X			Policies regarding operations, data use and security are made available to all relevant employees. DevOPS- and development personnel rotate into support roles on a regular basis to stay up to date on how to support our customer and control our services.
BCR-11.1	Do you have technical control capabilities to enforce tenant data retention policies?	X			Technical controls enforcing data retention policies are set and automated in our cloud infrastructure.
BCR-11.3	Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	X			
BCR-11.7	Do you test your backup or redundancy mechanisms at least annually?	X			

CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	X			The provisioning of infrastructure is automated, and our customers are not able to install software onto our systems. All human-driven activity in our cloud infrastructure is monitored and audited.
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)?	X			All traffic to and from the application is encrypted via the TLS 1.2 protocol, an open encryption standard.
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)?			X	Traffic to and from infrastructure components on public networks is encrypted via the TLS 1.2 protocol, an open encryption standard.
DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	X			Access to production systems and data is restricted to our own DevOps- and CSIRT teams. These teams are only authorized to access customer data during ongoing support-requests or in failure analysis situations. All data is encrypted at rest and no customer data resides outside of the production environment.
DSI-07.1	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?	X			Encrypted data backups are retained for 28 days and then automatically deleted. This control is inherited from our cloud infrastructure provider.
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?	X			Exiting the service agreement and sanitation of customer data is covered in our Data Processing Agreement.

DCS-01.2	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	X			All services (assets) are monitored and owned by the DevOps team.
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?	X			This control is inherited from our cloud infrastructure provider. See: https://azure.microsoft.com/en-us/resources/microsoft-azure-responses-to-cloud-security-alliance-consensus-assessments-initiative-questionnaire-v301/
DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	X			This control is inherited from our cloud infrastructure provider Microsoft Azure. See: https://azure.microsoft.com/en-us/resources/microsoft-azure-responses-to-cloud-security-alliance-consensus-assessments-initiative-questionnaire-v301/
EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?			X	Tenant provided encryption keys would not be relevant for our application.
EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	X			All non-transient customer data at rest is encrypted using 256-bit AES encryption using customer managed keys (CMK). All encryption related keys are safely stored in our Azure Key Vault.
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.)?	X			All infrastructure is based on services provided by our cloud infrastructure provider. Our cloud infrastructure provider is in alignment of ISO 27001 standards and all components of our infrastructure includes a default security baseline.
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	X			Both Pureservice and our main service/hosting provider (MS Azure) has security and privacy policies that align with ISO27001/27701 and other industry standards. For more details see Pureservice Security Policy and Microsoft compliance

	information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?				documentation: https://docs.microsoft.com/en-us/azure/compliance/
GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			Covered by data-use policy, our employee handbook and internal security policy for employees.
GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	X			Any changes to our information security and privacy policies are published on our website.
GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	X			We review our privacy and security policies at least twice a year.
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?	X			
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?	X			All employees undergo a background verification as a condition of employment.
HRS-03.1	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	X			All employees are trained to their specific role and trained in our security- and data use policies.
HRS-04.1	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	X			We have implemented a documented procedure and checklists for both on-boarding and off-boarding employees.
HRS-09.5	Are personnel trained and provided with awareness	X			Pureservice has a continuous awareness program for security in place. This includes but is not limited to: safety awareness

	programs at least once a year?				information issued throughout the year, internal phishing tests and other information sharing on all internal communication channels (e-mail, teams, posters in the office, meetings etc).
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.)?	X			Systems that impact production applications are restricted to authorized personnel. Managed systems that are delivered by our cloud infrastructure are in alignment with ISO 27001 standards.
IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	X			Systems that impact production applications are restricted to authorized personnel. Managed systems that are delivered by our cloud infrastructure are in alignment with ISO 27001 standards.
IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	X			All access is managed through infrastructure identities which are disabled and in turn deleted when employees no longer need access, e.g., during an employee offboarding process. Access to our cloud infrastructure is limited.
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?	X			The DevOps team uses AAD to manage and track all cloud infrastructure access.
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?	X			The development team utilizes Azure DevOps for its source control needs and team members and other employees with business needs have access. Identity and access control is maintained in AAD.
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?	X			The application provides several means of control to the customer to configure application authorization and authentication. Customers do not have access to application source code.
IAM-08.1	Do you document how you grant and approve access to tenant data?	X			The DevOps team manage and track all cloud infrastructure access to tenant data. External access to tenant data is secured using the “Customer Lockbox” feature

					provided by our cloud infrastructure provider. See: https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview
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?	X			We have implemented a documented procedure and checklists for both on- and off-boarding employees. A revision of user access is performed during an off-boarding event, and during internal auditing several times a year.
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?	X			
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?	X			Our cloud infrastructure provider has tools in place to detect such events.
IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	X			Access to logs is restricted to members of the DevOps-team.
IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)	X			
IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	X			Our cloud infrastructure provides this.

