

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/ Recommended)
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Atrixware maintains documented audit and assurance practices as part of its information security and governance program. These practices support review of security policies, procedures, controls, and compliance requirements.
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews and maintains its audit and assurance practices periodically and when significant changes occur.
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	No	CSP-owned	Atrixware does not currently conduct independent audit and assurance assessments according to relevant standards at least annually. Atrixware maintains documented security policies, procedures, and internal security assessment practices.
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies, and in response to significant changes or emerging risks?	No	CSP-owned	Atrixware does not currently conduct independent audit and assurance assessments according to risk-based plans or in response to significant changes or emerging risks. Atrixware evaluates security and operational risks through its established security and business continuity practices.
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Yes	CSP-owned	Atrixware identifies and evaluates applicable legal, regulatory, contractual, privacy, and security requirements as part of its security and compliance practices.
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 and aligned with relevant auditing standards?	Yes	CSP-owned	Atrixware maintains processes for security control review, risk analysis, remediation tracking, and review of supporting security documentation and evidence.
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	Atrixware maintains corrective action practices for identified security and audit findings. Remediation activities are prioritized based on the nature, severity, and potential impact of the finding.
A&A-06.2	Is the remediation status of audit findings regularly reviewed and reported to relevant stakeholders?	Yes	CSP-owned	Atrixware reviews the status of identified security and audit findings and tracks remediation activities through its security and operational practices.
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Atrixware maintains documented application security policies and procedures covering secure application development, access management, data protection, testing, vulnerability management, and deployment.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually, or upon any significant changes?	Yes	CSP-owned	Atrixware reviews and maintains its application security policies and procedures periodically and when significant changes occur.
AIS-02.1	Are baseline requirements to secure applications established, documented, and maintained?	Yes	CSP-owned	Atrixware maintains documented application security requirements within its security and software development procedures. These requirements include input validation, data sanitization, output encoding, error handling, static analysis, internal quality assurance testing, isolated development environments, and sandbox testing prior to production deployment.
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes	CSP-owned	Atrixware monitors application security and operational information as part of its ongoing software development, maintenance, and support processes. Security issues, vulnerabilities, bugs, and remediation activities are tracked and evaluated according to their nature and severity. Security-related issues may be addressed and patched on an expedited basis when appropriate.
AIS-04.1	Is a secure SDLC process defined and implemented for application requirements analysis, planning, design, development, testing, deployment, and operation per organizationally designed security requirements?	Yes	CSP-owned	Atrixware maintains a secure software development lifecycle incorporating security requirements, isolated development environments, static analysis, internal quality assurance, controlled testing, and sandbox testing prior to production deployment.
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 meeting organizational delivery goals?	Yes	CSP-owned	Atrixware's testing process establishes criteria for evaluating application updates, features, and revisions before production deployment. Changes undergo security analysis and internal quality assurance testing, followed by testing in the sandbox/semi-production environment.
AIS-05.2	Is testing automated when applicable and possible?	Yes	CSP-owned	Atrixware uses automated testing and analysis where applicable and supplements automated processes with manual testing and quality assurance. Application changes undergo static analysis and internal quality assurance testing before deployment.
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes	CSP-owned	Atrixware maintains controlled application deployment practices. Changes are developed and tested in controlled environments, undergo security analysis and quality assurance, and are deployed through the sandbox/semi-production environment before production implementation.
AIS-06.2	Is the deployment and integration of application code automated where possible?	Yes	CSP-owned	Atrixware utilizes a partially automated application deployment process. Automated tools and procedures are used where applicable, with appropriate personnel involvement for deployment activities and production changes. Application changes are first developed and tested in controlled environments before being deployed to production.
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes	CSP-owned	Atrixware maintains defined processes for identifying, evaluating, prioritizing, and remediating application security vulnerabilities. Security issues are addressed according to their severity and potential impact, with critical issues capable of being corrected and patched on an expedited basis.
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	Yes	CSP-owned	Atrixware utilizes both automated and manual processes for remediation of application security vulnerabilities, as appropriate to the nature of the vulnerability and available remediation methods. Vulnerabilities and security issues are evaluated and addressed based on their severity and potential impact, with critical security issues capable of being corrected and patched on an expedited basis.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
AIS-08.1	Are processes, procedures, and technical measures defined and implemented to secure APIs?	Yes	CSP-owned	Atrixware implements security controls for Axis LMS APIs, including authentication, authorization, TLS/HTTPS encryption, input validation, logging, and rate limiting/throttling. API access is subject to appropriate access controls and security monitoring to help protect the confidentiality, integrity, and availability of API-accessible information and functionality.
AIS-08.2	Are reviews and updates for any improvements conducted at least annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews API security as part of its ongoing application security practices. API security is reviewed periodically and when significant changes are made to API functionality or the supporting application. Security controls are evaluated and updated as appropriate based on changes to the application, technology, or security requirements.
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Atrixware maintains a documented Business Continuity and Disaster Recovery plan and associated procedures for supporting the continued operation and recovery of Axis LMS services.
BCR-01.2	Are the policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews and updates its Business Continuity and Disaster Recovery plan at least annually and when significant changes occur.
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	Atrixware assesses business impact as part of its Business Continuity and Disaster Recovery planning. Critical business functions, systems, and dependencies are considered in planning for potential service disruptions and recovery.
BCR-02.2	Are the risk assessment and impact analysis reviewed and updated at least annually or upon significant changes?	Yes	CSP-owned	Atrixware identifies key dependencies and resources as part of its Business Continuity and Disaster Recovery planning. These considerations are incorporated into planning for maintaining and recovering critical business functions during a disruption.
BCR-03.1	Are strategies being established to reduce the impact of business disruptions, and are resiliency and recovery from business disruptions being improved?	Yes	CSP-owned	Atrixware establishes recovery objectives and targets as part of its Business Continuity and Disaster Recovery planning. Recovery expectations are considered in planning and response activities, although they are not formally documented as specific RTO and RPO values.
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	CSP-owned	Atrixware maintains a documented Business Continuity and Disaster Recovery plan that incorporates operational resilience strategies and recovery capabilities. The plan is maintained and used to support continuity and recovery of critical business operations and Axis LMS services.
BCR-05.1	Is relevant documentation developed, identified, and acquired both internally and from external parties, to support business continuity and operational resilience plans?	Yes	CSP-owned	Atrixware maintains and utilizes relevant internal documentation to support its Business Continuity and Disaster Recovery planning. External documentation and information from service providers, including the data center provider, are also considered where applicable to support operational resilience and recovery planning.
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes	CSP-owned	Atrixware makes relevant Business Continuity and Disaster Recovery documentation available to authorized personnel and stakeholders who require access to support business continuity and operational resilience activities.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
BCR-05.3	Is business continuity and operational resilience documentation reviewed at least annually or upon significant changes?	Yes	CSP-owned	Atrixware reviews its Business Continuity and Disaster Recovery documentation at least annually and when significant changes occur. Updates are made as appropriate to reflect changes to business operations, systems, or recovery requirements.
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	Atrixware performs recovery exercises and testing as part of its Business Continuity and Disaster Recovery planning and operational practices. Testing is performed periodically and when significant changes occur to help evaluate recovery procedures and identify areas for improvement.
BCR-07.1	Are communication channels with all relevant stakeholders established and maintained during business continuity and resilience procedures?	Yes	CSP-owned	Atrixware maintains communication methods for operational and support activities
BCR-08.1	Are backups performed periodically?	Yes	3rd-party outsourced	Atrixware's hosting provider performs full server backups nightly. Backup data is transferred via a secure private network and retained for up to 30 days. Additional off-site backup storage and retention options are available depending on the hosting package.
BCR-08.2	Is the confidentiality, integrity, and availability of the backup ensured?	Yes	3rd-party outsourced	Atrixware's hosting provider protects backup data through secure transfer to backup storage and maintains retained backup copies to support availability and recovery. Backup data is transferred from the hosting server to backup storage over a secure private network, with additional off-site storage and retention options available depending on the hosting package.
