CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	JobAdder's Information Security Management System (ISMS) is certified to ISO/IEC 27001:2022 by LRQA. Our ISMS includes a framework of documented, communicated, and maintained policies, procedures, and standards.		Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.		
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed and approved by JobAdder leadership at least annually, or more frequently as needed.	A&A-01		Audit and Assurance Policy and Procedures	
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes	CSP-owned	JobAdder undergoes annual surveillance and recertification audits by LRQA (ISO 27001:2022). Additionally, annual penetration testing is performed by independent CREST-certified testers.	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Independent Assessments	
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes	CSP-owned	The scope and priority of our internal and external audit programs are determined by our formal risk management framework, aligned with ISO 27005.	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	Risk Based Planning Assessment	
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Yes	CSP-owned	JobAdder's legal counsel monitors the legal, statutory, and regulatory landscape. Compliance is verified as part of our internal and external audit processes.	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	Requirements Compliance	
A&A-05.1	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?	Yes	CSP-owned	JobAdder's ISMS includes a formal audit management process aligned with ISO 27001 covering planning, risk analysis, reporting, and evidence retention.	A&A-05	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	Audit Management Process	
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	All audit findings are tracked as corrective actions in a central ticketing system. Remediation plans are established and prioritised based on risk.		Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.		
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	Yes	CSP-owned	The status of corrective actions is tracked and reported to key stakeholders during quarterly security committee meetings and annual ISMS Management Review meetings.	A&A-06		Remediation	Audit & Assurance
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security	Yes	CSP-owned	Our ISO 27001 certified ISMS includes documented policies and standards governing our Secure SDLC, communicated to all development personnel.		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually.		
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	All application security policies and procedures are reviewed annually by JobAdder leadership at least annually, or more frequently as needed.	AIS-01		Application and Interface Security Policy and Procedures	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes	CSP-owned	JobAdder maintains documented secure baseline configurations for applications and infrastructure, aligned with industry best practices as part of our ISO 27001 ISMS certified requirements.	AIS-02	Establish, document and maintain baseline requirements for securing different applications.	Application Security Baseline Requirements	
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes	CSP-owned	Jobadder defines and monitors security metrics (e.g. vulnerabilitiy remediation SLAs, incident response times) aligned with busines objectives and our ISO 27001 framework	AIS-03	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	Application Security Metrics	
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security	Yes	CSP-owned	JobAdder has a defined and documented System Development Life Cycle (SDLC) that is aligned OWASP secure coding best practices as part of our ISO 27001 certified ISMS, including secure design, development, code review, testing, and release.	AIS-04	Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	Secure Application Design and Development	
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Yes	CSP-owned	Our SDLC. integrated testing strategy includes SAST, SCA, DAST, and annual penetration by CREST-certified testers to ensure application security and compliance.	AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.	Automated Application Security Testing	
AIS-05.2	Is testing automated when applicable and possible?	Yes	CSP-owned	As per our System Development Life Cycle (SDLC), automated security testing, including SAST and SCA, is integrated into our CI/CD pipeline for every code change.				
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes	CSP-owned	Deployment is governed by our secure SDLC, using a standardised pull-request model with peer review, automated security scanning, and formal change management.	AIS-06	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Automated Secure Application Deployment	
AIS-06.2	Is the deployment and integration of application code automated where possible?	Yes	CSP-owned	Automated tools are used where feasible throughout JobAdder's Software Development Life Cycle.				
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes	CSP-owned	All security vulnerabilites are tracked, risk-prioritised, and remediated prior to deployment. Production issues are managed via a formal remediation procedure.	AIS-07	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.	Application Vulnerability Remediation	Application & Interface Security
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	Yes	CSP-owned	Vulnerability detection is automated; remediation is a developer-led process involving code review and testing to ensure effectiveness and stability.				
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	JobAdder maintains formal Business Continuity Program (BCP) and Disaster Recovery Plan (DRP) plans as part of our ISO 27001 certified ISMS, documented and available to relevant personnel. Reviewed annually or when a significant change occurs.	BCR-01	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually.	Business Continuity Management Policy and Procedures	
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.				

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes	CSP-owned	JobAdder's business continuity strategy includes a formal Business Impact Assessment (BIA) to evaluate potential disruption scenarios and define RTOs/RPOs for critical systems.	BCR-02	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.	Risk Assessment and Impact Analysis	
BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	Yes	CSP-owned	Jobadder's BCP is based on establishing and maintaining high availability and automated recovery for customer facing services. The program is managed by JobAdder's Technology and Engineering team and implemented in coordination with all major lines of business, with oversight from senior management.	BCR-03	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.	Business Continuity Strategy	
BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a	Yes	CSP-owned	Resilient architecture capabilities (e.g., multi-AZ deployment, automated backups, data replication) are documented and form the foundation of our BCP and DRP.	BCR-04	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.	Business Continuity Planning	
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	Yes	CSP-owned	JobAdder maintains all relevant documentation to support our BCP and DRP, including key procedures, system architecture diagrams, and emergency contact lists.	BCR-05	Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review periodically.	Documentation	
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes	CSP-owned	Documentation is stored centrally in our internal wiki and accessible to authorised personnel.				
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Yes	CSP-owned	All BCP and DRP documentation is reviewed annually to ensure it remains current and effective.				
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	Yes	CSP-owned	BCP and DRP are tested annually or when significant changes occur. Each annual test validates recovery objectives defined in our BIA.	BCR-06	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	Business Continuity Exercises	
BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	Yes	CSP-owned	JobAdder's BCP establishes communication plans including notifying affected customers via our public status page and direct outreach as appropriate.	BCR-07	Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.	Communication	
BCR-08.1	Is cloud data periodically backed up?	Yes	CSP-owned	Production databases are backed up weekly (full), nightly (differential), and every 15 minutes (transaction logs). Backups are retained for 60 days and encrypted at rest using AWS server-side encryption.	BCR-08	Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.	Backup	
BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	Yes	CSP-owned	See BCR-08.1.				
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	CSP-owned	Backups are tested periodically to confirm successful restoration and system resiliency.				

