AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Boomi has an internal audit team and an audit charter pending board approval. Boomi is externally audited several times annually, including SOC, HIPAA, PCI, ISO and for FedRAMP moderate authorization. Audit findings are documented in a risk registry and shared with the appropriate stakeholders. Boomi creates risk-based remediation plans to address audit findings.
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Yes	
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes	
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes	
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Yes	
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	
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	Yes	
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 capabilities?	Yes	Boomi has approved and adopted a suitable software development lifecycle (SDLC) policy. Boomi performs automated code quality and security scans with metrics to monitor changes and improvements. Code deployment is automated. Application vulnerabilities are remediated using a defined process. Major application changes are subject to a security impact assessment by Boomi's Dev/Sec/Ops security council.
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Yes	
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes	
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes	
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	
AIS-05.2	Is testing automated when applicable and possible?	Yes	
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes	
AIS-06.2	Is the deployment and integration of application code automated where possible?	Yes	
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes	
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	No	
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Boomi has approved and adopted a suitable business continuity (BC) policy and business functions have plans for corporate applications. All corporate policies are reviewed annually. BC plans are also tested annually. Cloud data is backed up in near real-time to support Boomi's service level commitments. Boomi Engineering has documented disaster recovery plans that are tested annually. Boomi's cloud infrastructure is highly redundant within AWS regions. Boomi's incident response plan does include contact information for local authorities. More information can be found in Boomi's Business Continuity Summary on our compliance page. Boomi Compliance https://boomi.com/compliance/
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes	
BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	Yes	
BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	Yes	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	Yes	
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes	
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Yes	
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	Yes	
BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	Yes	
BCR-08.1	Is cloud data periodically backed up?	Yes	
BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	Yes	
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	
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	
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes	
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes	
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	Yes	
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	
CCC-01.1	Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established,	Yes	Boomi has approved and adopted a suitable change management policy and business functions have change management plans. All corporate policies are reviewed annually. Boomi has a quality engineering (QE) team that tests all new features before being

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
	documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)?		promoted to production. Changes to baseline requirements follow change procedures. Boomi cloud nodes are scanned monthly to ensure continued compliance with security hardening standards. Monthly release schedules are posted to Boomi's Status page. Boomi encourages customers to register for notifications. Emergency changes that may impact customers will be posted to the status page. In the event a release causes a performance issue, Boomi has a defined rollback process. Boomi Status https://status.boomi.com/
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Yes	
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	
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes	
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	
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes	
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Yes	
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes	
CCC-08.2	Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?'	Yes	
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	
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Boomi has approved and adopted a suitable cryptographic standard. All corporate policies are reviewed annually. Boomi Operations configures key management roles inside AWS. Boomi considers all customer data highly sensitive and uses industry

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Yes	standard encryption to ensure data confidentiality and integrity. Boomi encrypts data in transit using TLS 1.2 and all data at rest using AES 256. Changes to encryption algorithms follow change management procedures. Changes to an encryption algorithm are fully tested for backward compatibility before implementation and requires a security impact assessment (SIA). Data encryption at rest keys are stored in an AWS managed KMS. Keys are rotated annually. BYOK are on Boomi's Product roadmap for implementation in 2023.