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	3rd-party outsourced	Atrixware's hosting provider maintains full server backups to support restoration and recovery in the event of a service disruption. Backups are performed nightly and retained for up to 30 days, supporting recovery and operational resiliency.
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	Atrixware maintains a documented Business Continuity and Disaster Recovery plan and associated procedures to support response to and recovery from natural and man-made disasters. The plan is applied and evaluated as part of Atrixware's business continuity and recovery practices.
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes	CSP-owned	Atrixware reviews and updates its Business Continuity and Disaster Recovery documentation at least annually and when significant changes occur. Updates are made as appropriate to reflect changes to business operations, systems, or recovery requirements.
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes	CSP-owned	Atrixware exercises its disaster response and recovery procedures periodically and when significant changes occur. These exercises are used to evaluate recovery procedures and identify areas for improvement.
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	Yes	3rd-party outsourced	The Axis LMS hosting environment is supported by the third-party data center provider, which incorporates applicable emergency response and business continuity considerations into its exercise and preparedness activities, including coordination with relevant local emergency authorities where appropriate and feasible.
BCR-11.1	Are business-critical equipment supplemented with both locally redundant and geographically dispersed equipment located at a reasonable minimum distance, in accordance with applicable industry standards?	Yes	3rd-party outsourced	Atrixware's hosting provider maintains redundant infrastructure within its data center environment to support service resiliency. Additional off-site backup storage is available depending on the hosting package. Atrixware's documented policies do not establish that business-critical equipment is geographically dispersed at a specified minimum distance in accordance with applicable industry standards.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
CCC-01.1	Are policies and procedures for managing the risks associated with applying changes to assets owned, controlled, or used by the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Atrixware maintains documented policies and procedures for managing changes to its applications and supporting systems. Application updates, features, and revisions undergo static analysis and internal quality assurance testing in controlled development environments before being deployed to a sandbox/semi-production environment and subsequently to production. Security and operational risks associated with changes are evaluated as part of the development and deployment process.
CCC-01.2	Are the policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews its security and operational policies and procedures periodically and updates them as appropriate, including when significant changes occur.
CCC-02.1	Is a defined quality change control, approval and testing process, incorporating baselines, testing, and release standards, established, maintained and implemented?	Yes	CSP-owned	Atrixware maintains a defined software change and quality process. Development occurs in an isolated environment, and each update, feature, or revision undergoes static analysis and internal quality assurance testing before being deployed to a sandbox/semi-production environment for additional testing prior to production release.
CCC-03.1	Is a change management procedure implemented to manage the risks associated with applying changes to assets, owned, controlled or used by the organization?	Yes	CSP-owned	Atrixware implements change management practices for application and system changes. Changes are developed and tested in controlled environments, undergo static analysis and internal quality assurance testing, and are deployed to a sandbox/semi-production environment for testing before production deployment. These practices help manage security and operational risks associated with changes.
CCC-04.1	Is a procedure to authorize the addition, removal, update, and management of assets owned, controlled, or used by the organization, implemented and enforced?	Yes	CSP-owned	Atrixware maintains procedures for managing changes to its application and supporting systems. Changes are developed and tested in controlled environments, undergo quality assurance and security testing, and are progressed through controlled deployment environments before production implementation.
CCC-05.1	Are provisions to limit changes directly impacting service customer-owned environments (tenants) to explicitly authorized requests included within service level agreements?	Yes	CSP-owned	Atrixware's service agreement defines provisions governing changes to customer Axis LMS environments. Urgent security patches and changes expected to cause no more than three minutes of downtime may be automatically applied. Changes expected to cause more than three minutes of downtime are scheduled through an agreed-upon window with the client. Clients may also elect not to accept an upgrade or update, subject to the support and other terms specified in the service agreement.
CCC-06.1	Are change management and configuration baselines established, documented and implemented for all relevant authorized changes on organizational assets?	Yes	CSP-owned	Atrixware maintains documented change management and controlled deployment practices for relevant changes to its applications and supporting systems. Changes are developed and tested in controlled environments, undergo static analysis and internal quality assurance testing, and are deployed through a sandbox/semi-production environment before production implementation.
CCC-06.2	Are the baselines reviewed and updated at least annually or upon significant changes?	Yes	CSP-owned	Atrixware reviews its change management practices and configuration baselines periodically and upon significant changes to help ensure they remain appropriate for the organization's applications and supporting systems.
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Yes	CSP-owned	Atrixware manually reviews changes against established configuration baselines. Deviations from established baselines are identified through the review process and addressed as appropriate, with relevant personnel notified when corrective action is required.
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes	CSP-owned	Atrixware manages exceptions and emergency changes through its established change management practices. Changes are evaluated based on their nature and urgency, with security-related and emergency changes capable of being addressed on an expedited basis. Changes are subsequently reviewed and documented through the applicable change and configuration management processes.

	CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0			
CCC-08.2	Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?	Yes	CSP-owned	Atrixware's change and configuration exception process is aligned with its policy exception practices. Exceptions, including emergency changes that require deviation from established procedures, are reviewed and approved by the CEO, and the reason for the exception is documented.
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	Atrixware maintains versioning of application changes that allows production changes to be rolled back to a previously known good version when errors or security concerns are identified. This capability supports recovery from unsuccessful or problematic changes.
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Atrixware maintains documented requirements and procedures governing cryptography, encryption, and key management. These requirements address the protection of data in transit and at rest, approved cryptographic methods, management and protection of encryption keys and cryptographic secrets, and access restrictions for authorized personnel. Responsibilities for managing encryption and cryptographic controls are defined, and the requirements are approved by management, communicated to applicable personnel, implemented, evaluated, and maintained. Encryption and key-management practices are reviewed periodically and when significant changes occur.
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually, upon significant changes?	Yes	CSP-owned	Atrixware reviews its cryptography, encryption, and key-management requirements periodically and when significant changes occur. The review evaluates whether encryption and key-management controls remain effective and appropriate, including applicable configurations, certificates, keys, access controls, and security requirements. Documentation is updated when changes to the requirements or practices are identified, and updates are approved and communicated as appropriate.
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes	CSP-owned	Atrixware defines and implements roles and responsibilities for cryptography, encryption, and key management. Responsibilities include management of encryption configurations, certificates, keys, and cryptographic secrets, with access restricted to authorized personnel.
CEK-03.1	Are data protection at-rest and in-transit, and where applicable in use, provided using cryptographic libraries certified to approved standards?	Yes	Shared CSP and 3rd-party	Encryption in transit is provided using mandatory HTTPS with TLS 1.2 and TLS 1.3 through Apache mod_ssl and the OpenSSL cryptographic library supplied by AlmaLinux. The underlying AlmaLinux platform provides a FIPS 140-3 validated OpenSSL cryptographic provider. Production systems are not configured to operate in FIPS mode, and Atrixware does not represent Axis LMS as operating in a FIPS 140-2/140-3 validated mode. At-rest storage encryption is provided and managed by the underlying infrastructure provider; Atrixware does not independently claim or attest to certification of the provider-managed storage cryptographic implementation.
CEK-04.1	Are encryption algorithms following industry standards utilized for protecting data, based on the data classification and associated risks?	Yes	CSP-owned	Encryption in transit is mandatory for LMS web traffic and uses TLS 1.2 and TLS 1.3 with industry-standard cryptographic algorithms. Configured cipher suites use authenticated encryption (AEAD), including AES-128-GCM, AES-256-GCM, and ChaCha20-Poly1305, with ECDHE/DHE ephemeral key exchange for TLS 1.2. SSLv2, SSLv3, TLS 1.0, and TLS 1.1 are disabled. Encryption requirements are applied to LMS web traffic based on the security requirements and risk associated with protecting customer information. Atrixware does not currently use a separate formal data-classification scheme to select among encryption algorithms.