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	Yes	CSP-owned	JobAdder maintains a documented and approved Disaster Recovery Plan that is tested and reviewed annually.		Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.		
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.	BCR-09		Disaster Response Plan	
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes	CSP-owned	See BCR-09.1		Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities.		
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	Yes	CSP-owned	As a cloud-native SaaS provider, disaster recovery exercises focus on AWS service restoration. Physical site recovery is managed by AWS.	BCR-10		Response Plan Exercise	
BCR-11.1	Is business-critical equipment supplemented with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards?	Yes	CSP-owned	Core infrastructure is hosted on AWS, utilising multiple Availability Zones (AZs) to ensure redundancy for business-critical systems.	BCR-11	Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.	Equipment Redundancy	Business Continuity Management and Operational Resilience
CCC-01.1	Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless	Yes	CSP-owned	JobAdder maintains a formal Risk Management Program aligned with ISO 27001. Risks associated with changes are identified, assessed, and tracked through a Risk Register.		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.		
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.	CCC-01		Change Management Policy and Procedures	
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Yes	CSP-owned	All changes follow a defined quality control process including peer review, automated security checks, and testing. Major changes require a formal change ticket and approval.	CCC-02	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.	Quality Testing	
CCC-03.1	Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?	Yes	CSP-owned	All changes to JobAdder's assets including applications, systems, infrastructure, and configurations are subject to risk assessment. Our Change Management Policy ensures risks are identified, assessed, and mitigated prior to implementation.	CCC-03	All changes to Jobadder's asset including applications, systems, infrastructure, and configurations are subject to risk assessment and management. Our Change Management Policy, aligned with our ISO 27001, ensures risks are identified, assessed and mitigated for all changes.	Change Management Technology	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes	CSP-owned	Unauthorised changes are restricted through role-based access control, formal change management, and MDM for corporate assets.	CCC-04	Restrict the unauthorized addition, removal, update, and management of organization assets.	Unauthorized Change Protection	
CCC-05.1	Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs?	Yes	CSP-owned	Material changes impacting customers are communicated in accordance with our customer agreements and SLAs.	CCC-05	Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.	Change Agreements	
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes	CSP-owned	Secure baseline configurations are established and maintained for all JobAdder assets. Changes are evaluated against these baselines.	CCC-06	Establish change management baselines for all relevant authorized changes on organization assets.	Change Management Baseline	
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Yes	CSP-owned	We use automated tools to monitor for configuration changes that deviate from established baselines. Alerts are sent to the relevant engineering team.	CCC-07	Implement detection measures with proactive notification in case of changes deviating from the established baseline.	Detection of Baseline Deviation	
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes	CSP-owned	A formal exception process is defined within our Change Management Policy for managing deviations or emergency changes.		'Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.'		
CCC-08.2	Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?'	Yes	CSP-owned	All changes are managed through a formal process including risk assessment and approval. Emergency changes are logged and subject to retrospective review.	CCC-08		Exception Management	
CCC-09.1	Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?	Yes	CSP-owned	Automated deployment processes include the ability to roll back changes to a previously known stable state in the event of deployment errors.	CCC-09	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.	Change Restoration	Change Control and Configuration Management
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	A formal policy for cryptography, encryption, and key management is established and maintained as part of our ISO 27001 certified ISMS.		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually.		
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.	CEK-01		Encryption and Key Management Policy and Procedures	
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes	CSP-owned	Roles and responsibilities for cryptography and key management are defined in our ISMS and assigned to relevant engineering personnel.	CEK-02	Define and implement cryptographic, encryption and key management roles and responsibilities.	CEK Roles and Responsibilities	
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes	CSP-owned	Data in transit is protected using TLS 1.3. Data at rest is encrypted using AWS server-side encryption (AES-256).	CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.	Data Encryption	
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Yes	CSP-owned	Encryption algorithms are selected based on data classification, risk assessment, and technology suitability.	CEK-04	Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.	Encryption Algorithm	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
CEK-05.1	Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and	Yes	CSP-owned	Changes to cryptographic configurations are managed through our formal Change Management Policy.	CEK-05	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.	Encryption Change Management	
CEK-06.1	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?	Yes	CSP-owned		CEK-06	Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.	Encryption Change Cost Benefit Analysis	
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	Yes	CSP-owned	Cryptographic risks are managed within our broader ISO 27001 Risk Management Framework, ensuring continuous monitoring and treatment.	CEK-07	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	Encryption Risk Management	
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	Yes	CSP-owned	Customers do not have the capacity to manage their own encryption keys.	CEK-08	CSPs must provide the capability for CSCs to manage their own data encryption keys.	CSC Key Management Capability	
CEK-09.1	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?	Yes	CSP-owned	Encryption systems are audited at least annually and after any significant security event as part of our ISMS audit program.	CEK-09	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s).	Encryption and Key Management Audit	
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Yes	CSP-owned	See CEK-09.1.				
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Yes	CSP-owned	Cryptographic keys are generated using industry-accepted cryptographic libraries (via AWS KMS) specifying algorithm strength and random number generation.	CEK-10	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	Key Generation	
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes	CSP-owned	Private keys are managed via AWS Key Management Service (KMS), ensuring unique provisioning, strict access controls, and secrecy.	CEK-11	Manage cryptographic secret and private keys that are provisioned for a unique purpose.	Key Purpose	
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Yes	CSP-owned	Keys are rotated automatically on a recurring schedule managed by AWS KMS, in compliance with industry standards.	CEK-12	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.	Key Rotation	
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and	Yes	CSP-owned	Processes are in place to revoke keys immediately if compromised or no longer needed, using AWS KMS key management features.	CEK-13	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.	Key Revocation	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
CEK-14.1	Are processes, procedures and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable	Yes	CSP-owned	Key destruction is managed via AWS KMS, which handles the secure deletion of key material in accordance with NIST standards.	CEK-14	Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements.	Key Destruction	
CEK-15.1	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?	Yes	CSP-owned	Forms part of our processes and technical measures as part of our ISO 27001 certified ISMS.	CEK-15	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.	Key Activation	
CEK-16.1	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?	Yes	CSP-owned	Key state transitions are monitored and logged via AWS CloudTrail, ensuring visibility into all key management activities.	CEK-16	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.	Key Suspension	
CEK-17.1	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?	Yes	CSP-owned	Procedures are in place to disable keys upon expiration or when no longer required, preventing further cryptographic operations.	CEK-17	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.	Key Deactivation	
CEK-18.1	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	Yes	CSP-owned	Forms part of our processes and technical measures as part of our ISO 27001 certified ISMS.	CEK-18	Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.	Key Archival	
CEK-19.1	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?	Yes	CSP-owned	Compromised keys are immediately disabled and used only for decryption (recovery) purposes in a controlled environment, never for new encryption.	CEK-19	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.	Key Compromise	
CEK-20.1	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?	Yes	CSP-owned	Forms part of our processes and technical measures as part of our ISO 27001 certified ISMS.	CEK-20	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.	Key Recovery	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
CEK-21.1	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?	Yes	CSP-owned	Forms part of our processes and technical measures as part of our ISO 27001 certified ISMS.	CEK-21	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.	Key Inventory Management	Cryptography, Encryption & Key Management
DCS-01.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	Yes	CSP-owned	Policies and procedures for the secure disposal of equipment are established and maintained in accordance with our Asset Management Policy.	DCS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually.	Off-Site Equipment Disposal Policy and Procedures	
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Yes	CSP-owned	A data destruction procedure is applied that renders information recovery impossible if equipment is not physically destroyed, as specified in our Asset Management Policy.				
DCS-01.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.				
DCS-02.1	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?	Yes	CSP-owned	Policies for the relocation or transfer of hardware and data are established and maintained in accordance with our Asset Management Policy.	DCS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually.	Off-Site Transfer Authorization Policy and Procedures	
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	Yes	CSP-owned	A relocation or transfer request requires written authorisation, as specified in our Asset Management Policy.				
DCS-02.3	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?	Yes	CSP-owned	See DCS-01.3.				

