CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)			CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Wolters Kluwer maintains a written global information security program of policies, procedures and controls aligned to NIST CSF, ISO27001, and other equivalent standards, governing the processing, storage, transmission and security of data (the "Security Program")				A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and	Audit and Assurance Policy and Procedures	Audit & Assurance
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.							
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes	3rd-party outsourced	Wolters Kluwer has established and maintains sufficient controls to meet certification and attestation requirements for the objectives stated in ISO27001 for the Security Program. At least once per calendar year, Wolters Kluwer obtains an assessment against the referred standards and audit methodologies by an independent third-party auditor.				A&A-02	Conduct independent audit and assurance assessments according to	Independent Assessments	
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes	Shared CSP and 3rd-party	Wolters Kluwer performs information security risk assessments as part of a risk governance program that is established with the objective to regularly assess and evaluate the effectiveness of the Security Program				A&A-03	Perform independent audit and assurance assessments according to	Risk Based Planning Assessment	
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Yes	Shared CSP and 3rd-party	Wolters Kluwer audit policies ensure compliance with all the applicable and relevant standards, regulations, statutory requirements and industry standards				A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory	Requirements Compliance	
A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence?	Yes	Shared CSP and 3rd-party	Risk assessments are designed to identify and assess potential risks impacting confidentiality, integrity, availability, and/or privacy of the information and data processed, stored or transmitted by the organization, resulting from any changes in the business or technology environments. The Wolters Kluwer Security Program is audited annually by an independent third-party.				A&A-05	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion,	Audit Management Process	
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and 3rd-party	Risk assessments findings mitigation plan is documented, communicated and approved by company management.				A&A-06	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation	Remediation	
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	Yes	CSP-owned	Wolters Kluwer internal auditing, control and risk management processes provide accurate visibility of remediation and risk across the organization.							
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities?	Yes	CSP-owned	Wolters Kluwer maintains a written global information security framework of policies, procedures and controls aligned to NIST CSF, ISO27001, and other equivalent standards, governing the processing, storage, transmission and security of data (the "Security Program")				AIS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's	Application and Interface Security Policy and Procedures	Application & Interface Security
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.							
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	No	CSP-owned	Baseline requirements to secure different applications are established but not documented.				AIS-02	Establish, document and maintain baseline requirements for securing	Application Security Baseline Requirements	
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes	CSP-owned	Wolters Kluwer impleented metrics that are functional to business objectives and security requirements. The software service is available 24X7 with the eception of ordinary and extraordinary maintenance activities, notified with 3 days of advanced notice. The Monitoring of the Production environment is active H24. The following SLAs are applied: - Infrastructure availability: 99,70% - Response time for incidents with severity "Emergency" and "Critical": by 120 minutes (from Monday to Friday, 9-18, excluding official holidays. Response time for all the other incidents: by 16 hours from Monday to Friday, 9-18, excluding official holidays. The metrics are checked regularly to identify issues and/or opportunities, in order to ensure continuous improvement in processes and services. In addition, we execute monthly reporting on the open bugs trends, on the type of requirements opened and developed, basing on the requirements classification.				AIS-03	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	Application Security Metrics	
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes	CSP-owned	the process is structured into several phases: - definition of specifications and design requirements; - software solution design; - threat modeling; - development; - code scanning (SAST/OSS); - testing; - release.				AIS-04	Define and implement a SDLC process for application design, development, deployment, and operation in	Secure Application Design and Development	

AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	No	CSP-owned	We are working on Test procedures on Atlantide product.	AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and	Automated Application Security Testing
AIS-05.2	Is testing automated when applicable and possible?	No	CSP-owned				
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes	CSP-owned	There are procedures that refer to standards that we use both for development, for releases, and for architectural changes in environments.	AIS-06	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Automated Secure Application Deployment
AIS-06.2	Is the deployment and integration of application code automated where possible?	No	CSP-owned	Research & Development team use automation processes like DevOps pipelines for checking code but not for building.			
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes	CSP-owned	The Wolters Kluwer vulnerability management program is focused on the collection, analysis, summarization, tracking and reporting of identifiable vulnerabilities in applications, infrastructure, endpoint systems and networks. This process is vital for providing accurate visibility of risk across the organization. Monthly vulnerability scans are conducted, and third-party penetration tests are performed annually, which follow the remediation schedule in accordance with established vulnerability management standards.	AIS-07	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.	Application Vulnerability Remediation
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	No	CSP-owned	Research & Development team use automatic systems for vulnerability evidence detection (Coverity for SAST / Black Duck for OSS) but the remedy is managed in a punctual and manual manner. It is not possible to automate completeley the process. Each single vulnerability is analyzed in its peculiarity, so as to identify if it is a false positive or real vulnerability to remediate.			
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Wolters Kluwer maintains business continuity plans ("BCP") which includes processes for protecting personnel and assets and restoring functionality in accordance with the time frames outlined therein. Such BCP is tested annually and updated based on any deficiencies identified during such tests.	BCR-01	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures.	Business Continuity Management Policy and Procedures
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.			
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	Wolters Kluwer maintains business continuity plans ("BCP") which include processes for protecting personnel and assets and restoring functionality in accordance with the time frames outlined therein. Such BCP is tested annually and updated based on any deficiencies identified during such tests.	BCR-02	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience	Risk Assessment and Impact Analysis
BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	Yes	CSP-owned	Wolters Kluwer (i) maintains an IT disaster recovery plan ("DR"); (ii) tests the DR plan at least once every year; (iii) makes available summary test results which will include the actual recovery point and recovery times; (iv) documents any action plans within the summary test results to promptly address and resolve any deficiencies, concerns, or issues that prevented or may prevent the services from being recovered in accordance with the DR plan.	BCR-03	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.	Business Continuity Strategy
BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	Yes	CSP-owned	Wolters Kluwer maintains business continuity plans ("BCP") which include processes for protecting personnel and assets and restoring functionality in accordance with the time frames outlined therein. Such BCP is tested annually and updated based on any deficiencies identified during such tests.	BCR-04	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the	Business Continuity Planning
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	Yes	CSP-owned	Wolters Kluwer ensures that: a) an adequate management structure is in place to be prepared, mitigate and respond to adverse events, using proper personnel with the necessary authority, experience and competence; b) specific personnel is appointed to respond to incidents, with the necessary competence, authority and resposibility to manage incidents and to keep information security; c) all the necessary documents are developed and approved, such as plans, reponse and restore procedures, detailing how the organization will manage an adverse event and how it will keep the information security at a predefined level, basing on approved business continuity and information securityobjectives. Basing on the security information continuity requirements, the organization estabilishes, documents, executes and maintains: a) controls of the information security within the processes, procedures and systems, as well as within the tools supporting the business continuity and/or the disaster recovery; b) processes, procedures and implementation changes to mantain the existing security controls even in the adverse situations; c) compensative controls to check information security for the security control which cannot be kept during an adverse situasion.	BCR-05	Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review periodically.	Documentation
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes	CSP-owned	Wolters Kluwer documents and maintains a company Business Continuituy Plan (BCP) applicable to all Divisions, Business Unit and Departmental/Funcional Areas. As a baseline, the BCP is reviewed annualy. Wolters Kluwer manages also the specific Atlantide Disaster Recovery program to guarantee the product service continuity and its target RPO and RTO. This plan is tested annualy.			
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Yes	CSP-owned	The Business Contintuity Plan is updated annually			