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	CSP-owned	Atrixware applies its established change management procedures to changes affecting cryptography, encryption, and key management. Changes are reviewed, tested, approved, implemented through controlled deployment processes, and communicated to applicable personnel and stakeholders as appropriate. Changes originating from internal activities or external sources, including technology and infrastructure providers, are evaluated through the applicable change management process before adoption.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
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	Atrixware evaluates changes affecting cryptography, encryption, and key management as part of its change management and security review practices. Proposed changes are evaluated for security and operational impacts, including downstream effects, residual risk, implementation considerations, and expected benefits. Changes are reviewed and approved through the applicable change management process before implementation, with additional evaluation performed when significant changes to technology, infrastructure, or security requirements occur.
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	Atrixware incorporates cryptography, encryption, and key management risks into its security and risk management practices. Risks are evaluated in the context of the information and systems being protected, with appropriate risk treatment and mitigation measures identified as needed. Encryption and key-management practices are monitored and periodically evaluated, with changes and security findings considered as part of ongoing risk management and improvement activities.
CEK-08.1	Are service providers providing service customers with the capacity to manage their own data encryption keys?	No	CSP-owned	Atrixware does not provide the ability to independently manage encryption keys.
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	3rd-party outsourced	Hosting partner maintains processes for auditing encryption and key management systems, policies, and procedures based on the risk exposure of the systems and applicable security requirements. These controls are subject to Liquid Web's security and compliance assessment processes, including independent assessment activities.
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Yes	3rd-party outsourced	Hosting partner maintains ongoing security and compliance assessment processes covering encryption and key management systems, policies, processes, and controls. Independent assurance activities are performed as part of Liquid Web's security and compliance program.
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	Atrixware generates cryptographic keys using industry-accepted cryptographic libraries and operating-system cryptographic facilities. Key generation relies on established cryptographic algorithms and cryptographically appropriate random-number generation rather than custom application-level key-generation methods.
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes	CSP-owned	Atrixware manages private keys and cryptographic secrets according to their intended purpose and restricts access to authorized personnel and systems. Cryptographic secrets are protected from unauthorized disclosure, and access is limited based on operational requirements and least-privilege principles.
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Yes	3rd-party outsourced	Hosting Partner maintains cryptographic key management processes that include key rotation based on defined rotation periods and the intended use and security exposure of the cryptographic keys. Key management practices consider key lifecycle, information disclosure risks, and applicable security and compliance requirements.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
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?	No	3rd-party outsourced	The applicable third-party hosting provider has not provided assessment evidence sufficient to substantiate this specific control. The provider has indicated that this control was outside the scope of its available assessments and cannot attest to its implementation.
CEK-14.1	Are processes, procedures and technical measures to securely destroy cryptographic keys when they are no longer needed, defined, implemented, and evaluated, and include provisions for legal and regulatory requirements?	No	3rd-party outsourced	The applicable third-party hosting provider has not provided assessment evidence sufficient to substantiate this specific control. The provider has indicated that this control was outside the scope of its available assessments and cannot attest to its implementation.
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?	No	3rd-party outsourced	Cryptographic key management is provided by our hosting partner as part of the hosted infrastructure. Atrixware does not independently implement or manage a documented process for creating cryptographic keys in a pre-activated state as specified by this control.
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?	No	3rd-party outsourced	The applicable third-party hosting provider has not provided assessment evidence sufficient to substantiate this specific control. The provider has indicated that this control was outside the scope of its available assessments and cannot attest to its implementation.
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?	No	3rd-party outsourced	The applicable third-party hosting provider has not provided assessment evidence sufficient to substantiate this specific control. The provider has indicated that this control was outside the scope of its available assessments and cannot attest to its implementation.
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?	No	3rd-party outsourced	The applicable third-party hosting provider has not provided assessment evidence sufficient to substantiate this specific control. The provider has indicated that this control was outside the scope of its available assessments and cannot attest to its implementation.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
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?	No	3rd-party outsourced	Cryptographic key management is provided by our hosting partner as part of the hosted infrastructure. Atrixware does not independently implement or manage a documented process governing the controlled use of compromised cryptographic keys as specified by this control.
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?	No	3rd-party outsourced	The applicable third-party hosting provider has not provided assessment evidence sufficient to substantiate this specific control. The provider has indicated that this control was outside the scope of its available assessments and cannot attest to its implementation.
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?	No	3rd-party outsourced	The applicable third-party hosting provider has not provided assessment evidence sufficient to substantiate this specific control. The provider has indicated that this control was outside the scope of its available assessments and cannot attest to its implementation.
DCS-01.1	Are policies and procedures for physical and environmental security established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	3rd-party outsourced	Physical and environmental security policies and procedures are established and maintained by Atrixware's data center provider and include physical access controls, surveillance, environmental protections, power continuity, and infrastructure security
DCS-01.2	Are policies and procedures for physical and environmental security reviewed and updated at least annually, or upon significant changes?	Yes	3rd-party outsourced	Physical and environmental security policies and procedures are reviewed and updated periodically and upon significant changes by the data center provider.
DCS-02.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	Yes	3rd-party outsourced	The data center maintains secure equipment decommissioning and disposal policies, including controlled storage, sanitization, and destruction of equipment.
DCS-02.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Yes	3rd-party outsourced	A hardware sanitization process is used to irreversibly remove data from equipment prior to disposal when equipment is not physically destroyed.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
DCS-02.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually or upon significant changes?	Yes	3rd-party outsourced	Equipment disposal and sanitization policies are reviewed and maintained as part of the data center's security program.
DCS-03.1	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	3rd-party outsourced	The data center maintains procedures for the secure transfer and storage of hardware, software, and data to alternate or offsite locations as part of its infrastructure and backup practices.
DCS-03.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	No	3rd-party outsourced	The applicable third-party hosting provider has not provided assessment evidence sufficient to substantiate this specific control. Its available PCI DSS assessment does not address this requirement, and the provider cannot attest to its implementation.
DCS-03.3	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, or upon significant changes?	Yes	3rd-party outsourced	Data center relocation and transfer policies and procedures are reviewed and maintained as part of the provider's security and operational program.
DCS-04.1	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	3rd-party outsourced	The data center maintains policies and procedures for safe and secure working environments, including controlled physical access, surveillance, visitor management, and environmental protections.
DCS-04.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually, or upon significant changes?	Yes	3rd-party outsourced	Physical and environmental security policies and procedures are reviewed and maintained as part of the data center's ongoing security program.
DCS-05.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	Yes	3rd-party outsourced	The data center maintains procedures for the secure handling and transportation of physical media, including controlled handling and secure transfer practices.
DCS-05.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually, or upon significant changes?	Yes	3rd-party outsourced	Physical media transportation policies and procedures are reviewed and maintained as part of the data center's ongoing security program.
DCS-06.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Yes	3rd-party outsourced	The data center maintains formal asset inventory and audit practices to track physical infrastructure and equipment.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
DCS-06.2	Are assets' classifications reviewed and updated at least annually or upon significant changes?	Yes	3rd-party outsourced	Asset inventories are regularly reviewed and audited as part of the data center's security and operational practices.
DCS-07.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Yes	3rd-party outsourced	The data center maintains a formal inventory system to catalog and track physical assets within its facilities, with regular audits to maintain accuracy and compliance.
DCS-07.2	Is the catalogue reviewed and updated at least annually or upon significant changes?	Yes	3rd-party outsourced	The data center regularly audits and updates its asset inventory as part of its security and operational practices.
DCS-08.1	Are physical security perimeters designed and implemented to safeguard personnel, data, and information systems?	Yes	3rd-party outsourced	Physical security perimeters are implemented using reinforced facility structures, electronic access controls, surveillance systems, visitor controls, and restricted access to authorized personnel to safeguard personnel, data, and information systems.
DCS-09.1	Is equipment identification used as a method for connection authentication?	No	3rd-party outsourced	The applicable third-party hosting provider has not provided assessment evidence sufficient to substantiate this specific control. Its available PCI DSS assessment does not address this requirement, and the provider cannot attest to its implementation.