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	Yes	CSP-owned	JobAdder maintains policies and procedures for physical security in accordance with our ISO 27001 certification.	DCS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually.	Secure Area Policy and Procedures	
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.				
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	Yes	CSP-owned	Policies for secure transportation of media are reviewed and approved by JobAdder leadership at least annually.	DCS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually.	Secure Media Transportation Policy and Procedures	
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.				
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Yes	CSP-owned	Physical and logical assets are classified based on business risk in accordance with our Information Classification Policy and Asset Management Procedure.	DCS-05	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.	Assets Classification	
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Yes	CSP-owned	All relevant physical and logical assets are catalogued and tracked within a secured system (Asset Panda for hardware, internal registers for logical assets).	DCS-06	Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.	Assets Cataloguing and Tracking	
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	Yes	Shared CSP and CSC	Physical security perimeters for data centres are managed by AWS. JobAdder manages physical security for its corporate offices / co-working spaces using access cards and perimeter controls.	DCS-07	Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas.	Controlled Access Points	
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	Yes	CSP-owned	See DCS-07.1.				
DCS-08.1	Is equipment identification used as a method for connection authentication?	Yes	CSP-owned	All devices and laptops are assigned unique item tags as identifiers in accordance with our Asset Management Procedure.	DCS-08	Use equipment identification as a method for connection authentication.	Equipment Identification	
DCS-09.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	Yes	3rd-party outsourced	Physical access is managed by AWS as part of their data centre security controls. JobAdder employees do not have physical access to data centres.	DCS-09	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.	Secure Area Authorization	
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Yes	CSP-owned	Logical access control records are retained in accordance with our Access Control Policy.				