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	As described in BCR-02.1, BCP is tested annually and updated based on any deficiencies identified during such tests.	BCR-06	Exercise and test business continuity and operational resilience plans at least annually or upon significant	Business Continuity Exercises	Business Continuity Management and Operational Resilience
BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	Yes	CSP-owned	The Business Contintiuity Plan and Disaster Recovery Plan establish communication with all the relevant stakeholders, participants and critical roles involved in its execution	BCR-07	Establish communication with stakeholders and participants in the	Communication	
BCR-08.1	Is cloud data periodically backed up?	Yes	CSP-owned	Wolters Kluwer maintains a backup plan to ensure all critical data is backed up without affecting system operations. The type and frequency of backup and type of backup media used take into consideration the volume of data, criticality of data and recovery time constraints.	BCR-08	Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.	Backup	
BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	Yes	CSP-owned	Backup are executed in line with Wolter Kluwers internal policies on Backup and Disaster Recovery. In detail: a. Data on backup media are secured against unauthorized access. Backup media / data are encrypted b. Backup media are secured against environmental and physical threats. c. Backup media are securely disposed. Backup media are disposed when media life has expired or when media is damaged and data is not accessible. d. Following security measures are taken before disposing of the media or re-using the media: - Essential data are copied to another media. - All the data on the media are erased before disposing the media. e. Backups are stored at a geographically diverse location from the primary location of the data. The customers are informed on: - backup perimeter and calendar; - backup methods and data formats, including encryption; - backup storage timeframes and retention times; - backup data integrity check procedures; - backup procedures and restore time of data from backup;				
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	CSP-owned	According to Wolter Kluwers policies and process on Backup and Disaster Recovery: a. Testing is done periodically to ensure that data can be recovered from the backup media, and at a minimum on an annual basis. b. Application owner determines the frequency of recovery testing c. Recovery testing accurately captures relevant scenarios (e.g. natural disasters, cybersecurity events, other events that would trigger disaster recovery, etc.) to Wolters Kluwer environment. d. The integrity of backup media is tested on a periodic basis by performing a data restoration process to ensure that the backup is working properly. e. Key suppliers / third-party providers are included in recovery planning and				
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	Wolters Kluwer (i) maintains an IT disaster recovery plan (“DR”); (ii) tests the DR plan at least once every year; (iii) makes available summary test results which will include the actual recovery point and recovery times; and (iv) documents any action plans within the summary test results to promptly address and resolve any deficiencies, concerns, or issues that prevented or may prevent the services from being recovered in accordance with the DR plan.	BCR-09	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon	Disaster Response Plan	
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes	CSP-owned	The Disaster response plan is updated annually or at least if a significant changes occur.				
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes	CSP-owned	Wolters Kluwer (i) maintains an IT disaster recovery plan (“DR”); (ii) tests the DR plan at least once every year; (iii) makes available summary test results which include the actual recovery point and recovery times; (iv) documents any action plans within the summary test results to promptly address and resolve any deficiencies, concerns, or issues that prevented or may prevent the services from being recovered in accordance with the DR plan.	BCR-10	Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities.	Response Plan Exercise	
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	No	CSP-owned	There are no external third parties (local emergency authorities) involved in the DR exercise.				
BCR-11.1	Is business-critical equipment supplemented with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards?	Yes	CSP-owned	Technology Components underpinning the Application's infrastructure environment are duplicated at the DR Environment to meet the RTO & RPO.	BCR-11	Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in	Equipment Redundancy	
CCC-01.1	Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)?	Yes	CSP-owned	The organizational changes, business process changes and infrastructure and system changes which may affect the information security are controlled, and when the change may potentially impact features related to IT security, a risk analysis is performed and evaluated. In case of changes which impact the customers, a prompt information to the customer is guaranteed in accordance with contractual SLAs	CCC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration,	Change Management Policy and Procedures	
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council (“Security Council”), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.				
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	No	CSP-owned		CCC-02	Follow a defined quality change control, approval and testing process with established	Quality Testing	

CCC-03.1	Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?	Yes	CSP-owned	The organizational changes, business process changes and infrastructure and system changes which may affect the information security are controlled, and when the change may potentially impact features related to IT security, a risk analysis is performed and evaluated.		CCC-03	Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc.,	Change Management Technology	Change Control and Configuration Management
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes	CSP-owned	Asset management is performed in line with the related Wolters Kluwer Global Policy. In detail: a) Proper and regular maintenance is performed over time on all assets treated as critical for business, per local laws and client requirements b) Methods, tools, and personnel used to conduct maintenance and repair is defined, documented and managed c) Maintenance is done in accordance to an assets manufacturer and is performed by authorized and capable personal only. d) If such skills are not available in the organization, then designated service maintenance centers are consulted. e) Records of maintenance activities are maintained showing: i. when the service took place ii. what was done iii. any cost associated iv. by whom f) If any maintenance is performed by third parties or outside the organization, any confidential information is cleared or secured from the equipment. g) After maintenance is implemented, the equipment is tested for any tampering or malfunctioning before being put back into operation. h) Surplus equipment if any procured to support business continuity is managed securely while not in use, and disposed of or sanitized when no longer required, per Asset Disposal standard		CCC-04	Restrict the unauthorized addition, removal, update, and management of organization assets.	Unauthorized Change Protection	
CCC-05.1	Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs?	Yes	CSP-owned	In case of changes which impact the customers, a prompt information to the customer is guaranteed in accordance with contractual SLAs		CCC-05	Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level	Change Agreements	
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes	CSP-owned	Wolters Kluwer has a process in place to identify, document, evaluate, and approve all changes that could impact organizational assets.		CCC-06	Establish change management baselines for all relevant authorized	Change Management Baseline	
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Yes	CSP-owned	The Change Management process includes the process of documenting and approving deviations from standard baseline.		CCC-07	Implement detection measures with proactive notification in case	Detection of Baseline Deviation	
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes	CSP-owned	Wolters Kluwer follows an exception management process to manage situations not in line with the standard processes. This process requires: - involvement of all the interested stakeholder - definition of roles and responsibilities - exceptions identification, documentation and classification (basing on their severity) - exceptions evaluation (basing on their impact on the standard change and configuration process) - exception approval. Emergency changes policies are defined in Change Management Policy and Procedures.		CCC-08	'Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.'	Exception Management	
CCC-08.2	'Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?'	Yes	CSP-owned	Wolters Kluwer follows an exception management process to manage situations not in line with the standard processes. This process requires: - involvement of all the interested stakeholder - definition of roles and responsibilities - exceptions identification, documentation and classification (basing on their severity) - exceptions evaluation (basing on their impact on the standard change and configuration process) - exception approval.					
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	In case of unsuccessful changes, roll-back and recovery procedures defined in the change planning phase are followed.		CCC-09	Define and implement a process to proactively roll back changes to a previous known good state in case of errors	Change Restoration	
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and 3rd-party	Wolter Kluwer uses industry standard encryption to encrypt data in transit over public networks to the Wolters Kluwer environment and data at rest for systems, applications and services that involve or impact sensitive data.	On specific request of the Customer, Wolters Kluwer installs the keys generated and supplied by the customer. Customer key management is performed on the basis of rules and procedures that can be specifically defined in the contract. The use of keys provided by the Customer is foreseen after the implementation of a specific configuration to be defined at design level.	CEK-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies	Encryption and Key Management Policy and Procedures	
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and 3rd-party	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.					
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes	Shared CSP and 3rd-party	Wolter Kluwer uses industry standard encryption to encrypt data in transit over public networks to the Wolters Kluwer environment and data at rest for systems, applications and services that involve or impact sensitive data. On specific customer request, WK installs the keys generated and provided by the customer. Customer key management is performed on the basis of rules and procedures that can be specifically defined in the contract. The use of keys supplied by the customer is envisaged, after the implementation of a specific configuration to be defined at design level.	On specific customer request, WK installs the keys generated and provided by the customer. Customer key management is performed on the basis of rules and procedures that can be specifically defined in the contract. The use of keys supplied by the customer is envisaged, after the implementation of a specific configuration to be defined at design level.	CEK-02	Define and implement cryptographic, encryption and key management roles and responsibilities.	CEK Roles and Responsibilities	
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes	CSP-owned	Wolter Kluwer uses industry standard encryption to encrypt data in transit over public networks to the Wolters Kluwer environment and data at rest for systems, applications and services that involve or impact sensitive data.		CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic	Data Encryption	

CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Yes	CSP-owned	Encryption keys are created and protected with at least the same level of security and access control as the data being protected. The encryption strength is based on industry standards for strong encryption and does commensurate with the data classification.	CEK-04	Use encryption algorithms that are appropriate for data protection, considering the	Encryption Algorithm	Cryptography, Encryption & Key Management
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	Shared CSP and 3rd-party	The Wolters Kluwer Change Management procedure ensures that changes are fully and thoroughly tested before implementation.	CEK-05	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval,	Encryption Change Management	
CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	Yes	CSP-owned	Wolters Kluwer has defined a procedure for the management of cryptography and key management systems. The procedure considers aspects of configuration and implementation, analysis of risk aspects to costs and benefits.	CEK-06	Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully	Encryption Change Cost Benefit Analysis	
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	No	CSP-owned	The risk assessment process is active and reviewed annualy. This does not include risk assessment related to encryption.	CEK-07	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment,	Encryption Risk Management	
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	NA			CEK-08	CSPs must provide the capability for CSCs to manage their own data encryption keys.	CSC Key Management Capability	
CEK-09.1	Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event?	No	Shared CSP and 3rd-party	The risk assessment process is active reviewed and audited at least annualy.	CEK-09	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously	Encryption and Key Management Audit	
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Yes	Shared CSP and 3rd-party	At least once per calendar year, Wolters Kluwer obtains an assessment against the referred standards and audit methodologies by an independent third-party auditor. For select systems, applications and services, Wolters Kluwer annually receives third party audits for compliance with SOC 2 Type 2				
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	Wolters Kluwer uses industry standard encryption to encrypt data in transit over public networks to the Wolters Kluwer environment and data at rest for systems, applications and services that involve or impact sensitive data.	CEK-10	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the	Key Generation	
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes	Shared CSP and 3rd-party	Encryption keys are created and protected with at least the same level of security and access control as the data being protected. The encryption strength is based on industry standards for strong encryption and does commensurate with the data classification.	CEK-11	Manage cryptographic secret and private keys that are provisioned for a unique purpose.	Key Purpose	
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Yes	Shared CSP and 3rd-party	The following rules are applied: i. Rotate, Retire or Replace keys that have reached the end of their usefulness or “when the integrity of the key has been weakened,” including after termination of an employee “with knowledge of a clear-text key component” or upon suspicion that the key has been compromised. ii. Retired keys are not reused or reissued except for recovery purposes. iii. Data encryption keys are retired within a retirement period depending on hey type iv. Encryption keys related to sensitive data may be rotated in two ways: Encryption and Encryption Key Management • Regular rotation: regularly rotate the encryption key used, limiting the amount of data protected by a single key. Rotate keys once in 30 or 90 days based on the data associated. • Irregular rotation: ad-hoc rotation after a suspected incident, Data encrypted with the previous version of the key may also need to be re-encrypted.	CEK-12	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.	Key Rotation	
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	Keys are revoke in the way described below. i. Rotate, Retire or Replace keys that have reached the end of their usefulness or “when the integrity of the key has been weakened,” including after termination of an employee “with knowledge of a clear-text key component” or upon suspicion that the key has been compromised. ii. Retired keys are not reused or reissued except for recovery purposes. iii. Data encryption keys retirement period is based on key type (e.g. Master Key/Rppt Key, One Time Disposable, Partner Communication, Internal Use - Certificates, Customer Use - Certificate, Internal Use - Algorithm/Hash, Customer Use, Algorithm/Hash). iv. Encryption keys related to sensitive data may be rotated in two ways: • Regular rotation: regularly rotate the encryption key used, limiting the amount of data protected by a single key. Rotate keys once in 30 or 90 days based on the data associated. • Irregular rotation: ad-hoc rotation after a suspected incident, Data encrypted with the previous version of the key may also need to be re-encrypted.	CEK-13	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer	Key Revocation	

CEK-14.1	Are processes, procedures and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	The key are rotated and retired in compliance with the requirement.	CEK-14	Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys	Key Destruction
CEK-15.1	Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	Atlantide uses the Azure Transparent Data Encryption (TDE). The key generation process is owned by the Azure Third Party Cloud Provider.	CEK-15	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have	Key Activation
CEK-16.1	Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	The key management ensures the following elements of an encryption key lifecycle are performed securely: A. Key Generation B. Key Distribution C. Key Usage D. Key Storage E. Key Recovery F. Key Rotation and Retirement (Rollover, Update, and Renewal) This process is used when creating, storing, and retiring encryption keys for all WK resources.	CEK-16	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from	Key Suspension
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	The Key Rotation and Retirement is performed in compliance with the requirement	CEK-17	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their	Key Deactivation
CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	Cryptographic keys are be stored in the fewest possible locations The master key and/or root key are contained in an encrypted container that is access controlled. Keys may be split into multiple parts for storage purposes as required by a contract or where feasible. Access to these containers is held by authorized individuals with segregation of duties. Keys are protected on both volatile and persistent memory. Keys are never be stored in plaintext. Where applicable, encrypt the keys using Key Encryption Keys (KEKs) before exporting the key material. KEK length (and algorithm) should be equivalent to or greater in strength than the keys being protected. It is ensured that keys have integrity protections applied while in storage. It is ensured that standard application-level code never reads or uses cryptographic keys in any way and use key management libraries. It is ensured that keys and cryptographic operations are done inside the sealed vault. All work is done in the vault (such as key access, encryption, decryption, signing, etc.).	CEK-18	Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.	Key Archival
CEK-19.1	Are processes, procedures, and technical measures to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	Use of cryptographic modules, algorithms, primitives, keys, applications, and any associated artifacts is limited only to those that have proven resilient against known attacks and are of sufficient strength to protect assets. The use is limited to components that have received a public review, that have withstood public and open examination, and that have been vetted by personnel and deemed reliable and robust. Any applicable governing regulation, contractual requirement, or other standards is followed with respect to cryptography, It is ensured that the use of cryptography is appropriate and legal	CEK-19	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance,	Key Compromise
CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	Shared CSP and 3rd-party	The risk assessment process is active and reviewed annualy. The risk assessment related to encryption is currently ongoing as we are implementing encryption as evolution of the product.	CEK-20	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the	Key Recovery
CEK-21.1	Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions?	Yes	Shared CSP and 3rd-party	Processes are in place to identify and classify the data that will be encrypted, technical measures are implemented to protect the appropriate data based on its classification, and regular testing and reviews are conducted to validate the effectiveness of the implemented security controls (Audit/ISO).	CEK-21	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and	Key Inventory Management
DCS-01.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	Yes	CSP-owned	Wolters Kluwer maintains procedures ensuring secure disposal of information. Secure disposal of data requires, at minimum, secure erasure of media and secure disposal of records so that the information cannot be read or reconstructed.	DCS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data	Off-Site Equipment Disposal Policy and Procedures
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Yes	Shared CSP and 3rd-party	Our secure disposal of data requires, at minimum, secure erasure of media and secure disposal of records so that the information cannot be read or reconstructed.			

DCS-01.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually?	Yes	Shared CSP and 3rd-party	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.		destruction procedure that renders recovery of information impossible must be applied. Review and		Datacenter Security
DCS-02.1	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	Yes	CSP-owned	Wolters Kluwer defined policy processes and procedure for transfer systems, software and data.	DCS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the	Off-Site Transfer Authorization Policy and Procedures	
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	Yes	CSP-owned	Transfer or data relocation is protect by encription in transit and at rest.				
DCS-02.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.				
DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	Yes	CSP-owned	Offices and data center facilities that are owned or leased by Wolters Kluwer include physical access restrictions and fire detection and fire suppression systems both localized and throughout the building. The implemented controls are commensurate with the risk exposure of each facility. Controls include access by authorized personnel only, visitor access controls, secure areas which are physically separated from other workspaces, and systems, machines and devicesincluding physical protection mechanisms and entry controls to limit physical access.	DCS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and	Secure Area Policy and Procedures	
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.				
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	Yes	CSP-owned	Wolters Kluwer has defined policy processes and procedure for transfer systems, software and data.	DCS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least	Secure Media Transportation Policy and Procedures	
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.				
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Yes	Shared CSP and 3rd-party	Wolters Kluwer maintains an inventory of its assets used within Wolters Kluwer and by any third parties authorized to act on its behalf, and an inventory of all media and equipment where data is stored. An asset is anything that has value to Wolters Kluwer, which includes hardware, software, information, infrastructure, outsourced services and even resources with specific skills and knowledge ("Asset").	DCS-05	Classify and document the physical, and logical assets (e.g., applications) based on the	Assets Classification	
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Yes	Shared CSP and 3rd-party	Wolters Kluwer maintains an inventory of its assets used within Wolters Kluwer and by any third parties authorized to act on its behalf, and an inventory of all media and equipment where data is stored. An asset is anything that has value to Wolters Kluwer, which includes hardware, software, information, infrastructure, outsourced services and even resources with specific skills and knowledge ("Asset").	DCS-06	Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured	Assets Cataloguing and Tracking	
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	Yes	Shared CSP and 3rd-party	Offices and data center facilities that are owned or leased by Wolters Kluwer include physical access restrictions and fire detection and fire suppression systems both localized and throughout the building. The implemented controls are commensurate with the risk exposure of each facility. Controls include access by authorized personnel only, visitor access controls, secure areas which are physically separated from other workspaces, and systems, machines and devicesincluding physical protection mechanisms and entry controls to limit physical access	DCS-07	Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities	Controlled Access Points	
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	Yes	CSP-owned	Offices and data center facilities that are owned or leased by Wolters Kluwer include physical access restrictions and fire detection and fire suppression systems both localized and throughout the building. The implemented controls are commensurate with the risk exposure of each facility. Controls include access by authorized personnel only, visitor access controls, secure areas which are physically separated from other workspaces, and systems, machines and devicesincluding physical protection mechanisms and entry controls to limit physical access				
DCS-08.1	Is equipment identification used as a method for connection authentication?	No	CSP-owned	Access to Assets by Wolters Kluwer employees and contractors is protected by authentication, authorization, and identity management mechanisms. User authentication is required to gain access to production and development environments. Individuals are assigned a unique user account. Sharing of individual user accounts is prohibited. Access privileges are based on job requirements using the principle of least privilege, are modified upon any applicable changes in job requirements, and are revoked upon termination of employment or contract. Infrastructure access is established using appropriate user account and authentication controls, which include the required use of VPN connections, complex passwords, enabling of account lock-out, and a multi factor authenticated connection.	DCS-08	Use equipment identification as a method for connection authentication.	Equipment Identification	