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?	x			Services built in our cloud infrastructure comes with a baseline standard for hardening.
IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	x			Testing environments are available for customers upon request.
IVS-08.3	Do you logically and physically segregate production and non-production environments?	x			Our dev-, test- and production environments are separated by controls provided by our cloud provider, such as separate namespaces, environment, and subscriptions.
IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	X			
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 technical controls (e.g., twofactor authentication, audit trails, IP address filtering, firewalls and TLSencapsulated communications to the administrative consoles)?	x			Only members of the DevOps team have access to management functions in our cloud infrastructure. Access is secured using two-factor authentication.
IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and			x	As a cloud tenant our wireless networks are not connected to our cloud infrastructure in any way.

	to restrict unauthorized wireless traffic?				
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)?			X	As a cloud tenant our wireless networks are not connected to our cloud infrastructure in any way.
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?			X	As a cloud tenant our wireless networks are not connected to our cloud infrastructure in any way.
IPY-01.1	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	X			The API-documentation is maintained and available to customers. See: https://api-docs.pureservice.com/
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?			X	We do not issue mobile devices to employees.
SEF-02.1	Do you have a documented security incident response plan?	X			Our CSIRT team have a documented incident response plan.
SEF-02.4	Have you tested your security incident response plans in the last year?	X			Our CSIRT team exercise and reviews our incident response plan at a regular basis.
SEF-03.1	Does your security information and event management (SIEM) system merge data	X			Our cloud provider provides such tooling. Analysis and alerting capabilities are built into every service and reported on in an automated and granular manner.

	sources (e.g., app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?				
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?	X			Every customer has its own logging namespace and storage. Each customer-specific component in our cloud environment is tagged with customer identification which allows for easy isolation in the case of an incident event.
SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X			All customer data is stored encrypted and isolated from other customers data.
STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?		X		Incident reports are available upon request.
STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	X			Several mechanisms are in place to collect capacity and use data metrics.
STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	X			All third-party providers have a data processing agreement or other public terms and policies that includes security and protection of information and assets.
STA-05.5	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	X			Geo redundant point-in-time recovery (PITR) backups are taken continuously, and the retention policy is 28 days for each individual database. This enables the capability to restore a specific customer's data down to second precision in the event of failure or data loss.
STA-07.4	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	X			This information is issued on request along with any incident report if applicable.

STA-09.1	Do you permit tenants to perform independent vulnerability assessments?	X			Customers may perform independent vulnerability assessments on our public facing interfaces upon request.
TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	X			Services running Microsoft Windows have antivirus installed. Our cloud provider ensures that all components and systems are kept up to date.
TVM-02.5	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?	X			The DevOps team have the capabilities to patch all services through our automated deploy and release process.
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?			X	We don't issue employees with mobile technology such as mobile phones or tablets that have access to our infrastructure.

Glossary

DevOps: DevOps is a set of practices that combines software development (Dev) and IT operations (Ops).
OWASP: The Open Web Application Security Project.
CSIRT: Computer Security Incident Response Team.

Document history

08.12.2021	Document created
07.01.2022	IAM-08.1 - Added information about “Customer Lockbox”.
18.02.2022	EKM-02.1/03.1 - Clarified information regarding encryption keys and storage of these.
21.06.2022	- Added section list AAC-02.1 - Changed expected availability for audit reports. EKM-02.1 - Changed to N/A as this is not relevant for our application. STA-05.5/07.4 - Added missing answer, "Yes". HRS-09.5 - Safety awareness information is issued throughout the year. Not limited to a single month.
09.11.2022	DSI-05.1 - Clarified information regarding customer data access.
06.12.2023	EKM-03.1 - Encryption key information for platform changed from “platform managed” to “customer managed”. AAC-02.1 - Audit and certification report available on demand.