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Yes	3rd-party outsourced	Managed by AWS as part of their third-party data centre controls.	DCS-10	Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.	Surveillance System	
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	Yes	3rd-party outsourced	Managed by AWS as part of their third-party data centre controls.	DCS-11	Train datacenter personnel to respond to unauthorized ingress or egress attempts.	Unauthorized Access Response Training	
DCS-12.1	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?	Yes	3rd-party outsourced	Managed by AWS. JobAdder relies on AWS's physical security controls for power and cabling protection within data centres.	DCS-12	Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.	Cabling Security	
DCS-13.1	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	Yes	3rd-party outsourced	Managed by AWS as part of their third-party data centre controls.	DCS-13	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	Environmental Systems	
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	Yes	3rd-party outsourced	Utility services are managed by AWS for data centre infrastructure. JobAdder responsible for logical and application-level controls.	DCS-14	Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.	Secure Utilities	
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	Yes	3rd-party outsourced	All business-critical equipment is hosted with AWS, which ensures physical segregation from high-risk locations as part of their data centre controls.	DCS-15	Keep business-critical equipment away from locations subject to high probability for environmental risk events.	Equipment Location	Datacenter Security
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	Yes	CSP-owned	Policies and procedures for data classification, protection, and handling are established and maintained in accordance with applicable laws, regulations, and standards.		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.		
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.	DSP-01		Security and Privacy Policy and Procedures	
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Yes	Shared CSP and 3rd-party	Industry-accepted methods for secure data disposal are applied by JobAdder and AWS to ensure information is not recoverable (e.g., NIST 800-88).	DSP-02	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.	Secure Disposal	
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Yes	CSP-owned	JobAdder maintains a centralised Systems/Application register tracking system ownership, data location and classification which sensitive and personal information (DC3/DC4) is labelled in accordance with JobAdder's policies and ISO 27001.	DSP-03	Create and maintain a data inventory, at least for any sensitive data and personal data.	Data Inventory	
DSP-04.1	Is data classified according to type and sensitivity levels?	Yes	CSP-owned	Data is classified according to type and sensitivity levels (e.g., DC1, DC2, DC3, DC4) in accordance with JobAdder's Information Classification Policy.	DSP-04	Classify data according to its type and sensitivity level.	Data Classification	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Yes	CSP-owned	Data flow documentation is created to identify what data is processed, stored, and transmitted, and is updated during the Secure SDLC process.	DSP-05	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.	Data Flow Documentation	
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Yes	CSP-owned	Data flow documentation is reviewed at least annually and after any significant change.				
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Yes	CSP-owned	Ownership and stewardship of all relevant personal and sensitive data are documented in accordance with JobAdder's policies.	DSP-06	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.	Data Ownership and Stewardship	
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	Yes	CSP-owned	Data ownership documentation is reviewed annually as part of our ISO 27001 risk management process.				
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Yes	CSP-owned	JobAdder products comply with Secure Development guidelines (OWASP Top 10) and security-by-design principles.	DSP-07	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.	Data Protection by Design and Default	
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Yes	CSP-owned	Privacy-by-design principles are integrated into our engineering process, including legal review of new data collection mechanisms.	DSP-08	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	Data Privacy by Design and Default	
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	Yes	CSP-owned	Privacy settings are configured by default to ensure compliance. Features are provided to assist customers with consent management.				
DSP-09.1	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?	Yes	CSP-owned	As part of our ISO 27001 certification, privacy and risk management policies are assessed and reviewed frequently to evaluate risks. The responsibility to conduct a DPIA rests primarily with the data controller (the recruiter/company) if their data processing activities are likely to result in a high risk to the rights and freedoms of individuals (as defined under GDPR Article 35).	DSP-09	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.	Data Protection Impact Assessment	
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	Yes	CSP-owned	Transfers of personal data are protected via encryption (TLS 1.2 +) and access is restricted to authorised personnel on a least-privilege basis.	DSP-10	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Sensitive Data Transfer	
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	Yes	CSP-owned	JobAdder provides features to assist customers in managing data subject requests for access, modification, or deletion.	DSP-11	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.	Personal Data Access, Reversal, Rectification and Deletion	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data	Yes	CSP-owned	As the Data Controller, the Customer is responsible for obtaining their own legal advice on when privacy consents are appropriate and applicable. JobAdder (as Data Processor) provides features to assist with compliance (e.g., "Pending Candidates" state) but relies on the Customer to obtain necessary consents for data collection.	DSP-12	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	Limitation of Purpose in Personal Data Processing	
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable	Yes	CSP-owned	JobAdder provides a current list of all sub-processors under the GDPR compliance section of the Trust Centre. For candidate information (i.e., information stored in the system), we only engage sub-processors for the EEA that are located in the EEA.	DSP-13	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	Personal Data Sub-processing	
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	Yes	CSP-owned	Customers may object to the use of a new sub-processor by notifying JobAdder in writing (dataprivacy@jobadder.com) within ten (10) business days of the updated list being published on the Trust Centre. If an objection is raised, we will use reasonable efforts to resolve reasonable objection(s). If no objection is received within the specified period, the use of the new sub-processor(s) is deemed agreed.	DSP-14	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.	Disclosure of Data Sub-processors	
DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	Yes	CSP-owned	We do not permit the use of production data in non-production environments.	DSP-15	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.	Limitation of Production Data Use	
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes	CSP-owned	Data retention, archiving, and deletion are managed in accordance with JobAdder's Data Retention Policy and data schedules.	DSP-16	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	Data Retention and Deletion	
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Yes	CSP-owned	Sensitive data is protected via AES-256 encryption at rest (DB/S3) and strict access controls throughout its lifecycle.	DSP-17	Define and implement, processes, procedures and technical measures to protect sensitive data throughout it's lifecycle.	Sensitive Data Protection	
DSP-18.1	Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations?	Yes	CSP-owned	JobAdder maintains a procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities. We give special attention to the notification procedure to interested Customers, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.		The CSP must have in place, and describe to CSCs the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations. The CSP must give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.		
DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?	Yes	CSP-owned	Customers are notified of law enforcement data requests unless prohibited by law, as required by our ISO 27001 policies.	DSP-18		Disclosure Notification	
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	Yes	CSP-owned	We document physical data locations (AWS Regions) where data is processed and backed up.	DSP-19	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.	Data Location	Data Security and Privacy Lifecycle Management

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Our ISMS and Information Security Policy are fully endorsed by the CEO and communicated to all employees, establishing the framework for our ISO 27001 certification.		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.		
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.	GRC-01		Governance Program Policy and Procedures	
GRC-02.1	Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?	Yes	CSP-owned	Risk identification, ownership, assessment, and treatment are documented and enforced via our Risk Management Policy and Procedure (aligned with ISO 27005). The Risk Register is managed in Jira and reviewed regularly.	GRC-02	Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.	Risk Management Program	
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Yes	CSP-owned	All relevant organisational policies and associated procedures are reviewed at least annually or upon significant changes, as required by our ISO 27001 certified ISMS.	GRC-03	Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.	Organizational Policy Reviews	
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Yes	CSP-owned	An approved exception process is mandated and documented in our Information Security Policy	GRC-04	Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.	Policy Exception Process	
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Yes	CSP-owned	An information security program has been developed and implemented in accordance with our ISO/IEC 27001:2022 certified ISMS.	GRC-05	Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.	Information Security Program	
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes	CSP-owned	Roles and responsibilities for the information security program are defined and documented in our ISMS and Information Security Policy.	GRC-06	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	Governance Responsibility Model	
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Yes	CSP-owned	All relevant standards, regulations, and legal requirements are identified and documented by the General Counsel in a Legal & Compliance register.	GRC-07	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.	Information System Regulatory Mapping	
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	Yes	CSP-owned	JobAdder maintains contact with relevant special interest groups and industry forums to stay informed of emerging threats and best practices.	GRC-08	Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.	Special Interest Groups	Governance, Risk and Compliance