DCS-09.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	Yes	Shared CSP and 3rd-party	Facility security prevents unauthorized physical access or damage to Wolters Kluwer's premises, Wolters Kluwer's information and systems, and provides for a safe working environment for all Wolters Kluwer employees. Physical access to the facility are controlled by access controls at all entry and exit points to limit access to the facility, Verifying access authorizations before granting access to the facility, Visitors should be escorted and their activity once inside the facility be monitored, Logs of entry to the facility for all employees, visitors, service engineers and vendors are maintained for a period of 90 days, at a minimum, all Wolters Kluwer Non-Data Center Facilities will have alarm systems in place to notify professional security personnel and/or local law enforcement in the event of a security incident.	
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Yes	CSP-owned	Logs of entry to the facility for all employees, visitors, service engineers and vendors are maintained for a period of 90 days, at a minimum.	
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Yes	Shared CSP and 3rd-party	Security guards are in place at all data center facilities to control access and authorization to the facility. The security guards should patrol the facility in addition to monitoring access points and Closed Circuit Television (CCTV) systems, The hosted infrastructure and networks should be maintained within a third party hosting provider's datacenter that is SAS 70 Type II audited, all Wolters Kluwer Non-Data Center Facilities will have alarm systems in place to notify professional security personnel and/or local law enforcement in the event of a securitv incident.	
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	Yes	Shared CSP and 3rd-party	Security personnel are trained to follow and strictly enforce physical security policies for the facility.	
DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	Yes	Shared CSP and 3rd-party	The various electrical and communication systems are created in order to prevent tampering and unauthorized intervention, together with the prevention of wiretapping on communication structures.	
DCS-13.1	Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?	Yes	Shared CSP and 3rd-party	In order to maintain a safe, secure and fully available and operational facility the Data Center standards and policies are maintain for meeting local, regional and international standards, as well as local regulation and laws or legal requirements the following areas: Facility Infrastructure, Environmental Controls, Fire Prevention/Protection such as Fire extinguishers and detectors, Emergency Lighting, Temperature and Humidity Controls, Disaster Recover, Offsite Backup, Redundant Power.	
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	Yes	Shared CSP and 3rd-party	The 3-rd party managing the Data Center follows independent frameworks for the documentation and management of cloud risks according to standards. Examples are ISO 27001 standard for information security, CIS Benchmark e NIST SP 800-53	
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	Yes	CSP-owned	Offices and data center facilities that are owned or leased by Wolters Kluwer include physical access restrictions and fire detection and fire suppression systems both localized and throughout the building. The implemented controls are commensurate with the risk exposure of each facility. Controls include access by authorized personnel only, visitor access controls, secure areas which are physically separated from other workspaces, and systems, machines and devices including physical protection mechanisms and entry controls to limit physical access.	
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	Yes	CSP-owned	Wolters Kluwer defined processes and procedures for management of data and for their entire life cycle in accordance with national laws, regulations (GDPR) and ISO standards (ISO27001, ISO27017, ISO27018).	
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and 3rd-party	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer business divisions and corporate functions.	
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Yes	Shared CSP and 3rd-party	Wolters Kluwer has established process and procedures for provide data removal and verification in compliance with NIST 800-88 Revision 1. This can be accomplished off-site by a third party.	
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Yes	Shared CSP and CSC	Wolters Kluwer stores and maintans data for all kind of data classification.	The classification of the customer data is charge of Customer.
DSP-04.1	Is data classified according to type and sensitivity levels?	Yes	Shared CSP and CSC	Wolters Kluwer classify data, according to its own defined standards and the type of information that the application is expected to process, from CSC prospective in accordance with the purpose for which Application was built.	The classification of the customer data is charge of Customer.
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Yes	CSP-owned	Documents describing the solution architecture and data flow are present and update. These documents containded the resources where data and documents are stored. The data is also classified according to the level of confidentiality as required by the ISO 27001 certification.	
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Yes	CSP-owned	As per ISO/IEC 27001, 27017 and 27018 certification, documents are reviewed and updated at least once a year	

DCS-09	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate	Secure Area Authorization
DCS-10	Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress	Surveillance System
DCS-11	Train datacenter personnel to respond to unauthorized ingress or	Unauthorized Access Response Training
DCS-12	Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication	Cabling Security
DCS-13	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the	Environmental Systems
DCS-14	Secure, monitor, maintain, and test utilities services for continual	Secure Utilities
DCS-15	Keep business-critical equipment away from locations subject to high probability for environmental risk	Equipment Location
DSP-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations,	Security and Privacy Policy and Procedures
DSP-02	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable	Secure Disposal
DSP-03	Create and maintain a data inventory, at least for any sensitive data and personal data.	Data Inventory
DSP-04	Classify data according to its type and sensitivity level.	Data Classification
DSP-05	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals,	Data Flow Documentation

DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Yes	Shared CSP and CSC	Wolters Kluwer data processing agreement (attached to the Customer agreement contract) defines obligations relating to the ownership of personal data.	The classification of the customer data is charge of Customer.	DSP-06	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.	Data Ownership and Stewardship	Data Security and Privacy Lifecycle Management
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	Yes	CSP-owned	Legal Department reviews Terms & Conditions and all contractual standards and templates at least annually					
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Yes	CSP-owned	Principles of security by design and best practices are adopted.		DSP-07	Develop systems, products, and business practices based upon a principle	Data Protection by Design and Default	
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Yes	CSP-owned	Principles of security by design and best practices are adopted in accordance with the GDPR.		DSP-08	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured	Data Privacy by Design and Default	
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	Yes	Shared CSP and CSC	The application allows the configuration and profiling of security measures that must be put in place according to all applicable laws and regulations	The application allows the configuration and profiling of security measures that must be put in place or requested by the customer at startup.				
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	TEAM Privacy - verificare e confermare: The DPIA (Data Protection Impact Assessment) is performed using the online Verifield (PrivacyEye) platform and this process has obtained the positive advisory opinion of the DPO (Data Protection Officer). We are planning the replacement of this platform with OneTrust in the following months		DSP-09	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks	Data Protection Impact Assessment	
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	Yes	CSP-owned	Wolters Kluwer puts in place all the necessary procedures for secure data transfer: - before starting the treatment, the customer deposits the source data on his own secure areas from which WK downloads the data using the credentials provided by the customer - during the entire period of data processing, all internal and external connections are in https and calls to services require an authorization token - at the end of the life cycle, data delivery takes place via a secure channel. The proprietary application WKFS (WK File Sharing) is usually used, which is GDPR compliant. In all the stages described, the data is processed and transferred by personnel appointed as system administrators.		DSP-10	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized	Sensitive Data Transfer	
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	Yes	CSC-owned		The application allows the Customer to process data in accordance with the regulations and the requests of its customer's interested parties.	DSP-11	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or	Personal Data Access, Reversal, Rectification and Deletion	
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	Shared CSP and CSC	Personal data is processed and treated according to current regulations.	The application allows the Customer to process data in accordance with the regulations.	DSP-12	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to	Limitation of Purpose in Personal Data Processing	
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	Yes	Shared CSP and 3rd-party	Wolters Kluwer has in place a supplier qualification process and contractual agreements with 3rd parties about compliance with Wolters Kluwer's security standard.		DSP-13	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal	Personal Data Sub-processing	
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	Yes	CSP-owned	Names of all sub-processors are indicated in contracts with customers. Wolters Kluwer asks each sub-processors to sign a document where they are appointed as sub-responsible of data processing.		DSP-14	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive	Disclosure of Data Sub-processors	
DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	Yes	Shared CSP and CSC	Wolters Kluwer policy do not permit use or reproduction customer data in environments other than production environments. Specific cases are allowed only after getting Customer's authorization.		DSP-15	Obtain authorization from data owners, and manage associated risk before replicating or using production data	Limitation of Production Data Use	
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes	CSP-owned	Information on data retention is given in the Contract in the attachment "SLA Document" to the contract.		DSP-16	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	Data Retention and Deletion	
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Yes	CSP-owned	Wolters Kluwer defined processes and procedures for management of data and for their entire life cycle in accordance with national laws, regulations (GDPR) and ISO standards (ISO27001, ISO27017, ISO27018).		DSP-17	Define and implement, processes, procedures and technical measures to protect sensitive	Sensitive Data Protection	