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes	
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes	
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Yes	
CEK-05.1	Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	Yes	
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	
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	
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	No	
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	
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Yes	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Yes	
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes	
CEK-12.1	Are cryptographic keys rotated based on a crypto period calculated while considering information disclosure risks and legal and regulatory requirements?	Yes	
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?	Yes	
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 legal and regulatory requirement provisions?	Yes	
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	
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	
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	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
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 regulatory requirement provisions?	Yes	
CEK-19.1	Are processes, procedures, and technical measures to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	
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	
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	
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	AtomSphere is hosted in AWS. AWS inherits the physical and environmental security of the data center. AtomSphere is a fully virtualized cloud infrastructure. There is no physical hardware managed by Boomi. Customers determine the processing and storage location of scoped data. Boomi will never relocate customer data without prior notice and consent. AWS destroys the physical media at the end of its useful life compliant with NIST 800-88. Boomi has a Secure Workplace standard. All corporate policies are reviewed annually. Boomi maintains a cloud asset inventory that is updated daily. Additional information about AWS physical and environmental controls can be found on the AWS data center page. AWS Data Center Controls https://aws.amazon.com/compliance/data-center/controls/
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Yes	
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	
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?	NA	
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	NA	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
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?	NA	
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	
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Yes	
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	NA	
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	NA	
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Yes	
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Yes	
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	Yes	
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	Yes	
DCS-08.1	Is equipment identification used as a method for connection authentication?	NA	
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	
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Yes	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Yes	
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	Yes	
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	
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 and maintained?	Yes	
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	Yes	
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	Yes	
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	Boomi provides customers with the AtomSphere application to integrate, process and temporarily store processed data. Boomi does not have visibility into the data our customers choose to process through our services. As a result, Boomi does not categorize customer data, instead, treating all data as highly sensitive. AtomSphere is designed to ensure compliance with security and privacy industry best practices, and has achieved ISO Certification (27001, 27701) and FedRAMP authorization. In providing its services, Boomi agrees to abide by all applicable laws and regulations. Boomi's privacy compliance program aligns to GDPR. The nature of the Boomi services means that (i) the data subject is generally not aware of the sub-processing of their data by Boomi and (ii) Boomi generally does not store the underlying processed data which the customer processes using our Services. Sub-processor contracts contain data protection obligations materially similar to those in our Customer agreements.
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes	
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	
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	NA	
DSP-04.1	Is data classified according to type and sensitivity levels?	Yes	
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Yes	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Yes	Unless required by law, Boomi will notify customers of a Law Enforcement Authority's request for personal data. Boomi's releases an annual Transparency Report to disclose any such requests. Annual Transparency Report https://boomi.com/wp-content/uploads/Transparency-Report.pdf Data Transfers https://boomi.com/wp-content/uploads/White-Paper_-Data-Transfers.pdf AtomSphere Atom/MDH Cloud Locations https://help.boomi.com/bundle/atomsphere_platform/page/atm-Connecting_to_the_boomi_atom_clouds_and_hub_clouds.html Flow Cloud Locations https://help.boomi.com/bundle/flow/page/c-flo-Techref_Architecture.html Boomi's DPA https://boomi.com/DPA Boomi Sub-processors https://boomi.com/legal/sub-processors/
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	NA	
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	NA	
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Yes	
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Yes	
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	Yes	
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	
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	
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	
DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?	Yes	
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	Yes	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
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?	NA	
DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	NA	
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes	
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Yes	
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	
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	
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	
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Boomi has an internal audit charter, approved information governance standard and technical compliance program. All corporate policies are reviewed annually. Boomi's corporate risk management program is led by Boomi's head of internal audit. Boomi's audit team maintains a risk management process to frame, assess, respond to, and monitor risk, consistent with applicable contractual and legal obligations. Boomi performs periodic risk assessments of its environment and systems. Identified risks are documented in a risk registry. Appropriate controls are applied to manage and mitigate risks.
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	
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?	No	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Yes	
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	
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Yes	
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes	
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Yes	
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	No	
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	Boomi Human Resources (HR) has approved and adopted suitable HR policies and procedures that include background checks. Boomi has an approved Acceptable Use policy. All corporate policies are reviewed annually. Boomi performs background checks for all employees. Employees sign a code of conduct within 30 days of employment. Boomi has a secure workspace standard that includes security guidance for unattended workspaces. Boomi has an information governance standard with security requirements for the protection of information accessed, processed, or stored at remote sites. Boomi has a termination checklist that includes the return of all corporate owned devices. Boomi conducts annual security awareness training (SAT) for all employees and contractors. Training material is updated 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	
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes	
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	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
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	
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes	
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	
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	
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Yes	
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Yes	
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes	
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Yes	
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	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Yes	
HRS-11.2	Are regular security awareness training updates provided?	Yes	
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	
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	
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	
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	Boomi has approved and adopted a suitable identity and access management policy and an approved corporate password policy that enforces strong passwords through Boomi's corporate IAM tool. All corporate policies are reviewed annually. Access to Boomi's cloud infrastructure follows the separation of duties and principle of least privilege. Only employees that require access to the backend infrastructure are granted access by role. Access to the cloud infrastructure requires credentials, keys and MFA from a corporate managed device. Administrator access is reviewed quarterly. Administrator access is modified within 24 hours of a role change or employee separation. Employees have unique user IDs. Cloud administrators have a regular user ID for common business tasks and a privilege ID that is only used for privileged commands. Shared accounts are not used. Passwords are hashed and encrypted. Passwords must not be shared. Infrastructure security logs are stored in an immutable infrastructure and are saved for one year.