DCS-10.1	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	Access to secure areas is restricted to authorized personnel through electronic physical access controls. Ingress and egress are monitored and access activity is logged, with visitor identification and escort procedures also enforced.
DCS-10.2	Are access control records retained periodically, as deemed appropriate by the organization?	Yes	3rd-party outsourced	Physical access records are retained for at least 90 days, including successful and unsuccessful badge access attempts, and are reviewed as part of the data center's physical security practices.
DCS-11.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Yes	3rd-party outsourced	The data center operates and maintains surveillance systems throughout the facility, including areas covering physical access points, work areas, and server rooms.
DCS-12.1	Are datacenter personnel trained to safely manage adverse events, including but not limited to unauthorized ingress and egress attempts?	Yes	3rd-party outsourced	Data center personnel receive security awareness training that includes physical security practices, tailgating prevention, and situational awareness to support safe response to adverse physical security events.
DCS-13.1	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	The data center protects power and telecommunications cabling through secured-area access controls, including restricted access and CCTV monitoring. Diverse redundant fiber and power paths are used to reduce risks from damage and interference, and inter-site traffic is encrypted to mitigate interception.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
DCS-14.1	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	3rd-party outsourced	Data center environmental control systems monitor and maintain temperature and humidity conditions within established operating parameters. Environmental systems are maintained and monitored as part of the data center's ongoing facility operations.
DCS-15.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	Yes	3rd-party outsourced	Data center utility services, including power and telecommunications, are secured, monitored, maintained, and supported by redundant infrastructure. Utility and infrastructure systems are maintained and tested as part of the data center's operational practices.
DCS-16.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	Yes	3rd-party outsourced	Business-critical equipment is housed within controlled data center facilities designed to reduce exposure to environmental risks. Facilities include environmental controls, physical security, redundant power, and other infrastructure protections.
DCS-17.1	Are datacenter security metrics established, monitored, and reported to secure data center assets and services?	Yes	3rd-party outsourced	Data center security and operational activities are monitored through established security practices, including risk assessments, incident and action reviews, access reviews, infrastructure monitoring, and physical security controls.
DCS-18.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure continuous operations?	Yes	3rd-party outsourced	The data center maintains processes, procedures, and technical measures supporting continuous operations, including infrastructure redundancy, power continuity, network redundancy, environmental controls, backups, physical security, and business continuity practices.
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the preparation, classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	Yes	CSP-owned	Atrixware maintains documented security policies and procedures addressing the protection and handling of customer data throughout its lifecycle. These practices include access controls, encryption, data protection, secure development, backup, retention, and secure removal of data.
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews and maintains its data security and privacy practices periodically and when significant changes occur to services, systems, or applicable requirements.
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	3rd-party outsourced	The data center maintains procedures for secure equipment decommissioning, including data sanitization and destruction of storage media to prevent unauthorized recovery.
DSP-03.1	Is a data inventory created and maintained for sensitive, regulated and personal information (at a minimum)?	Yes	Shared CSP and CSC	Narrative inventory of provider-collected personal data ("What we collect and why"); customer-uploaded content is not inventoried by Atrixware, as the customer determines and manages the data entered into its LMS environment.
DSP-03.2	Is the inventory reviewed and updated at least annually or upon significant changes?	Yes	Shared CSP and CSC	Atrixware reviews and updates its inventory of provider-collected personal data periodically and when significant changes occur. Customer-managed LMS content is maintained by the customer within its Axis LMS environment.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
DSP-04.1	Is data classified according to type and sensitivity levels?	Yes	Shared CSP and CSC	Atrixware maintains a documented Data Classification and Handling Procedure that classifies information based on sensitivity, business importance, and potential impact. The procedure defines Public, Internal, Confidential, and Restricted classifications and establishes handling, access, protection, and disposal requirements appropriate to each classification.
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Yes	Shared CSP and CSC	Atrixware maintains documented Axis LMS boundary and data flow diagrams identifying system components, data storage locations, external connections, backup storage, and data transmission paths. The Data Flow Diagram identifies applicable encryption for data transmitted between system components and external parties, as well as encryption applied to backup and storage environments.
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, or upon significant changes?	Yes	Shared CSP and CSC	Data flow information is maintained as part of Atrixware's application and operational documentation. Customer-managed LMS content is maintained within the customer's Axis LMS environment.
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Yes	Shared CSP and CSC	Atrixware's provider-collected personal data is managed by Atrixware, while customer-entered LMS data remains under the customer's ownership and stewardship within its Axis LMS environment.
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	Yes	Shared CSP and CSC	Atrixware maintains a documented Data Ownership and Stewardship Procedure defining information ownership and stewardship responsibilities. Data ownership and stewardship responsibilities are reviewed at least annually and when significant changes occur to services, systems, information, business responsibilities, contractual requirements, or applicable security risks.
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Yes	CSP-owned	Atrixware incorporates security principles into the design and development of Axis LMS. Application security practices include input validation, data sanitization, output encoding, secure error handling, static analysis, quality assurance testing, controlled development environments, and sandbox testing before production deployment.
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Yes	CSP-owned	Atrixware incorporates privacy and data protection considerations into its application and business practices. Provider-collected personal data is limited to information needed to provide and administer the service, while customer-entered LMS content is managed by the customer.
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	Yes	CSP-owned	Axis LMS applies privacy and security settings through its standard application configuration and access controls. Provider-collected personal information is handled according to Atrixware's established data protection practices and applicable service requirements.
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	Atrixware follows GDPR requirements for applicable processing of personal data and evaluates privacy risks associated with such processing, including the nature and potential impact of the processing, as required by applicable requirements.
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	Shared CSP and CSC	Atrixware applies access controls, encryption, authentication, logging, and other security measures to protect personal and sensitive data during processing and transfer. Customer-managed LMS content is processed within the customer's Axis LMS environment according to the service relationship.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
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	Shared CSP and CSC	Atrixware supports requests concerning provider-collected personal data through its operational and customer-support processes. Customers manage personal data they enter into their Axis LMS environment, including access, modification, and deletion of that data.
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	CSP-owned	Atrixware processes provider-collected personal data for the purposes associated with providing and administering Axis LMS and in accordance with applicable privacy requirements, including GDPR. Customer-entered LMS data is processed within the customer's Axis LMS environment according to the customer's intended use.
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	Shared CSP and 3rd-party	Atrixware maintains controls governing the transfer and processing of personal data within its service supply chain. Third-party providers supporting Axis LMS are subject to applicable security and data protection requirements.
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	Shared CSP and 3rd-party	Atrixware provides applicable information regarding third-party service providers involved in processing customer data through its service and contractual/privacy documentation. Third-party processing is subject to applicable data protection and security requirements.
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	Shared CSP and CSC	Customer production data is not used or replicated in non-production environments. Atrixware uses separate, controlled environments for development and testing.
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes	Shared CSP and 3rd-party	Atrixware maintains data retention and deletion practices in accordance with business and applicable data protection requirements. Upon service termination, customer data is promptly removed, with backups purged within 30 days. The hosting provider maintains nightly backups with retention of up to 30 days.
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Yes	Shared CSP and 3rd-party	Atrixware and its hosting provider apply security controls to protect sensitive data throughout its lifecycle, including access controls, encryption in transit, secure hosting, backups, logging, and secure data removal.
DSP-18.1	Does the service provider ensure that a procedure is in place and communicated to service customers for managing and responding to requests by law enforcement authorities for the disclosure of personal data, in accordance with applicable laws and regulations?	Yes	CSP-owned	Atrixware maintains procedures for responding to lawful requests from law enforcement authorities for disclosure of personal data, in accordance with applicable laws and regulations. Applicable requirements are communicated through Atrixware's service and privacy documentation.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
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	Shared CSP and 3rd-party	Atrixware documents the locations where customer data is hosted and processed. Axis LMS is hosted through the designated data center infrastructure, with backups maintained by the hosting provider. Data center and backup locations are managed as part of the hosting infrastructure.