DSP-18.1	Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations?	No	CSP-owned	No procedure is in place; mandatory criminal law provides that CSP needs to answers within the given term and Corporate Legal Department is in charge for this.	DSP-18	The CSP must have in place, and describe to CSCs the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations. The CSP must give special attention to the notification procedure	Disclosure Notification	
DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?	No	CSP-owned	Notification to CSCs is forbidden by criminal law in case of investigation from authorities; in case of inquiries coming from privates, CSP needs the authorization from CSC as per contractual obligation.				
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	Yes	CSP-owned	The data is located in two Azure data centers of the European community (North and West Europe). The North Europe data center serves as a Disaster Recovery Zone. Backup copies are managed by and in the Azure cloud.	DSP-19	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data,	Data Location	
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	Wolters Kluwer has implemented a three-tiered information security management structure to facilitate the management, architecture, and operations of security functions. The Security Council oversees the management of this structure. Members of the Security Council include leadership representatives including commercial division CTOs, Legal, Internal Audit, Internal Controls, the Global Information Security team, and Risk Management. Wolters Kluwer has a Chief Information Security Officer who is responsible for oversight, management, and monitoring of Wolters Kluwer's Security Program.	GRC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the	Governance Program Policy and Procedures	Governance, Risk and Compliance
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.				
GRC-02.1	Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?	Yes	CSP-owned	Wolters Kluwer performs information security risk assessments as part of a risk governance program that is established with the objective to regularly assess and evaluate the effectiveness of the Security Program. Such assessments are designed to identify and assess potential risks impacting confidentiality, integrity, availability, and/or privacy of the information and data processed, stored or transmitted by the organization, resulting from any changes in the business or technology environments.	GRC-02	Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for	Risk Management Program	
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.	GRC-03	Review all relevant organizational policies and associated procedures at least annually or	Organizational Policy Reviews	
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Yes	CSP-owned	Wolters Kluwer has stablised an Exception Management process that allows the IT Security Governance and IT Risk Management function, to assess the risk associated with each exception request and allow management to consider the impact on the business, the cost of correction, and the residual risk of the exception when making the final decision on whether to accept or deny a request.	GRC-04	Establish and follow an approved exception process as mandated by the governance program whenever a	Policy Exception Process	
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Yes	CSP-owned	Wolters Kluwer maintains a written global information security program of policies, procedures and controls aligned to NIST CSF, ISO27001, and other equivalent standards, governing the processing, storage, transmission and security of data (the "Security Program"). The Security Program mandates industry-standard practices designed to protect data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to data transmitted, stored or otherwise processed.	GRC-05	Develop and implement an Information Security Program, which includes programs for all the	Information Security Program	
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes	CSP-owned	Wolters Kluwer has implemented a three-tiered information security management structure to facilitate the management, architecture, and operations of security functions. The Security Council oversees the management of this structure. Members of the Security Council include leadership representatives including commercial division CTOs, Legal, Internal Audit, Internal Controls, the Global Information Security team, and Risk Management. Wolters Kluwer has a Chief Information Security Officer who is responsible for oversight, management, and monitoring of Wolters Kluwer's Security Program.	GRC-06	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving	Governance Responsibility Model	
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Yes	CSP-owned	The Legal Department annually identifies regulations that have come into force that affect the company's object or activity; in any case, this is also done on a permanent basis at the instigation of the DPO, the Privacy Team, Group Compliance and Internal Control	GRC-07	Identify and document all relevant standards, regulations, legal/contractual, and statutory	Information System Regulatory Mapping	
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	Yes	Shared CSP and 3rd-party	Wolters Kluwer has established and actively maintains contacts with associations, organizations and companies in the area of Cloud management and for the provision of security and IT services.	GRC-08	Establish and maintain contact with cloud-related special interest groups and other	Special Interest Groups	
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	Shared CSP and 3rd-party	Wolters Kluwer defined processes and procedures for background verification of all new employees, contractors, and third parties, in accordance with national laws, regulations (GDPR) and ISO standards (ISO27001, ISO27017, ISO27018).		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new		

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	Wolters Kluwer performs background screening on new employees and all contractors who have access to Wolters Kluwer information and customers' information, subject to applicable laws and regulations.	HRS-01	employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements,	Background Screening Policy and Procedures	Human Resources
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.				
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	Users who are given access to Assets must abide by the Wolters Kluwer Acceptable Use Policy.	HRS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least	Acceptable Use of Technology Policy and Procedures	
HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.				
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	Policies and procedures specify and document how confidential data should be protected when unattended. Policies and procedures are communicated to all employees who need to know how to protect confidential data. Employees are trained at least annually on how to apply the policies and procedures.	HRS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the	Clean Desk Policy and Procedures	
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.				
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	Users who have access to Wolters Kluwer's proprietary data or who have access to Wolters Kluwer's network, store and or process Wolters Kluwer's information, or any system where Wolters Kluwer's customer data is stored or processed, must adhere to Wolters Kluwer's Acceptable Use Policy.	HRS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and	Remote and Home Working Policy and Procedures	
HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.				
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	CSP-owned	Wolters Kluwer adopt disposal and return procedures to ensures that access to company data will be revoked immediately upon termination or when access is no longer needed.	HRS-05	Establish and document procedures for the return of organization-owned	Asset returns	
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Yes	CSP-owned	Wolters Kluwer adopts a Global Career Framework and other procedures to document and communicate organizational change roles and responsibilities to all staff.	HRS-06	Establish, document, and communicate to all personnel the procedures outlining the roles and	Employment Termination	
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Yes	CSP-owned	These kinds of agreements are provided for and signed in the employment contract with the employee.	HRS-07	Employees sign the employee agreement prior to being granted access to organizational	Employment Agreement Process	
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes	CSP-owned	Users who have access to Wolters Kluwer's proprietary data or who have access to Wolters Kluwer's network, store and or process Wolters Kluwer's information, or any system where Wolters Kluwer's customer data is stored or processed, must adhere to Wolters Kluwer's Acceptable Use Policy.	HRS-08	The organization includes within the employment agreements provisions and/or terms for	Employment Agreement Content	
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Yes	CSP-owned	Roles are are communicated and documented	HRS-09	Document and communicate roles and responsibilities of employees,	Personnel Roles and Responsibilities	
HRS-10.1	Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?	Yes	CSP-owned	Non Disclosure Agreements are defined to reflect the requirements for confidentiality. NDAs are periodically reviewed	HRS-10	Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting	Non-Disclosure Agreements	

HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Yes	Shared CSP and 3rd-party	Wolters Kluwer maintains a security and privacy awareness program that includes both regularly scheduled and unannounced training and education of its personnel, including any contractors or other third parties working on its behalf with access to data or Assets.		HRS-11	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular	Security Awareness Training
HRS-11.2	Are regular security awareness training updates provided?	Yes	CSP-owned	Wolters Kluwer maintains a security and privacy awareness program. This training is conducted at time of hire and at least annually.				
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	CSP-owned	Wolters Kluwer offers role-based security training for critical roles such as application developers to enhance security awareness throughout the organization.		HRS-12	Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional	Personal and Sensitive Data Awareness and Training
HRS-12.2	Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	Yes	CSP-owned	Tabletop exercises are scheduled on at least an annual basis for all commercial divisions and involve a cross-functional team from across the organization.				
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	All Wolters Kluwer employees are required to complete basic periodic training, relating to their roles, on security. Wolters Kluwer maintains a security and privacy awareness program that includes both regularly scheduled and unannounced training and education of its personnel, including any contractors or other third parties working on its behalf with access to data or Assets. Such training is conducted at time of hire and at least annually. In addition, Wolters Kluwer offers role-based security training for critical roles such as application developers to enhance security awareness throughout the organization. Tabletop exercises are scheduled on at least an annual basis for all commercial divisions and involve a cross-functional team from across the organization.		HRS-13	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and	Compliance User Responsibility
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	Wolters Kluwer has defined processes and procedures for managing access and identities. Access to Assets by Wolters Kluwer employees and contractors is protected by authentication, authorization, and identity management mechanisms. User authentication is required to gain access to production and development environments. Individuals are assigned a unique user account. Sharing of individual user accounts is prohibited. Access privileges are based on job requirements using the principle of least privilege, are modified upon any applicable changes in job requirements, and are revoked upon termination of employment or contract. Infrastructure access is established using appropriate user account and authentication controls, which include the required use of VPN connections, complex passwords, enabling of account lock-out, and a multifactor authenticated connection.		IAM-01	Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually.	Identity and Access Management Policy and Procedures
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.				
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	Wolters Kluwer sets a standard that includes any password for any account (or any form of login that supports or requires a password) on any system owned or hosted by Wolters Kluwer, hosted on Wolters Kluwer's behalf by a Cloud provider, that has access to the Wolters Kluwer network, which stores and or processes any Wolters Kluwer information, or any system in which Wolters Kluwer customer data is stored or processed. Some applications (internal or customer facing) may be subject to additional specific regulations, such as HIPAA, PCI DSS, FedRAMP, etc. which may impose safety requirements other than those set out in the standard. Indicate any stricter controls than those listed in the standard. The management of application user passwords follows the rules established by the OWASP 4.0 standard - Authentication Verification Requirements	Application provided to the customer with a standard configuration setting, which privileged customer account can modify according to their needs.	IAM-02	Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.	Strong Password Policy and Procedures
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.				
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes	CSP-owned	Wolters Kluwer system identity information and access levels are typically managed, stored, and reviewed through the use of identity and access management (IAM) systems. These systems allow administrators to control and monitor user access to resources within an organization. IAM systems often include features such as password management, role-based access controls, and auditing to ensure that access is properly managed and monitored.		IAM-03	Manage, store, and review the information of system identities, and level of access.	Identity Inventory
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes	Shared CSP and 3rd-party	Wolters Kluwer implements and maintains a formal separation of duties, including those managed by third-parties or otherwise outsourced, System's access is based on separation of duties and least privilege principle.		IAM-04	Employ the separation of duties principle when implementing information	Separation of Duties
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes	Shared CSP and 3rd-party	Wolters Kluwer implements and maintains a formal separation of duties, including those managed by third-parties or otherwise outsourced, System's access is based on separation of duties and least privilege principle.		IAM-05	Employ the least privilege principle when implementing information	Least Privilege
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes	CSP-owned	Wolters Kluwer has a process in place for managing and defining access to its assets systems. Access privileges are based on job requirements using the principle of least privilege, are modified upon any applicable changes in job requirements, and are revoked upon termination of employment or contract.		IAM-06	Define and implement a user access provisioning process which authorizes, records, and	User Access Provisioning
IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	Yes	CSP-owned	Wolters Kluwer has a process in place for managing and defining access to its assets systems. Access privileges are based on job requirements using the principle of least privilege, are modified upon any applicable changes in job requirements, and are revoked upon termination of employment or contract.		IAM-07	De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in	User Access Changes and Revocation

IAM-08.1	Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?	Yes	CSP-owned	Periodically checks are performed, at least annually, and in any case of changes in role assignment of each individual user.		IAM-08	Review and revalidate user access for least privilege and separation of duties with a frequency that is	User Access Review	Identity & Access Management
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	Yes	Shared CSP and CSC	Wolters Kluwer defined a specific process for managing Privileged access by System Administrators	The application allows costomer to profile data access privileges based on the roles of individual end users and end user groups.	IAM-09	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative	Segregation of Privileged Access Roles	
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Yes	CSP-owned	Wolters Kluwer allow Elevation and Just-In-Time (JIT) practices if supported by the systems. The assignment and termination of a privilege right occurs through an ad hoc process or with the employee's change of role or resignation. All privileges are checked periodically (several times during the year) and disabled if inactive or not used for a defined period of time.		IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the	Management of Privileged Access Roles	
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	Yes	CSP-owned	Wolters Kluwer has a process in place for managing and defining access to its assets systems. Access privileges are based on job requirements using the principle of least privilege, are modified upon any applicable changes in job requirements, and are revoked upon termination of employment or contract.					
IAM-11.1	Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?	Yes	Shared CSP and CSC	Procedures to allow administrator-level customers to define access permissions for standard users are defined, implemented and tested. All activities of this kind are properly logged.	The Customers are in charge of managing standard and privileged user's only at application level.	IAM-11	Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for	CSCs Approval for Agreed Privileged Access Roles	
IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated?	Yes	CSP-owned	Logs generated by the systems, e.g. log of events, user activities, exceptions, errors, falures and security related events are captured, mainained and reviewed periodically, The logs are controlled, they are not changeable and not deleteable. Key roles (security event analyst, system owners, division/BU, information security policy & standard taskforce (SPST), security concil, leadership council) and related reponsibilities of each individual participating in Security Logging and Monitoring are defined.		IAM-12	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it	Safeguard Logs Integrity	
IAM-12.2	Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?	Yes	CSP-owned	The log integrity policy is compliant with the requirement. In detail, logs are protected from breaches of their confidentiality and itegrity ensuring proper integrity controls (e.g. logginf factilities and information protection against tampering, modification, desctruction and unaithorized access, Systems Administrators do not have permission to erase, deactivate or modify logs of their own activvities)					
IAM-13.1	Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?	Yes	CSP-owned	Wolters Kluwer has a process in place for managing user account naming convention and provides a single name that can use for identification within and across various systems. User Identities should not be reused, each username must be historically unique.		IAM-13	Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable	Uniquely Identifiable Users	
IAM-14.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?	Yes	Shared CSP and CSC	Wolters Kluwer has defined processes and procedures to allows access to privileged users in MFA (Multifactor Authentication).	The application is built to use (base on customer request) authentication with Multifactor or third-party authentication system.	IAM-14	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive	Strong Authentication	
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Yes	CSP-owned	It is possible to configure access through MFA or 3° party authentication provider.					
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Yes	CSP-owned	Password complexity meets the OWASP 4.0 standard. Specific and detailed technical measures for password management are defined and followed for secure password management		IAM-15	Define, implement and evaluate processes, procedures and technical measures for the	Passwords Management	
IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Yes	CSP-owned	Each access to data from the application and from the infrastructure is subject to checks by the application itself on the user's access authorizations. Any unauthorized access is not permitted.		IAM-16	Define, implement and evaluate processes, procedures and technical measures to verify	Authorization Mechanisms	
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	Yes	CSP-owned	This control is being integrated into the Software Development Lifecycle (SDLC) process.			Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces		
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Yes	CSP-owned	For the development of Atlandite the interoperability with external systems is usually implemented through the standard foreseen in the company policies (use of REST API or webservices for data transfer and use of strong standard protocols for authentication and autorization). We have procedures and policies to document this type of interoperability.					

IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	Yes	CSP-owned	The delivery model is not linked to the platform. Atlantide is a web application platform indipendent.	IPY-01	b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually.	Interoperability and Portability Policy and Procedures	Interoperability & Portability
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	Yes	CSP-owned	The data is kept encrypted, data modifications are governed by permissions granted to specific users and user groups, portability is managed according to precise procedures, integrity is guaranteed by development standards and access policies for such data. Also adopt the backup procedures according to the contractually regulated SLA.				
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	The Application Security Taskforce periodically (i.e., at least once a year), reviews the guidance developed by the teams, and consider them for publication in Wolters Kluwer company-wide guidelines.				
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes	CSP-owned	The application has application interfaces (REST APIs) that can be invoked programmatically after passing an authentication.	IPY-02	Provide application interface(s) to CSCs so that they programmatically	Application Interface Availability	
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	Yes	CSP-owned	The application data are managed with secure protocols, communications take place in https.	IPY-03	Implement cryptographically secure and standardized network	Secure Interoperability and Portability Management	
IPY-04.1	Do agreements include provisions specifying CSC data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Yes	CSP-owned	Customer data will be returned in BK DB SQL SERVER format files, and the documents will also be returned in their standard original format. Delivery, without additional costs to be borne by the Customer, will take place within 30 working days from the date of conclusion of the contract. Within 90 days from the effective date of termination of the Agreement, Wolters Kluwer will securely destroy the data and related backups. At the request of the Customer, the data can be obtained in another format after preliminary technical checks and with methods, times and costs to be agreed.	IPY-04	Agreements must include provisions specifying CSCs access to data upon contract termination and will include: a. Data format b. Length of time the	Data Portability Contractual Obligations	
IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Wolters Kluwer maintains a written global information security program of policies, procedures and controls aligned to NIST CSF, ISO27001, and other equivalent standards, governing the processing, storage, transmission and security of data (the “Security Program”). The Security Program mandates industry-standard practices designed to protect data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to data transmitted, stored or otherwise processed. Wolters Kluwer updates the Security Program to address (i) new and evolving security threats, (ii) changes to industry standards, (iii) technological advances in security tools, and (iv) amendments required following risk assessments undertaken. Additionally, all security policies and standards governing the Security Program are reviewed, updated, and approved annually by the Wolters Kluwer Security Council (“Security Council”), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.	IVS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.	Infrastructure and Virtualization Security Policy and Procedures	Infrastructure & Virtualization Security
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council (“Security Council”), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.				
IVS-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?	Yes	CSP-owned	The resource usage is defined and monitored by the Infrastructure team. Forecasts and projections on future capacity requirements are performed in order to guarantee the system performance, performing cost/Benefit analysis. The Cloud Service provider monitors the total capacity of the resources on order to prevent information security incidents caused by lacking of resources.	IVS-02	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required	Capacity and Resource Planning	
IVS-03.1	Are communications between environments monitored?	Yes	CSP-owned	Wolters Kluwer has defined policies, procedures and formal controls to protect information transfer through all the kind of communication structures and tools. There is a Cloud Native Web Application Firewall in place to protect and monitor the traffic. Network Intrusion Detection Svstem is enabled and monitored.	IVS-03	Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.	Network Security	
IVS-03.2	Are communications between environments encrypted?	Yes	CSP-owned	Wolter Kluwer uses industry standard encryption to encrypt data in transit over public networks to the Wolters Kluwer environment and data at rest for systems, applications and services that involve or impact sensitive data.				
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes	CSP-owned	Network segmentation or zoning is used that allows network communications between multiple devices to be controlled. Network devices will generally fall into one of the following categories: Trust, Semi-Trusted,Untrusted, or Regulated. Final determination as to which category a network device falls under shall be made by GBS Network Security. The geographic placement of network devices (data center, campus, branch, home office, cloud, etc.) does not impact zone designation. Network security zone standards apply to all Wolters Kluwer facilities regardless of the size of geographic location.				
IVS-03.4	Are network configurations reviewed at least annually?	Yes	CSP-owned	The standard policies, processes and procedures related to Network Information Security are reviewed and updated: 1) following a regularly schedyled annual review 2) as required to correct or enhance the critical information content Basing on this review, network configurations are reviewed accordingly, so at leat annualv and on reauest to correct or enhance securitv level				
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Yes	CSP-owned	All the network configuration and firewall rules are compliant with the documents describing the policies related to the Network Information Security policies				

IVS-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	Yes	CSP-owned	All servers in Wolters Kluwer's cloud environment are configured as a minimum against the CIS Level1 hardening framework with approved deviations, appropriate documentation and monitoring processes are implemented and maintained.		IVS-04	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best	OS Hardening and Base Controls	
IVS-05.1	Are production and non-production environments separated?	Yes	CSP-owned	For Wolters Kluwer critical Assets, Wolters Kluwer deploys separate development, Quality Assurance and Production environments. Wolters Kluwer does not use customer data in development environment and maintains controls to prevent such use.		IVS-05	Separate production and non-production environments.	Production and Non-Production Environments	
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	Yes	Shared CSP and CSC	Application and customer data are stored in the same infrastructure, data in the same infrastructure is properly segmented and segregated, data access is properly monitored.	Customer has the rights of monitoring access exclusively to their own data through application features.	IVS-06	Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access	Segmentation and Segregation	
IVS-07.1	Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?	Yes	CSP-owned	Wolters Kluwer has defined policies, procedures and formal controls to protect information transfer through all the kind of communication structures. The communication protocols are updated and approved; we consider as secure and reliable at least TLS 1.2, if possibile 1.3. The VPN usage is suggested.		IVS-07	Use secure and encrypted communication channels when migrating servers, services, applications,	Migration to Cloud Environments	
IVS-08.1	Are high-risk environments identified and documented?	Yes	CSP-owned	Wolters Kluwer performs information security risk assessments as part of a risk governance program that is established with the objective to regularly assess and evaluate the effectiveness of the Security Program. Such assessments are designed to identify and assess potential risks impacting confidentiality, integrity, availability, and/or privacy of the information and data processed, stored or transmitted by the organization, resulting from any changes in the business or technology environments.		IVS-08	Identify and document high-risk environments.	Network Architecture Documentation	
IVS-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?	Yes	CSP-owned	Wolters Kluwer implements and maintains security mechanisms on endpoints using Threat detection tools, Network security tool (including firewalls, WAF, anti DDOS).		IVS-09	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection,	Network Defense	
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Wolters Kluwer utilizes a Security Incident Event Monitoring (SIEM) tool which feeds event notification into the Security Operations Center. Events are reviewed, prioritized, and tracked to remediation according to the established service level agreements.		LOG-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies	Logging and Monitoring Policy and Procedures	
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council (“Security Council”), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.					
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Yes	CSP-owned	The Log management System ensures the security and immutability of the logs.		LOG-02	Define, implement and evaluate processes, procedures and technical measures to ensure the	Audit Logs Protection	
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes	Shared CSP and 3rd-party	External attacks are monitored (as well as blocked) by the Web Application Firewalls.Wolters Kluwer uses a Security Incident Event Monitoring (SIEM) tool which feeds event notification into the Security Operations Center. Events are reviewed, prioritized, and tracked to remediation according to the established service level agreements.		LOG-03	Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on	Security Monitoring and Alerting	
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	Wolters Kluwer uses a Security Incident Event Monitoring (SIEM) tool which feeds event notification into the Security Operations Center. Events are reviewed, prioritized, and tracked to remediation according to the established service level agreements.e established service level agreements. Intrusion Detection System/Intrusion Prevention System are in place					
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes	CSP-owned	Only authorized personnel is able to access the logs and the administration console which allows the extraction of data related to the logs. Wolters Kluwer utilizes a Security Incident Event Monitoring (SIEM) tool which feeds event notification into the Security Operations Center. Events are reviewed, prioritized, and tracked to remediation according to the established service level agreements.		LOG-04	Restrict audit logs access to authorized personnel and maintain records that provide unique	Audit Logs Access and Accountability	
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	No	CSP-owned			LOG-05	Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely	Audit Logs Monitoring and Response	
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes	CSP-owned	Wolters Kluwer uses a Security Incident Event Monitoring (SIEM) tool which feeds event notification into the Security Operations Center. Events are reviewed, prioritized, and tracked to remediation according to the established service level agreements.e established service level agreements.					
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes	CSP-owned	The Azure NTP servers in Europe are managed by Microsoft and certified for conformity to several standards, including; NIST Special Publication 800-52 NIST Special Publication 800-53 ISO 17025		LOG-06	Use a reliable time source across all relevant information processing	Clock Synchronization	
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	No	CSP-owned	The data logged and the related formats for logging are defined		LOG-07	Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or	Logging Scope	Logging and Monitoring
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council (“Security Council”), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.					