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
HRS-01.1	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?	Yes	CSP-owned	Background checks are conducted in accordance with our documented Hiring & Change Policy, which is approved, communicated, and updated annually.		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually.		
HRS-01.2	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?	Yes	CSP-owned	JobAdder conducts employment history and criminal background checks, as permitted by applicable law, as part of pre-employment screening practices commensurate with the employee's position and level of access to JobAdder systems.				
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.	HRS-01		Background Screening Policy and Procedures	
HRS-02.1	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?	Yes	CSP-owned	Acceptable use of organisational assets is defined, communicated, and enforced through our Acceptable Use Policy and Information Security Policy.		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually.		
HRS-02.2	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?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.	HRS-02		Acceptable Use of Technology Policy and Procedures	
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Concealment of confidential data in unattended workspaces is required by our Acceptable Use Policy (Clean Desk).		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually.		
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.	HRS-03		Clean Desk Policy and Procedures	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
HRS-04.1	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	JobAdder is a remote-first organisation. Policies regarding remote work security (e.g., VPN use, screen locks) are established and enforced as part of our ISO 27001 ISMS.		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually.		
HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.	HRS-04		Remote and Home Working Policy and Procedures	
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	CSP-owned	Return procedures for organisational assets by terminated employees are established and documented in our Asset Management Procedure.	HRS-05	Establish and document procedures for the return of organization-owned assets by terminated employees.	Asset returns	
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Yes	CSP-owned	Procedures outlining roles and responsibilities concerning changes in employment are documented in our Hiring & Change Policy.	HRS-06	Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment.	Employment Termination	
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems,	Yes	CSP-owned	Employees are required to sign an employment agreement before being granted access to organisational systems, resources, and assets.	HRS-07	Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.	Employment Agreement Process	
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes	CSP-owned	Yes, adherence to established information governance and security policies is a stipulated clause in employment agreements.	HRS-08	The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.	Employment Agreement Content	
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Yes	CSP-owned	Employee roles and responsibilities regarding information security are documented in the Information Security Roles & Responsibilities procedure.	HRS-09	Document and communicate roles and responsibilities of employees, as they relate to information assets and security.	Personnel Roles and Responsibilities	
HRS-10.1	Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?	Yes	CSP-owned	Confidentiality agreement requirements are identified and reviewed by our General Counsel to reflect data protection needs.	HRS-10	Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details.	Non-Disclosure Agreements	
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Yes	CSP-owned	A security awareness training program is established and maintained as part of our ISO 27001 certified ISMS, delivered via our Learning Management System (LMS).		Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.		
HRS-11.2	Are regular security awareness training updates provided?	Yes	CSP-owned	Regular security awareness training updates are provided to all employees via our LMS, at least annually.	HRS-11		Security Awareness Training	
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	CSP-owned	All employees with access to sensitive data receive appropriate data privacy and security training.		Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.		

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
HRS-12.2	Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	Yes	CSP-owned	Yes, employees receive regular updates on procedures, processes, and policies relevant to their role.	HRS-12		Personal and Sensitive Data Awareness and Training	
HRS-13.1	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?	Yes	CSP-owned	Employees are made aware of their compliance responsibilities through onboarding, employment agreements, and ongoing training.	HRS-13	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.	Compliance User Responsibility	Human Resources
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	Identity and Access Management (IAM) policies are established and documented in our Access Control Policy as part of our ISO 27001 certified ISMS.	IAM-01	Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually.	Identity and Access Management Policy and Procedures	
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.				
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	Strong password policies including MFA are enforced through our Access Control Policy and Information Security Policy, managed centrally via Okta.	IAM-02	Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.	Strong Password Policy and Procedures	
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.				
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes	CSP-owned	We use enterprise IDAM (Okta) for user provisioning, role-based access, and identity lifecycle management.	IAM-03	Manage, store, and review the information of system identities, and level of access.	Identity Inventory	
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes	CSP-owned	Separation of duties is enforced when implementing information system access via our IDAM (Okta), as outlined in our Access Control Policy.	IAM-04	Employ the separation of duties principle when implementing information system access.	Separation of Duties	
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes	CSP-owned	We employ the principle of least privilege for all information system access, ensuring users only have access necessary for their role.	IAM-05	Employ the least privilege principle when implementing information system access.	Least Privilege	
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes	CSP-owned	A formal provisioning process is defined which authorises, records, and communicates access changes via our IDAM solution.	IAM-06	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	User Access Provisioning	
IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	Yes	CSP-owned	Our IDAM solution automates the de-provisioning of access when staff leave or change roles, ensuring timely revocation.	IAM-07	De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.	User Access Changes and Revocation	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IAM-08.1	Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?	Yes	CSP-owned	User access reviews are conducted quarterly to ensure least privilege and separation of duties are maintained.	IAM-08	Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.	User Access Review	
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	Yes	CSP-owned	Administrative access is segregated from standard user accounts, and privileged roles are strictly defined and monitored.	IAM-09	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated.	Segregation of Privileged Access Roles	
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Yes	CSP-owned	Privileged access is granted based on security approval via Okta with a set expiry date and is automatically revoked upon expiration.	IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.	Management of Privileged Access Roles	
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	Yes	CSP-owned	Procedures are in place to prevent the accumulation of segregated privileged access rights (creeping privileges).				
IAM-11.1	Are processes and procedures for 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?	Yes	CSP-owned	Customers are responsible for managing their own user access and roles within the JobAdder application.	IAM-11	Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.	CSCs Approval for Agreed Privileged Access Roles	
IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated?	Yes	CSP-owned	Audit logs are stored in a secure, read-only repository to prevent tampering by users with write access.	IAM-12	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.	Safeguard Logs Integrity	
IAM-12.2	Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?	Yes	CSP-owned	Disabling logging requires high-level privileges and is monitored/alerted to ensure segregation of duties.				
IAM-13.1	Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?	Yes	CSP-owned	All users are assigned unique IDs; shared accounts are prohibited for individual user access.	IAM-13	Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.	Uniquely Identifiable Users	
IAM-14.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?	Yes	CSP-owned	Multi-Factor Authentication (MFA) is enforced for all access to systems, applications, and sensitive data via Okta.		Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.		