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	Atrixware maintains an information security governance program supported by organizational leadership. Security policies and procedures are documented, approved, communicated, implemented, and maintained as part of Atrixware's ongoing security practices.
GRC-01.2	Are the policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews its information security policies and procedures at least annually and when significant changes occur. Updates are maintained and communicated as appropriate.
GRC-02.1	Is there an established and maintained formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of risks?	Yes	CSP-owned	Atrixware maintains a documented, leadership-sponsored information security risk management program for identifying, assessing, prioritizing, treating, and monitoring information security risks. Risks are evaluated based on likelihood, potential impact, existing controls, and other relevant security and business factors, with significant risks subject to management oversight.
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	Atrixware reviews its relevant organizational security policies and associated procedures at least annually and when significant organizational or operational changes occur.
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	Atrixware maintains an approved exception process for deviations from established policies and procedures. Exceptions are reviewed and approved by the CEO, with the reason for the exception documented.
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Yes	CSP-owned	Atrixware maintains an information security program covering security policies, procedures, application security, access control, data protection, business continuity, change management, and other applicable security practices.
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes	CSP-owned	Atrixware defines responsibilities for implementing, operating, reviewing, and improving its information security and governance practices. Responsibilities are assigned to appropriate personnel and management.
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Yes	CSP-owned	Atrixware identifies and maintains applicable legal, regulatory, contractual, privacy, and security requirements relevant to its operations and Axis LMS services, including applicable GDPR requirements.

	CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0			
GRC-07.2	Are the identified requirements reviewed at least annually or upon significant changes?	Yes	CSP-owned	Atrixware reviews applicable legal, regulatory, contractual, privacy, and security requirements periodically and when significant changes occur.
GRC-08.1	Is contact established and maintained with related special interest groups and other relevant entities?	Yes	CSP-owned	Atrixware maintains contact with relevant technology, security, hosting, and industry organizations and other entities as appropriate to support its security and operational practices.
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	Atrixware requires prospective personnel to complete an application and undergo appropriate security and background verification prior to employment.
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	Atrixware's pre-employment screening practices are conducted in accordance with applicable employment requirements and are appropriate to the responsibilities and access associated with the position.
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews its personnel screening and background verification practices at least annually and when significant changes occur.
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	Atrixware maintains requirements governing the acceptable use of organizationally owned or managed systems, devices, and other company assets. Use is subject to security and access requirements appropriate to the assets and the user's responsibilities.
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, or upon significant changes?	Yes	CSP-owned	Atrixware reviews its acceptable-use requirements periodically and when significant changes occur to organizational systems, technology, or security requirements.
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	Atrixware maintains requirements for securing confidential information when workspaces are unattended, including appropriate protection of information displayed or accessible through organizational systems.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews its requirements for protecting confidential information in unattended workspaces at least annually and when significant changes occur.
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	Atrixware maintains security requirements for information accessed, processed, or stored at remote locations. These requirements include appropriate access controls, authentication, encryption, and protection of company and customer information.
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, or upon significant changes?	Yes	CSP-owned	Atrixware reviews its remote-work and remote-access security requirements at least annually and when significant changes occur.
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	CSP-owned	Atrixware maintains procedures for returning organizationally owned assets when employees terminate employment or no longer require access.
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all relevant personnel?	Yes	CSP-owned	Atrixware defines and communicates roles and responsibilities associated with changes in employment, including changes to access and organizational responsibilities.
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Yes	CSP-owned	Atrixware defines and communicates roles and responsibilities associated with changes in employment, including changes to access and organizational responsibilities.
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes	CSP-owned	Atrixware's employment requirements include adherence to applicable information security, confidentiality, and data protection requirements.
HRS-09.1	Are employee roles and responsibilities relating to information assets' security and privacy, established, documented and communicated?	Yes	CSP-owned	Atrixware establishes and communicates employee responsibilities for protecting organizational information assets and maintaining applicable security and privacy requirements.
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	Atrixware uses confidentiality and non-disclosure provisions appropriate to its data protection and operational requirements. These requirements are maintained as part of its employment and security practices.

	CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0			
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	Atrixware maintains a security awareness program for employees covering information security, data protection, access security, and applicable security responsibilities.
HRS-11.2	Are regular security awareness training updates provided?	Yes	CSP-owned	Atrixware provides regular security awareness training updates to employees as part of its ongoing security practices.
HRS-12.1	Are employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	CSP-owned	Employees with access to sensitive organizational or personal data receive security awareness training appropriate to their responsibilities and access.
HRS-12.2	Are 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	Employees receive updates to security procedures, processes, and policies relevant to their professional responsibilities as changes occur.
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	Atrixware communicates employee roles and responsibilities for maintaining compliance with applicable security policies, procedures, and legal, statutory, and regulatory requirements.
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	Atrixware maintains documented identity and access management practices covering user accounts, authentication, authorization, role-based access, least privilege, access restrictions, and logging.
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews its identity and access management practices periodically and when significant changes occur.
IAM-02.1	Are policies and procedures for the management of authentication credentials, including passwords, established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	Atrixware maintains requirements for authentication credentials, including unique user accounts, password controls, failed-login protections, password expiration settings, and access restrictions.
IAM-02.2	Are policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews its authentication credential and password-management requirements periodically and when significant changes occur.
IAM-03.1	Is the inventory of identities managed, stored, and regularly reviewed, and is their level of access monitored?	Yes	CSP-owned	Atrixware manages user identities and associated access within Axis LMS. User accounts, roles, access levels, and account activity are maintained and monitored through the LMS's access-control and logging capabilities.

	CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0			
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes	CSP-owned	Atrixware applies separation of duties through role-based access controls, limiting administrative and other privileged functions to personnel with appropriate responsibilities.
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes	CSP-owned	Atrixware applies least-privilege principles to access to client LMS environments, hosting infrastructure, source code, and underlying data. Access is restricted according to role and operational requirements.
IAM-06.1	Is an identity access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes	CSP-owned	Atrixware maintains an access provisioning process that assigns access based on authorized roles and responsibilities. Access changes are managed through established administrative and access-control procedures.
IAM-07.1	Is a process in place to de-provision or modify identity access in a timely manner?	Yes	CSP-owned	Atrixware maintains processes for timely modification or removal of user access when access requirements change or an account is no longer authorized.
IAM-08.1	Are reviews and revalidation of identity access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance, and at least annually or upon significant changes?	Yes	CSP-owned	Atrixware reviews and revalidates identity access based on least-privilege and separation-of-duties principles, including periodic reviews and reviews when significant changes occur.
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated?	Yes	CSP-owned	Atrixware separates privileged access roles through role-based access controls and restricts administrative and other privileged functions to authorized personnel based on their responsibilities.
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	Temporary access roles are not assigned
IAM-10.2	Are procedures implemented to prevent the accumulation of segregated privileged access?	Yes	CSP-owned	Atrixware manages privileged access through role-based access controls and access reviews to help prevent unnecessary accumulation of privileged access.
IAM-11.1	Are processes and procedures for service customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?	Yes	Shared CSP and 3rd-party	Atrixware manages privileged access to customer environments according to established access-control practices. Customer participation in granting high-risk privileged access is available where specifically required by the service arrangement.
IAM-12.1	Are processes, procedures, and technical measures that ensure identities' activities are identifiable through uniquely associated IDs defined, implemented, and evaluated?	Yes	CSP-owned	Atrixware uses uniquely associated user IDs and accounts to identify user activities within Axis LMS. User actions, login attempts, IP information, and device information are logged.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
IAM-13.1	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	Shared CSP and CSC	Atrixware uses authentication and authorization controls to restrict access to systems, applications, and data based on user roles and privileges. Axis LMS supports multifactor authentication through optional email or SMS-based 2FA which customers can enable for their LMS.
IAM-13.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Yes	CSP-owned	Atrixware uses digital certificates and TLS to establish secure system communications and authenticate protected connections.