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Yes	
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Yes	
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes	
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes	
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes	
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	
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	
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	
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	No	
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	Yes	
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	
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	
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	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
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	
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	
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Yes	
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Yes	
IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Yes	
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	Yes	As a cloud native iPaaS, Boomi has hundreds of connectors to help ensure information processing interoperability. Customers can also develop custom connectors. Boomi AtomSphere and Flow APIs are well documented on Boomi's help pages. Boomi encrypts all data in transit using TLS 1.2 and all data at rest using AES 256. Data deletion times are dependent on the product and the customer configuration. All processed data will be deleted shortly after contract termination. AtomSphere Platform configuration data specifically is deleted upon request only. The customer is the data owner. Boomi acts as the data processor. Therefore, the Boomi services are not portable after contract termination. All data exists at the customer's application endpoint. AtomSphere API https://help.boomi.com/bundle/developer_apis/page/r-atm-AtomSphere_API.html Flow API https://manywho.github.io/docs-api/
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Yes	
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	NA	
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	
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	NA	
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	NA	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	Yes	
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	NA	
IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Boomi has approved and adopted a suitable information security policy and subsequent security procedures. All corporate policies are reviewed annually. Boomi monitors the health and capacity of the cloud infrastructure continuously. Boomi encourages customers to register for health notifications on Boomi's Status page. Boomi uses firewalls to ensure communications between environments are restricted to only authenticated and authorized connections. Firewalls are deployed as Infrastructure as Code (IaC) and rulesets are regularly reviewed. Cloud nodes are configured with a hardened security baseline based on CIS standards. Boomi has separate development, testing and production environments. Boomi's multi-tenant environment is properly segmented to ensure customer data cannot be accessed by an unauthorized resource. Clear-text protocols are not permitted. Boomi has deployed a defense-in-depth security architecture with protection and detection tools to repel network-based attacks. Boomi Status https://status.boomi.com/
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Yes	
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	
IVS-03.1	Are communications between environments monitored?	Yes	
IVS-03.2	Are communications between environments encrypted?	No	
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes	
IVS-03.4	Are network configurations reviewed at least annually?	Yes	
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Yes	
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	
IVS-05.1	Are production and non-production environments separated?	Yes	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
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 restricted from other tenants?	Yes	
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	
IVS-08.1	Are high-risk environments identified and documented?	Yes	
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	
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Boomi has approved and adopted a suitable logging and monitoring standard. All corporate policies are reviewed annually. Network, application and host security logs are forwarded to a 24x7x365 managed SIEM service and logs are retained for one (1) year. Boomi's cloud infrastructure and SIEM are only accessible to authorized administrators. SIEM rules generate alerts on anomalous activity and are triaged by Boomi. Logs are synched to a central time server. Customers have access to their own audit logs for review and ingestion into their log management solution. AWS logs and reports on cryptographic operations, encryption, and key management policies. Physical access logs are maintained by AWS. AWS notifies Boomi of any logging failures.