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	No	CSP-owned	We use secure, cloud-native mechanisms (e.g., AWS IAM roles, API keys with rotation) for system identity and machine-to-machine authentication.	IAM-14		Strong Authentication	
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Yes	CSP-owned	Password management is enforced via Okta, requiring complex passwords and enabling of MFA.	IAM-15	Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.	Passwords Management	
IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Yes	CSP-owned	Access authorisation is verified by our IDAM solution before granting access to data or system functions.	IAM-16	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	Authorization Mechanisms	Identity & Access Management
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g.,APIs)?	Yes	CSP-owned	Policies for secure API communications are established and maintained. All API usage is governed by the JobAdder API Terms of Use and documented technical standards.		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually.		
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Yes	Shared CSP and CSC	Technical standards for interoperability (e.g., authentication, rate limiting, data schemas) are publicly documented in the JobAdder Developer Portal. Customers must adhere to the API Terms of Use when integrating.				
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	Yes	CSP-owned	Policies and procedures are in place to manage the portability of data entering and leaving our platform, ensuring security during import/export, in accordance with our Secure SDLC and Information Security Policies.				
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	Yes	CSP-owned	Policies regarding data persistence are defined in our Data Retention Policy. Data integrity is governed by our Backup Policy and SDLC procedures. Data exchange standards are documented in our API Terms of Use.				

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures, including API Terms and developer documentation, are reviewed, updated, and approved by JobAdder leadership at least annually.	IPY-01		Interoperability and Portability Policy and Procedures	
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes	Shared CSP and CSC	Customers can programmatically retrieve data via the JobAdder API. We provide comprehensive API documentation via our Developer Portal to support interoperability. Customers are responsible for securing their own integrations.	IPY-02	Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability.	Application Interface Availability	
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of	Yes	CSP-owned	We use TLS 1.3 for all data in transit, including data import/export and API communication, to ensure secure and standardised management of data.	IPY-03	Implement cryptographically secure and standardized network protocols for the management, import and export of data.	Secure Interoperability and Portability Management	
IPY-04.1	Do agreements include provisions specifying CSC 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 CSCs d. Data deletion policy	Yes	CSP-owned	Customer agreements and our Data Retention Policy specify that Customer account data is retained for 90 days from the date of account termination, after which it is deleted. Customers are able to request deletion of their data at any time by contacting support.	IPY-04	Agreements must include provisions specifying CSCs access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Data Portability Contractual Obligations	Interoperability & Portability
IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Infrastructure security is governed by our Secure Systems Development Policy, Configuration Management Policy, and Access Control Policy within our ISO 27001 ISMS.		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.		
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.	IVS-01		Infrastructure and Virtualization Security Policy and Procedures	
IVS-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?	Yes	CSP-owned	Resource availability and capacity are planned and monitored. Our AWS infrastructure leverages Auto Scaling Groups (ASG) to adjust capacity automatically based on demand.	IVS-02	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	Capacity and Resource Planning	
IVS-03.1	Are communications between environments monitored?	Yes	CSP-owned	Communications between environments are monitored for security and performance deviations using AWS CloudWatch and New Relic.		Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.		
IVS-03.2	Are communications between environments encrypted?	Yes	CSP-owned	Yes, internal and external communications are encrypted using TLS 1.3.				

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes	CSP-owned	Communications are restricted to authenticated and authorised connections in accordance with our Network Controls Policy and AWS Security Group configurations.				
IVS-03.4	Are network configurations reviewed at least annually?	Yes	CSP-owned	Network configurations are reviewed annually or upon significant change.				
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Yes	CSP-owned	Allowed services, protocols, and ports are documented and justified in accordance with our Network Controls Policy.	IVS-03		Network Security	
IVS-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	Yes	CSP-owned	All systems are hardened according to documented security baselines (aligned with CIS Benchmarks). Compliance is assessed and monitored using AWS Config.	IVS-04	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.	OS Hardening and Base Controls	
IVS-05.1	Are production and non-production environments separated?	Yes	CSP-owned	Production and non-production environments (e.g., UAT, QA, Dev) are strictly separated logically and physically, as required by our Secure Systems Development Policy.	IVS-05	Separate production and non-production environments.	Production and Non-Production Environments	
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and	Yes	CSP-owned	We utilise multi-tenancy controls and logical segmentation to ensure customer data is appropriately isolated.	IVS-06	Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants.	Segmentation and Segregation	
IVS-07.1	Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?	Yes	CSP-owned	Data migration is performed through encrypted tunnels (e.g., SFTP/SSH) using approved protocols (TLS 1.2+).	IVS-07	Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.	Migration to Cloud Environments	
IVS-08.1	Are high-risk environments identified and documented?	Yes	CSP-owned	High-risk environments are identified, documented, and subject to stricter controls as per our Risk Management Policy.	IVS-08	Identify and document high-risk environments.	Network Architecture Documentation	
IVS-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?	Yes	CSP-owned	Formal processes and procedures are in place for network security, utilising defense-in-depth techniques such as firewalls, network segmentation, and Endpoint Detection and Response (EDR). Security events from applications, endpoints, and cloud infrastructure are continuously monitored and correlated.	IVS-09	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.	Network Defense	Infrastructure & Virtualization Security

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Logging and monitoring policies are established and documented in our Logging & Monitoring Policy as part of our ISO 27001 certified ISMS.		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.		
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.	LOG-01		Logging and Monitoring Policy and Procedures	
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Yes	CSP-owned	Processes are in place to ensure audit logs are securely stored, protected from tampering, and retained in accordance with policy.	LOG-02	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.	Audit Logs Protection	
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes	CSP-owned	Security-related events are continuously identified and monitored across all layers, including applications, endpoints, and underlying infrastructure.		Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.		
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	Yes	CSP-owned	Automated alerts are generated for security events and sent to responsible stakeholders via internal communication channels (e.g., instant messaging, ticketing systems).	LOG-03		Security Monitoring and Alerting	
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes	CSP-owned	Access to audit logs is restricted to authorised engineering and security personnel on a least-privilege basis.	LOG-04	Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.	Audit Logs Access and Accountability	
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Yes	CSP-owned	Security audit logs are continuously monitored using automated systems to detect activity outside of typical or expected patterns.		Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.		
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes	CSP-owned	Detected anomalies are triaged and responded to in accordance with our Information Security Incident Management Plan.	LOG-05		Audit Logs Monitoring and Response	
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes	CSP-owned	We use Amazon Time Sync Service for AWS systems and NTP or platform time services for other environments and devices.	LOG-06	Use a reliable time source across all relevant information processing systems.	Clock Synchronization	
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Yes	CSP-owned	Logging requirements are established aligned with cloud security best practices and industry standards (e.g., CIS Benchmarks).		Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment.		