IAM-14.1	Are processes, procedures, and technical measures for the secure management of authentication credentials, including passwords, defined, implemented, and evaluated?	Yes	CSP-owned	Atrixware maintains secure authentication credential practices, including unique user accounts, password controls, failed-login protections, password expiration settings, and access restrictions.
IAM-15.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Yes	CSP-owned	Atrixware verifies authorization before granting access to data and system functions through role-based access controls, authentication, and least-privilege principles.
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application interfaces (e.g., APIs)?	Yes	CSP-owned	Atrixware maintains security requirements for communications between application interfaces, including APIs. Axis LMS API communications use authentication, authorization, TLS/HTTPS, input validation, logging, and rate limiting/throttling.
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Yes	CSP-owned	Atrixware maintains application and integration practices supporting interoperability between Axis LMS and connected systems. Interfaces and integrations are implemented using defined application and security requirements.
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	Yes	CSP-owned	Atrixware follows established application development practices that support maintainability and portability of Axis LMS components and integrations. Application changes are developed and tested in controlled environments before production deployment.
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	Shared CSP and CSC	Atrixware maintains controls supporting the secure exchange, use, integrity, and persistence of information within Axis LMS and its integrations. Customers are responsible for the data they enter and exchange through their LMS environment, while Atrixware provides the application and security controls supporting that data.
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews its interoperability and portability practices periodically and when significant changes occur to applications, integrations, or supporting technology.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
IPY-02.1	Are service customers able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes	Shared CSP and CSC	Axis LMS provides application interfaces that enable customers to programmatically retrieve and exchange data for interoperability and portability purposes.
IPY-03.1	Are cryptographically secure network protocols implemented for the management, import, and export of data in accordance with industry standards?	Yes	CSP-owned	Atrixware uses cryptographically secure network protocols for the management, import, and export of data. Axis LMS API and web communications use TLS/HTTPS with industry-standard cryptographic protocols.
IPY-04.1	Do agreements include provisions specifying service customers' data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the service customers d. Data deletion policy	Yes	Shared CSP and CSC	Atrixware's service agreement addresses customer data access and handling upon termination. Customer data is promptly removed following termination, with backups purged within 30 days. Data is provided and maintained in the formats and through the access methods supported by Axis LMS and applicable service terms.
I&S-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Atrixware maintains infrastructure and virtualization security practices covering access control, system hardening, network security, monitoring, vulnerability management, backups, and protection of hosted Axis LMS environments.
I&S-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews its infrastructure and virtualization security practices periodically and when significant changes occur.
I&S-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	Atrixware monitors system resources and capacity as part of ongoing operation of Axis LMS and its supporting infrastructure to help maintain required system performance and availability.
I&S-03.1	Are communications between environments, services, and applications monitored?	Yes	CSP-owned	Communications between environments, services, and applications are monitored through network security, logging, intrusion detection, and other operational security practices.
I&S-03.2	Are communications between environments, services, and applications encrypted?	Yes	CSP-owned	Communications between environments, services, and applications are protected using encrypted network protocols where applicable. Axis LMS web and API communications use TLS/HTTPS.
I&S-03.3	Are communications between environments, services, and applications restricted to only authenticated and authorized connections, as justified by the business?	Yes	CSP-owned	Communications between environments, services, and applications are restricted through authentication, authorization, access controls, firewalls, and network security configurations appropriate to the connection.
I&S-03.4	Are network configurations reviewed at least annually?	Yes	CSP-owned	Atrixware reviews network security configurations periodically and when significant changes occur.
I&S-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Yes	CSP-owned	Atrixware maintains network security configurations that restrict services, protocols, and ports to those required for operation. Network security controls, including firewalls and access restrictions, are used to limit unnecessary or unauthorized network communications.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
I&S-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	3rd-party outsourced	The hosting provider maintains hardened server and infrastructure configurations using established security practices and technical controls. Infrastructure security includes server hardening, firewalls, intrusion detection, malware protection, and other applicable security controls.
I&S-05.1	Are the environments separated into production and non production environments to reduce the risk of sensitive production data being used in non-production environments?	Yes	CSP-owned	Atrixware maintains separate development, sandbox/semi-production, and production environments. Application changes are developed and tested in controlled non-production environments before production deployment, and customer production data is not used in non-production environments.
I&S-05.2	Is production data sanitized or protected before being used for any authorized non-production purpose?	NA	CSP-owned	Customer production data is not used in non-production environments.
I&S-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that service customer (tenant) access is appropriately segmented, segregated, monitored, and restricted?	Yes	CSP-owned	Axis LMS uses tenant and role-based access controls to segregate customer environments and restrict access to authorized users. Access to customer LMS environments is authenticated, authorized, and logged.
I&S-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	3rd-party outsourced	Secure and encrypted communication channels using current approved protocols are used for applicable migration and transfer activities to cloud-hosted environments.
I&S-08.1	Are high-risk environments identified and documented based on data sensitivity, threat exposure, and business impact?	Yes	CSP-owned	Atrixware applies security controls based on the sensitivity and security requirements of the systems and information being protected.
I&S-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	Shared CSP and 3rd-party	Atrixware and its hosting provider use defense-in-depth controls to protect against network-based attacks, including firewalls, intrusion detection, malware protection, access controls, network monitoring, and DDoS protection where provided by the hosting service. These controls support detection, protection, and timely response to network security events.
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Atrixware maintains logging and monitoring practices for Axis LMS and its supporting systems. These practices include user activity, login attempts, IP/device information, application actions, and security-related events.
LOG-01.2	Are policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews and maintains its logging and monitoring practices periodically and when significant changes occur.
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Yes	CSP-owned	Atrixware maintains controls for protecting and retaining audit logs. Axis LMS records login attempts, user actions, IP and device information, and application changes through its logging and changelog capabilities.

	CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0			
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes	Shared CSP and 3rd-party	Security-related events are monitored through Axis LMS application logging and supporting infrastructure security controls. These include user activity and authentication logging, network security monitoring, intrusion detection, and other applicable security monitoring capabilities.
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	Atrixware maintains security monitoring and logging capabilities that generate alerts for detected security events and security-related activity. Alerts are reviewed and escalated to appropriate personnel based on the nature and significance of the event.
LOG-04.1	Is audit log access restricted to authorized identities, and are records of that access maintained?	Yes	CSP-owned	Access to audit and application logs is restricted to authorized personnel based on role and operational requirements. Access and user activity are logged where supported.
LOG-05.1	Are capabilities implemented and maintained to correlate and monitor security audit logs for the detection of suspicious or anomalous activity that deviates from typical or expected patterns?	No	3rd-party outsourced	The applicable third-party hosting provider has not provided assessment evidence sufficient to substantiate this specific control. The provider has indicated that the control was outside the scope of its available assessments and cannot attest to its implementation.
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes	CSP-owned	Atrixware evaluates identified security issues and anomalies through its security and operational processes, with appropriate action taken based on the nature and severity of the issue.
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes	3rd-party outsourced	Hosted systems use reliable system time sources as part of the underlying hosting and infrastructure environment.
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Yes	CSP-owned	Atrixware maintains logging requirements for relevant information system events, including authentication attempts, user activity, IP and device information, and application changes.
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment and as per relevant regulatory requirements?	Yes	CSP-owned	Atrixware reviews and updates logging requirements periodically and when significant changes occur to systems, security requirements, or the threat environment.
LOG-08.1	Are technical measures defined, implemented, and evaluated to enable service customers to detect and scrub or tokenize sensitive data from logs, in order to prevent unauthorized exposure as per applicable laws and regulations?	No	Shared CSP and CSC	Atrixware applies logging and access controls to protect information recorded in system logs; however, sufficient evidence has not been established to substantiate the specific requirement for detecting and scrubbing or tokenizing sensitive data from logs. The applicable third-party hosting provider has not provided assessment evidence sufficient to substantiate this control.
LOG-09.1	Are audit records generated, and do they contain relevant security information?	Yes	CSP-owned	Audit records are generated for relevant security and application events, including authentication attempts, user actions, IP and device information, and application changes.