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes	
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Yes	
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes	
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	Yes	
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes	
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Yes	
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes	
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Yes	
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	Yes	
LOG-08.1	Are audit records generated, and do they contain relevant security information?	Yes	
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Yes	
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	
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Yes	
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	Yes	
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Yes	
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Yes	
SEF-01.1	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Boomi has approved and adopted a suitable cybersecurity incident response (IR) standard. All corporate policies are reviewed annually. Boomi's IR plan is designed to ensure all cybersecurity incidents are promptly detected, investigated, documented, and resolved in a timely manner while maintaining necessary evidence for any further disciplinary, legal or law enforcement actions. The IR plan applies a risk-based approach and follows the NIST 800-61 IR lifecycle. The IR plan includes points of contact for applicable local law enforcement. Boomi conducts IR tabletop exercises and updates the plan accordingly. Boomi will notify the Customer without undue delay
SEF-01.2	Are policies and procedures reviewed and updated annually?	Yes	
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Yes	after becoming aware of any disclosure of or access to the Personal Data by a third party in breach of this section and will reasonably cooperate with Customer to remediate the effect of such disclosure or access.
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	
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	
SEF-05.1	Are information security incident metrics established and monitored?	Yes	
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Yes	
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes	
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	
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Yes	
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	Boomi has a documented shared security responsibility matrix (SSRM) that describes the security functions Boomi (CSP) is responsible for and the security settings our customers (CSC) may choose to configure. The SSRM is reviewed annually. Ownership and applicability of security settings is delineated within the SSRM. Boomi's Master Services Agreement (MSA) and Security Schedule include Boomi's security provisions. Boomi maintains an inventory of our sub-processors and provides a mechanism for customer to register for updates (as per the GDPR / SCC "General Authorisation" model). All Boomi vendors must provide audit materials, penetration tests and respond to a security questionnaire as appropriate. All Boomi
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Yes	
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes	
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	Yes	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
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	third parties must adhere to Boomi's Supplier Principles (or have their own code which is materially similar) which requires the implementation of appropriate safeguards to ensure the protection, integrity, security and availability of customer information in accordance with applicable data privacy laws. Critical hosting sub-processors are reviewed annually. Boomi Sub-processors https://boomi.com/legal/sub-processors/ Boomi Master Services Agreement https://boomi.com/msa/ Boomi Security Schedule https://boomi.com/secschedule/
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Yes	
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes	
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	Yes	
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Yes	
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 • Interoperability and portability requirements • Data privacy	Yes	
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	NA	
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	
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	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	No	
STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	No	
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 vulnerability exploitation?	Yes	Boomi has approved and adopted suitable threat and vulnerability management, and security patching policies. All corporate policies are reviewed annually. All Boomi cloud nodes contain managed EDR software which includes anti-malware. Security patches are deployed at least monthly and can be deployed following an emergency process if required. Malware signatures are updated continuously. Boomi runs software composition analysis (SCA) software against code to identify weaknesses in 3rd party libraries. Boomi conducts internal, authenticated vulnerability scans weekly, and external scans quarterly in compliance with PCI. Boomi engages an independent external consultant to perform web application penetration testing annually. Identified risks are addressed based on risk using the industry accepted CVSS scoring. Vulnerability metrics are reported to Boomi leadership monthly.
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Yes	
TVM-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Yes	
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	
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	
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 vulnerability management policy)?	Yes	
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Yes	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Yes	
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	Yes	
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes	
TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Yes	
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes	Boomi cloud node endpoints are hardened to CIS standards. Boomi performs monthly configuration scans to ensure cloud node configuration has not changed. Cloud nodes have managed EDR software that includes anti-malware. Boomi manages a cloud asset inventory that is updated daily. Changes to cloud node endpoints follow Boomi's change management policy. Cloud nodes do not have host or network DLP because Boomi does not inspect customer integrations and therefore cannot classify data.
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Yes	
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	
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	Yes	
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Yes	
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	
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes	
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	Yes	

AtomSphere CAIQ v4.0.2

Question	Question Text	CSP	Detailed Response
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	Yes	
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Yes	
UEM-10.1	Are software firewalls configured on managed endpoints?	Yes	
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	NA	
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	NA	
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	NA	
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	