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	Yes	CSP-owned	The logging scope is reviewed, updated, and approved by JobAdder leadership at least annually or when changes in threat environment.	LOG-07		Logging Scope	
LOG-08.1	Are audit records generated, and do they contain relevant security information?	Yes	CSP-owned	Audit records containing relevant security information (e.g., timestamp, user ID, event type) are generated for all critical systems.	LOG-08	Generate audit records containing relevant security information.	Log Records	
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Yes	CSP-owned	Audit records are protected from unauthorised access, modification, and deletion through strict access controls.	LOG-09	The information system protects audit records from unauthorized access, modification, and deletion.	Log Protection	
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	Yes	CSP-owned	Cryptographic operations (e.g., key usage) are monitored and logged via cloud infrastructure logging services (e.g., AWS CloudTrail).	LOG-10	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.	Encryption Monitoring and Reporting	
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Yes	CSP-owned	Key lifecycle management events (generation, rotation, destruction) are logged to enable auditing of cryptographic key usage.	LOG-11	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.	Transaction/Activity Logging	
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	Yes	3rd-party outsourced	Physical access logging and monitoring is managed by AWS for data centre infrastructure, evidenced by their SOC 2 reports.	LOG-12	Monitor and log physical access using an auditable access control system.	Access Control Logs	
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Yes	CSP-owned	Processes are in place to detect and report failures in the monitoring system itself.		Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.		
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Yes	CSP-owned	Anomalies and failures trigger immediate alerts to 24x7 on-call engineering responders.	LOG-13		Failures and Anomalies Reporting	Logging and Monitoring
SEF-01.1	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied,	Yes	CSP-owned	Documented in our Information Security Incident Management Policy as part of our ISO 27001 certified ISMS.		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually.		
SEF-01.2	Are policies and procedures reviewed and updated annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.	SEF-01		Security Incident Management Policy and Procedures	
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Policies and procedures for the timely management of security incidents are established and maintained.		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually.		
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.	SEF-02		Service Management Policy and Procedures	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
SEF-03.1	Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Our ISO 27001 certified ISMS includes a formal Incident Response Plan (IRP) covering internal teams, customers, and critical business relationships.	SEF-03	'Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted.'	Incident Response Plans	
SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	Yes	CSP-owned	Our incident response plan is tested annually through phishing simulations and disaster recovery exercises, with updates made as needed for effectiveness.	SEF-04	Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.	Incident Response Testing	
SEF-05.1	Are information security incident metrics established and monitored?	Yes	CSP-owned	Incident metrics are established and monitored as part of our ISO 27001 ISMS.	SEF-05	Establish and monitor information security incident metrics.	Incident Response Metrics	
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Yes	CSP-owned	Processes for triaging security events are defined and implemented to ensure appropriate prioritisation and response.	SEF-06	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.	Event Triage Processes	
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes	CSP-owned	Processes are implemented as part of our ISO 27001 certified ISMS, in line with our Data Breach Response Procedure.	SEF-07	Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.	Security Breach Notification	
SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	Yes	CSP-owned	Security breaches are reported to affected parties in accordance with applicable laws, regulations, and Service Level Agreements (SLAs).				
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Yes	CSP-owned	We maintain points of contact for relevant regulatory authorities and law enforcement agencies within our Incident Response Plan.	SEF-08	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.	Points of Contact Maintenance	Security Incident Management, E-Discovery, & Cloud Forensics
STA-01.1	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Documented in our Information Security Policy and Third Party Systems Policy for vendor and supplier risk management.	STA-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually.	SSRM Policy and Procedures	
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.				