LOG-10.1	Are audit records protected from unauthorized access, modification, and deletion?	Yes	CSP-owned	Audit records are protected through access controls and role-based restrictions to help prevent unauthorized access, modification, or deletion.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
LOG-11.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	Yes	3rd-party outsourced	Liquid Web maintains monitoring and internal reporting capabilities for cryptographic operations, encryption, and key management controls. Relevant system and security activity is captured through audit and system logging and is forwarded to monitoring and reporting tools for analysis as applicable.
LOG-12.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Yes	3rd-party outsourced	Liquid Web maintains logging and monitoring of cryptographic key management activities to support auditing and reporting throughout the key lifecycle. System and security activity is captured in audit and system logs and may be forwarded to monitoring and reporting tools for analysis.
LOG-13.1	Is physical access logged and monitored using an auditable access control system?	Yes	3rd-party outsourced	The data center uses an auditable physical access control system. Badge access activity, including successful and unsuccessful access attempts, is logged and retained, with physical access monitored through electronic access controls and surveillance.
LOG-14.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Yes	3rd-party outsourced	The data center maintains monitoring and operational processes for identifying and reporting system anomalies and failures. Infrastructure, network, security, and environmental systems are monitored as part of ongoing operations.
LOG-14.2	Are accountable parties immediately notified about anomalies and failures?	Yes	3rd-party outsourced	Appropriate personnel are notified of identified infrastructure, security, or operational anomalies and failures through the data center's monitoring and incident-management processes.
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	CSP-owned	Atrixware maintains security incident management practices addressing identification, response, investigation, remediation, and recovery of security incidents. These practices support the handling of security events involving Axis LMS and its supporting infrastructure.
SEF-01.2	Are policies and procedures reviewed and updated annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews and maintains its security incident management practices periodically and when significant changes occur.
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Atrixware maintains procedures for the timely identification, assessment, response, remediation, and recovery of security incidents involving Axis LMS and its supporting systems.
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews and maintains its security incident management procedures at least annually and when significant changes occur.
SEF-03.1	Is a security incident response plan that includes a communication strategy for notifying relevant internal departments, impacted service customers, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Atrixware maintains a security incident response process that includes communication and notification procedures for relevant personnel, affected customers, and other applicable parties.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
SEF-04.1	Is a structured approach followed to evaluate the effectiveness of incident response plans at planned intervals or upon significant changes?	Yes	CSP-owned	Atrixware evaluates its incident response capabilities through established security and operational practices and reviews them periodically and when significant changes occur.
SEF-05.1	Are information security incident metrics established, monitored and reported?	Yes	CSP-owned	Atrixware maintains documented security incident metrics covering incident volume, severity, detection, response and resolution timing, open and closed incidents, remediation status, and recurring trends. Security incident metrics are reviewed at least quarterly, with significant findings and trends communicated to appropriate management personnel and addressed through applicable security, incident response, risk management, and remediation processes.
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Yes	CSP-owned	Atrixware evaluates and triages security-related events based on their nature, severity, potential impact, and required response.
SEF-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for timely and effective response to security incidents in accordance with incident categories and severity levels?	Yes	CSP-owned	Atrixware maintains incident response practices for timely and effective handling of security incidents based on the nature and severity of the incident.
SEF-07.2	Are these processes and procedures reviewed, updated, and tested at least annually?	Yes	CSP-owned	Atrixware reviews and maintains its incident response procedures periodically and when significant changes occur.
SEF-08.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes	CSP-owned	Atrixware maintains procedures for assessing security incidents and communicating applicable security or breach notifications to affected parties in accordance with applicable requirements.
SEF-08.2	Are material security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	Yes	CSP-owned	Atrixware handles material security and breach notifications in accordance with applicable contractual, legal, regulatory, and customer requirements.
SEF-09.1	Is a secure repository of security incident records established and maintained?	Yes	CSP-owned	Atrixware maintains records of security incidents and related response activities through its established security and operational processes.
SEF-09.2	Are incident records regularly reviewed to identify patterns, root causes, and systemic vulnerabilities, and are relevant corrective measures implemented?	Yes	CSP-owned	Atrixware reviews security incidents and related issues to identify causes, trends, and opportunities for corrective action and improvement.
SEF-10.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Yes	CSP-owned	Atrixware maintains appropriate points of contact for applicable regulatory, legal, and law enforcement authorities as needed for security incident response and legal or regulatory matters.
SEF-10.2	Are points of contact reviewed and updated at least annually?	Yes	CSP-owned	Applicable regulatory, legal, and law enforcement contact information is maintained and updated as needed as part of Atrixware's security and compliance practices.

	CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0			
STA-01.1	Are policies and procedures for supply chain risk management established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Atrixware maintains a risk-based supply chain management process for identifying, assessing, and managing security and privacy risks associated with relevant third-party service providers supporting the Axis LMS service.
STA-01.2	Are policies and procedures for supply chain risk management reviewed and updated at least annually, or upon significant changes?	Yes	CSP-owned	Atrixware maintains documented supply chain risk management policies and procedures that are reviewed at least annually and updated when significant changes to services, providers, risks, or security requirements occur. The review and update process is part of Atrixware's Third-Party and Supply Chain Risk Management Procedure.
STA-02.1	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	Atrixware applies shared security responsibilities between Atrixware, its customers, and third-party service providers. Responsibilities for application security, customer-managed data, hosting infrastructure, access, and related security controls are assigned according to the services provided.
STA-02.2	Are the policies and procedures that apply the SSRM reviewed and updated annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews and maintains its shared security responsibility practices as part of its security program and when significant changes occur to services, systems, or responsibilities.
STA-03.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain?	Yes	CSP-owned	Atrixware applies shared security responsibilities across its service supply chain, including responsibilities involving Atrixware, customers, and third-party service providers.
STA-04.1	Is the service customer given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	Yes	CSP-owned	Atrixware provides customers with information regarding shared security responsibilities and the respective responsibilities of Atrixware, customers, and applicable third-party providers.
STA-05.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM?	Yes	CSP-owned	Atrixware delineates the ownership and applicability of CSA CCM controls between Atrixware, service customers, and applicable third-party providers through its documented shared security responsibility model.
STA-06.1	Is the SSRM documentation reviewed and validated?	Yes	CSP-owned	Atrixware reviews and validates its shared security responsibility documentation as part of its security and compliance practices.
STA-07.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes	CSP-owned	Atrixware implements and operates the portions of the shared security responsibility model assigned to Atrixware and evaluates those controls through its security and operational practices.
STA-08.1	Is an inventory of all supply chain relationships developed and maintained?	Yes	CSP-owned	Atrixware maintains information regarding its relevant supply chain relationships, including third-party providers supporting the Axis LMS service.
STA-09.1	Is a process defined, implemented, and enforced for establishing a Bill of Material for the service supply chain?	Yes	CSP-owned	Atrixware maintains a documented Supply Chain Bill of Materials (BOM) identifying significant third-party providers, infrastructure services, and material dependencies supporting the Axis LMS service. The BOM identifies the provider or component, service or function, dependency, and relevant security or operational significance.
STA-09.2	Is the Bill of Material reviewed and updated at least annually or upon significant changes?	Yes	CSP-owned	Atrixware reviews the Axis LMS Supply Chain BOM at least annually and when significant changes occur to the Axis LMS architecture, hosting environment, providers, material service dependencies, or security requirements. Identified changes are documented in the current BOM.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
STA-10.1	Are risk factors associated with supply chain relationships periodically reviewed?	Yes	CSP-owned	Atrixware evaluates security and operational risks associated with relevant third-party and supply chain relationships as part of its security and vendor management practices.
STA-11.1	Do service agreements between service providers and service customers (tenants) incorporate at least the following mutually agreed upon provisions and/or terms? • Scope, characteristics, and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third-party assessment • Service termination • Interoperability and portability requirements • Data privacy • Operational Resilience	Yes	CSP-owned	Atrixware's service agreements define the scope and characteristics of the services, security responsibilities, change management, incident communication, service termination, data privacy, and operational requirements.