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes	CSP-owned	The Shared Security Responsibility Model (SSRM) is applied, documented, and managed throughout our supply chain for the cloud service offering.	STA-02	Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.	SSRM Supply Chain	
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	Yes	CSP-owned	We provide SSRM guidance to Customers via our Trust Centre and standard compliance documentation.	STA-03	Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.	SSRM Guidance	
STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	Yes	CSP-owned	Shared ownership and applicability of controls are delineated in our CAIQ and compliance documentation based on the SSRM.	STA-04	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.	SSRM Control Ownership	
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Yes	CSP-owned	SSRM documentation for all cloud services the organisation uses is reviewed and validated as part of our vendor risk assessment process.	STA-05	Review and validate SSRM documentation for all cloud services offerings the organization uses.	SSRM Documentation Review	
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes	CSP-owned	We implement, operate, and assess all controls for which we are responsible under the SSRM.	STA-06	Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.	SSRM Control Implementation	
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	Yes	CSP-owned	An Application/Asset register is maintained as an inventory of all third-party, vendor, and supply chain relationships, populated via a formal Third Party Systems Request (TPSR) process.	STA-07	Develop and maintain an inventory of all supply chain relationships.	Supply Chain Inventory	
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Yes	CSP-owned	Supply chain risks are reviewed annually or upon contract renewal as part of our ISO 27001 certified ISMS.	STA-08	CSPs periodically review risk factors associated with all organizations within their supply chain.	Supply Chain Risk Management	
STA-09.1	Do service agreements between CSPs and CSCs (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	Yes	CSP-owned	JobAdder's standard Customer Agreement and Data Processing Agreement (DPA) incorporate security requirements, incident management, and data privacy provisions.	STA-09	Service agreements between CSPs and CSCs (tenants) must 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 and portability requirements • Data privacy	Primary Service and Contractual Agreement	
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	Yes	CSP-owned	Supply chain agreements are reviewed at least annually or upon renewal to ensure compliance with security and business requirements.	STA-10	Review supply chain agreements between CSPs and CSCs at least annually.	Supply Chain Agreement Review	
STA-11.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	Yes	CSP-owned	JobAdder conducts assessments of third-party suppliers and vendors to evaluate the effectiveness of their security, governance procedures, and SLAs.	STA-11	Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually.	Internal Compliance Testing	
STA-12.1	Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Yes	CSP-owned	We require supply chain partners to comply with relevant information security, confidentiality, and privacy requirements.	STA-12	Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards.	Supply Chain Service Agreement Compliance	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	Yes	CSP-owned	Partner governance policies are reviewed periodically as part of our ongoing vendor risk management program.	STA-13	Periodically review the organization's supply chain partners' IT governance policies and procedures.	Supply Chain Governance Review	Supply Chain Management, Transparency, and Accountability
STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	Yes	CSP-owned	We conduct periodic security assessments of supply chain organisations based on risk and criticality to the business.	STA-14	Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.	Supply Chain Data Security Assessment	
TVM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against	Yes	CSP-owned	A Vulnerability Management plan is established, documented, and maintained as part of our ISO 27001 certified ISMS.	TVM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually.	Threat and Vulnerability Management Policy and Procedures	
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.				
TVM-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Policies to protect against malware are established. All endpoints are protected with an enterprise Endpoint Detection and Response (EDR) solution.	TVM-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually.	Malware Protection Policy and Procedures	
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.				
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk)?	Yes	CSP-owned	Processes are in place for both scheduled and emergency vulnerability remediation based on risk and criticality.	TVM-03	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.	Vulnerability Remediation Schedule	
TVM-04.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	Yes	CSP-owned	Detection tools are updated continuously. Threat signatures and indicators of compromise are managed automatically by the vendor.	TVM-04	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.	Detection Updates	
TVM-05.1	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	Yes	CSP-owned	We utilise Software Composition Analysis (SCA) tools within our CI/CD pipeline to identify and remediate vulnerabilities in third-party libraries.	TVM-05	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.	External Library Vulnerabilities	
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Yes	CSP-owned	JobAdder engages CREST-certified independent testers for annual penetration tests (most recently retested in September 2025).	TVM-06	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.	Penetration Testing	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Yes	CSP-owned	Vulnerability scanning is performed continuously via automated tools and is event-driven based on code changes.	TVM-07	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.	Vulnerability Identification	
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	Yes	CSP-owned	Remediation is prioritised using a risk-based model and business context to ensure critical issues are addressed first.	TVM-08	Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.	Vulnerability Prioritization	
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes	CSP-owned	Vulnerability remediation activities are tracked and reported to stakeholders via our central ticketing system (Jira).	TVM-09	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.	Vulnerability Management Reporting	
TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Yes	CSP-owned	Vulnerability metrics (e.g., time to remediate) are established, monitored, and reported at defined intervals.	TVM-10	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.	Vulnerability Management Metrics	Threat & Vulnerability Management
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes	CSP-owned	Endpoint policies are established and enforced via our Enterprise Mobile Device Management (MDM) and EDR solutions, as part of our ISO 27001 ISMS.		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually.		
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed, updated, and approved by JobAdder leadership at least annually.	UEM-01		Endpoint Devices Policy and Procedures	
UEM-02.1	Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?	Yes	CSP-owned	A list of approved applications is maintained. Unapproved applications are restricted via MDM policies.	UEM-02	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.	Application and Service Approval	
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	Yes	CSP-owned	We use MDM platforms to monitor compliance with operating system versions and patch levels to ensure compatibility and security.	UEM-03	Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.	Compatibility	
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Yes	CSP-owned	An inventory of all endpoints is automatically maintained and tracked via our MDM and EDR solutions.	UEM-04	Maintain an inventory of all endpoints used to store and access company data.	Endpoint Inventory	
UEM-05.1	Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?	Yes	CSP-owned	Processes are defined and implemented to enforce security policies (e.g., encryption, password requirements) on all endpoints accessing organisational data.	UEM-05	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.	Endpoint Management	
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes	CSP-owned	Endpoint laptops are configured with a 10-minute inactivity timeout for automatic screen lock.	UEM-06	Configure all relevant interactive-use endpoints to require an automatic lock screen.	Automatic Lock Screen	

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.3

Question ID	Question	CSP CAIQ Answ	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	Yes	CSP-owned	Significant changes to endpoint configurations (e.g., OS upgrades, policy changes) are managed through our Change Management process.	UEM-07	Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.	Operating Systems	
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	Yes	CSP-owned	All managed endpoints are protected with full disk encryption to prevent unauthorised data access.	UEM-08	Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.	Storage Encryption	
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Yes	CSP-owned	All endpoints are protected by an enterprise Endpoint Detection and Response (EDR) solution.	UEM-09	Configure managed endpoints with anti-malware detection and prevention technology and services.	Anti-Malware Detection and Prevention	
UEM-10.1	Are software firewalls configured on managed endpoints?	Yes	CSP-owned	Host-based firewalls are enabled and managed centrally through MDM policies.	UEM-10	Configure managed endpoints with properly configured software firewalls.	Software Firewall	
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	Yes	CSP-owned	Endpoints are configured with Netskope DLP agents based on risk assessment to prevent unauthorised data exfiltration.	UEM-11	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.	Data Loss Prevention	
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	Yes	CSP-owned	Remote geolocation is enabled for managed mobile endpoints to assist with recovery or wiping of lost devices.	UEM-12	Enable remote geo-location capabilities for all managed mobile endpoints.	Remote Locate	
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	Yes	CSP-owned	All managed devices support remote wipe capabilities via MDM to ensure data deletion in case of loss or theft.	UEM-13	Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.	Remote Wipe	
UEM-14.1	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?	Yes	CSP-owned	Third-party access is restricted and managed; we do not permit direct access to internal assets from unmanaged third-party endpoints.	UEM-14	Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets.	Third-Party Endpoint Security Posture	Universal Endpoint Management

End of Standard