STA-12.1	Are supply chain agreements reviewed at least annually or upon significant changes?	Yes	CSP-owned	Atrixware reviews supply chain agreements and related requirements periodically and when significant changes occur.
STA-13.1	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	Atrixware maintains a documented Annual Internal Security Assessment Procedure requiring a formal internal security assessment at least annually. The assessment reviews applicable information security controls, policies, procedures, access management, application and infrastructure security, vulnerability and risk management, data protection, incident management, business continuity, third-party security, and applicable CAIQ/CCM requirements. Assessment findings are documented, evaluated, prioritized, and tracked through the applicable risk-management and remediation processes.
STA-14.1	Are policies that require all supply chain service providers to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Yes	CSP-owned	Atrixware requires applicable service providers to comply with relevant information security, confidentiality, access control, privacy, audit, personnel, and service requirements.
STA-15.1	Are the organization's service providers' IT governance policies and procedures reviewed at least annually or upon significant changes?	Yes	CSP-owned	Atrixware reviews applicable service provider governance policies and procedures periodically and when significant changes occur.
STA-16.1	Is a process defined and implemented for conducting risk-based security assessments of the supply chain?	Yes	CSP-owned	Atrixware maintains and implements a risk-based process for assessing the security of third-party service providers supporting the Axis LMS service. Assessments consider provider services, system and data access, operational dependency, security controls, business continuity, and other relevant security and privacy risks.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
TVM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities and threats to protect systems against vulnerability exploitation?	Yes	CSP-owned	Atrixware maintains documented vulnerability and threat management practices for identifying, reporting, prioritizing, and remediating security vulnerabilities and threats. Security issues are evaluated based on severity and potential impact, with critical issues addressed on an expedited basis.
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews and updates its threat and vulnerability management practices periodically and when significant changes occur.
TVM-02.1	Are policies and procedures to protect against malware and malicious instructions established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Atrixware maintains documented malware protection practices, including malware scanning and protective controls within the hosted environment.
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews and maintains applicable asset management and malware protection practices periodically and when significant changes occur.
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Yes	3rd-party outsourced	Atrixware's hosting provider performs ongoing vulnerability management and security monitoring of the hosted infrastructure including vulnerability scanning and related protective measures for all hosting tiers above standard.
TVM-04.1	Are a threat analysis process and procedures defined, implemented, and evaluated to identify, assess, and review the threat landscape for cloud systems?	Yes	CSP-owned	Atrixware evaluates security threats and vulnerabilities affecting its cloud-based Axis LMS environment through its security, vulnerability management, and risk assessment practices.
TVM-04.2	Are threat models built according to industry best practices to inform the risk mitigation strategy?	Yes	CSP-owned	Atrixware evaluates threats and vulnerabilities as part of its security and risk management practices.
TVM-05.1	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	3rd-party outsourced	The hosting environment uses security monitoring, malware protection, intrusion detection, and vulnerability management practices to identify and respond to security threats.
TVM-06.1	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	CSP-owned	Atrixware evaluates application dependencies and third-party/open-source components as part of application development, security testing, maintenance, and vulnerability remediation practices.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
TVM-07.1	Are processes, procedures and technical measures defined, implemented and evaluated for the periodic performance of penetration testing by independent third parties?	Yes	Shared CSP and 3rd-party	Atrixware has defined and documented processes, procedures, and technical measures governing the periodic performance of penetration testing by independent third parties. The process establishes testing scope, frequency, independent tester selection, authorization, reporting, remediation, retesting, and recordkeeping requirements. The penetration testing procedure is reviewed at least annually and updated as appropriate based on changes to the Axis LMS environment, security requirements, and identified risks.
TVM-08.1	Are processes, procedures and technical measures defined, implemented and evaluated based on identified risks to support scheduled and emergency responses to vulnerability identification?	Yes	CSP-owned	Atrixware maintains processes for scheduled and expedited remediation of identified vulnerabilities based on their severity, potential impact, and applicable security requirements.
TVM-09.1	Is vulnerability remediation prioritized using a risk-based method from an industry-recognized framework?	Yes	CSP-owned	Atrixware uses a documented, risk-based vulnerability prioritization process based on the Common Vulnerability Scoring System (CVSS). Vulnerabilities are evaluated based on technical severity and relevant environmental and business risk factors, including exploitability, system exposure, potential impact, and available mitigations. Remediation priorities are assigned based on the resulting risk.
TVM-10.1	Is a risk-based method used for the prioritization and mitigation of threats, leveraging an industry-recognized framework to guide threat decision-making and protection measures?	Yes	CSP-owned	Atrixware uses a documented, risk-based method for evaluating and prioritizing security threats aligned with recognized cybersecurity risk-management practices. Threats are evaluated based on likelihood, potential impact, affected systems or information, existing controls, and available mitigation measures. Mitigation activities are prioritized according to the resulting risk.
TVM-11.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes	CSP-owned	Atrixware tracks vulnerability and security issues through its application security and maintenance processes, with relevant personnel notified as appropriate.
TVM-12.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Yes	CSP-owned	Atrixware maintains vulnerability identification and remediation metrics, including vulnerability severity, remediation status, and remediation timing. Metrics are reviewed at least quarterly, with significant findings and trends communicated to appropriate personnel and addressed through applicable security and remediation processes.
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes	CSP-owned	Atrixware maintains security practices for endpoints used to access and manage organizational systems and data, including authentication, access control, security configuration, and protection of information.
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually, or upon significant changes?	Yes	CSP-owned	Atrixware reviews and maintains applicable endpoint security practices periodically and when significant changes occur.
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	Atrixware maintains a documented list of approved applications and software sources permitted for use on company-managed endpoints when accessing or storing company data. The list is reviewed as part of endpoint security management.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	Yes	CSP-owned	Atrixware validates endpoint compatibility with supported operating systems and applications when deploying or updating software to help ensure functionality and security requirements are maintained.
UEM-04.1	Is an inventory of all endpoints used and maintained to store, access and process company data?	Yes	CSP-owned	Atrixware maintains an inventory of company-managed endpoints used to store, access, or process company data. The inventory is maintained to support endpoint management and security oversight.
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	Atrixware applies security and access controls to endpoints permitted to access organizational systems and data, including authentication, access restrictions, security configuration, and protection of information.
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes	CSP-owned	Atrixware requires company-managed interactive-use endpoints to automatically lock after a defined period of inactivity to help prevent unauthorized access.
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	Yes	CSP-owned	Atrixware manages relevant endpoint operating system, patch, and application changes through its established change management and security practices.
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	No	Shared CSP and 3rd-party	Atrixware uses encryption and access controls to protect organizational information; however, sufficient evidence has not been established to substantiate storage encryption on managed endpoints as required by this control. The applicable third-party hosting provider has not provided assessment evidence sufficient to substantiate this specific control.
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Yes	CSP-owned	Atrixware configures company-managed endpoints with anti-malware protection to detect and help prevent malicious software and other known threats.
UEM-10.1	Are software firewalls configured on managed endpoints?	Yes	CSP-owned	Atrixware configures company-managed endpoints with software firewalls enabled to help protect endpoints from unauthorized network connections and malicious traffic.
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	Yes	CSP-owned	Atrixware maintains company-managed endpoints with automatic operating system and security updates enabled to help ensure security patches are applied in a timely manner.
UEM-12.1	Are remote geo-location capabilities enabled for all managed mobile endpoints, in accordance with applicable laws and regulations?	Yes	CSP-owned	Atrixware manages endpoint security through established access and security practices.
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	NA	CSP-owned	Atrixware does not provide or manage mobile endpoint devices requiring remote company data deletion. Company data is managed through the Axis LMS application and hosted environment rather than on company-managed mobile devices.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.1.0				
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	Atrixware restricts and manages third-party access to organizational systems and data through authorization, access controls, and applicable security requirements.