LOG-08.1	Are audit records generated, and do they contain relevant security information?	No	CSP-owned	Logs may contain operational and/or sensitive data and are classified and handled in a manner that is consistent with data's classification according to the Wolters Kluwer Data Classification and Handling Standard, data contains relevant security information (such as unencrypted passwords, whether correctly typed or not) are never recorded in the system logs.	LOG-08	Generate audit records containing relevant security information.	Log Records	
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	No	CSP-owned	Logs contain records of system and network security are protected from breaches of their confidentiality and integrity. Therefore, the minimal integrity controls are in place: a) For sensitive systems, real time collection occurs, and the logs are stored off the system. b) Logging facilities and log information are protected against tampering, modification, destruction, and unauthorized access. c) System Administrators do not have permission to erase, deactivate, or modify logs of their own activities.	LOG-09	The information system protects audit records from unauthorized access, modification, and deletion.	Log Protection	
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	Yes	3rd-party outsourced	Wolters Kluwer has developed and follows an internal policy for the usage of cryptografic control for information protection. Where encryption is used on Cloud, the native tools of the cloud service provider are used. The cryptografic key management operations are logged and audited and all logging processes support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterpise-level analysis and reporting, as described in Wolters Kluwer Encryption and Key Management document and Wolters Kluwer Security Logging and Monitoring document (internal proprietary)	LOG-10	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures	Encryption Monitoring and Reporting	
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Yes	3rd-party outsourced	The Key Management procedure includes logging and auditing of cryptographic key management ativities. Loggin and reporting activities allow to monitor the application of the policies on the usage, protection and duration of crptographic keys during their whole lifecicle	LOG-11	Log and monitor key lifecycle management events to enable auditing	Transaction/Activity Logging	
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	Yes	CSP-owned	Logs of entry to the facility for all employees, visitors, service engineers and vendors are kept and maintained for a period of 90 days. i. In the event a review of access logs is required, the investigation and review will be coordinated with the Incident Response team(s) responsible for the facility. - Physical access to information system output devices is controlled to prevent unauthorized individuals from obtaining the output	LOG-12	Monitor and log physical access using an auditable access control system.	Access Control Logs	
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Yes	CSP-owned	The Failure and Anomalies are monitored and reported according to The Failure and Anomalies are monitored and reported according to internal policies for Security Logging and Monitoring.	LOG-13	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the	Failures and Anomalies Reporting	
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Yes	CSP-owned	Wolters Kluwer utilizes a Security Incident Event Monitoring (SIEM) tool which feeds event notification into the Security Operations Center. Events are reviewed, prioritized, and tracked to remediation according to the established service level agreements, informing the related accountable parties				
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	Wolters Kluwer has policies and procedures for security incident management by a cross-functional global information security incident response team that provides 24/7, 365 days a year proactive security monitoring, management, and response, in accordance with Wolters Kluwer's established corporate incident management plan.	SEF-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and	Security Incident Management Policy and Procedures	Security Incident Management, E-Discovery, & Cloud Forensics
SEF-01.2	Are policies and procedures reviewed and updated annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.				
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Wolters Kluwer's security team use standards and process to promptly analyze potential security incidents to assess the impact, determine if immediate risk exists, and take immediate action to mitigate such damage.	SEF-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies	Service Management Policy and Procedures	
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.				
SEF-03.1	Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Wolters Kluwer adopt an organizational model for managing and remediating cyber security incidents with WK divisions and business units. All members of the WK-CSIRT will be available during an incident when their corresponding roles are activated. The WK-CSIRT will function as a cross-functional team. This approach will ensure the WK-GIS team provides overall governance while leveraging existing IT staff and other key business personnel for incident management responsibilities during a security incident. The WK-CSIRT includes primary roles and groups. The groups include several additional roles, activated as necessary for the incident.	SEF-03	'Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant	Incident Response Plans	
SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	Yes	CSP-owned	To ensure processes and procedures within WK-CSIRP are operating effectively, the Document Owner tests the CSIRP at least once a year including documented table-top exercises with appropriate teams.	SEF-04	Test and update as necessary incident response plans at planned intervals or upon significant organizational or	Incident Response Testing	
SEF-05.1	Are information security incident metrics established and monitored?	Yes	CSP-owned	Wolters Kluwer handles cyber security incidents according to industry standards and considering distinct phases in the incident response process. Wolters Kluwer plan contains 6 phases that have been adapted and highlight key points in the decision-making processes.	SEF-05	Establish and monitor information security incident metrics.	Incident Response Metrics	
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Yes	CSP-owned	As described in the answer to SEF-05.1 question, Wolters Kluwer handles cyber security incidents following industry standards. Incidents Management plan foresees 6 different phases that have been adapted and highlight key points in the decision-making processes.	SEF-06	Define, implement and evaluate processes, procedures and technical measures supporting	Event Triage Processes	
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes	CSP-owned	Wolters Kluwer has established processes to share threat information across the organization and third parties as well as with outside agencies, as required, by applicable local laws and regulations.		Define and implement, processes, procedures and technical measures for security breach	Security Breach	

SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	Yes	CSP-owned	As described in the answer to SEF-07.1 question, Wolters Kluwer has established and applies processes to share threat information across the organization, third parties and outside agencies, as required by applicable local laws and regulations.	SEF-07	notifications. Report security breaches and assumed security breaches including any relevant supply chain	Security Breach Notification
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Yes	CSP-owned	Wolters Kluwer maintains contacts with organizations, local authorities, national agencies and regulatory bodies.	SEF-08	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other	Points of Contact Maintenance
STA-01.1	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Wolters Kluwer staff, contractors, or Service Providers (external or internal) may perform different roles (e.g. Third Party Risk Manager, Third Party Relationship Owner/Business Owner, Third Party Security Assessor, Third Party Legal Assessor, Finance Assessor, Division/BU, Global Legal Compliance Department, Information Security Policy & Standards Taskforce (SPST), Information Secuirty Council, Leadership Council) . Detailed interface procedural manuals clearly define which party performs these roles and must accommodate the diversity of Wolters Kluwer, meaning that many individuals across multiple entities (e.g., global, regional, and local business units) may perform these roles.	STA-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization.	SSRM Policy and Procedures
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council (“Security Council”), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.			
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes	Shared CSP and 3rd-party	Signed third party contracts are managed in the Wolters Kluwer approved contract management system. The Contract Owners monitor the active contracts and, if changes are needed, deals with the Procurement deparment to apply the necessary contract revisions. Deviation from the standard conditions are reported to the IT department, in order to peform a risk evaluation and take mitigation actions, if necessary. A contract is in place for each Third Party prior to the commencement of services being rendered. The business shall consult with SMEs for specific details and additional contractual language. At a minimum, the following topics are addressed within the Third-Party contract, when applicable. i. Scope of Service ii. Compliance with Applicable Laws and Regulations (e.g., breach notification) iii. Business Resumption and Contingency Plans iv. Limits of Liability v. Performance Measures or Benchmarks vi. Cost and Compensation vii. Indemnification viii. Default and Termination ix. Process, Transmit and Store Sensitive Information x. Ownership and License xi. Insurance xii. Customer Complaints xiii. Confidentiality xiv. Dispute Resolution xv. Subcontracting xvi. Foreign-Based Third Parties xvii. Intellectual Property xviii. The Right to Audit and Require Remediation	STA-02	Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.	SSRM Supply Chain
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	Yes	CSP-owned	Wolters Kluwer maintains a vendor risk management program that assesses all vendors that access, store, process, or transmit Wolters Kluwer information and customers’ information for appropriate security and privacy controls and business disciplines. Before Wolters Kluwer provides a vendor with access to personal information or any other sensitive information of Wolters Kluwer employees or customers, or critical assets, it is required that appropriate security controls are in place. Access by vendors is required to be limited to only the access required to provide the contracted-for services. Security controls are required to be implemented to ensure that vendor access is limited appropriately. Periodic reviews of vendors, including third-party security audits, may be used to confirm whether vendors are adhering to their obligations and maintaining appropriate security measures. In the cases of service providers that have access to reserved information or personal data, the Contract specifies the way in which the services are provided, the security measures to be applied and the SLA guaranteed. In addition, to reduce the risk related to information security, it is necessary that the provider signs an NDA (Non Disclosure Agreement) for the exhange/transfer/access to confidential information. In case the third party provider has to know personal data and to perform personal data treatment on behalf of or for interest of the Data Owner, the third party is nominated External Responsible of the data treatment, in compliance with art. 28 of the Reg. UE 2016/679. The Data Treatment Owner must identiy every external third party to whom personal data re communicated (either for legal compliance or for contractual choice). The designation document must have a specific date and must be signed-off by the Responsible of Data Treatment and from the Data Owner. For Cloud Service Provider, in addition to the requisites described above, the Contracts include the following specifications: - roles and responsibilities related to the information security of the CSp and CSC;	STA-03	Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.	SSRM Guidance

STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	Yes	Shared CSP and 3rd-party	Wolters Kluwer maintains a vendor risk management program that assesses all vendors that access, store, process, or transmit Wolters Kluwer information and customers' information for appropriate security and privacy controls and business disciplines. Before Wolters Kluwer provides a vendor with access to personal information or any other sensitive information of Wolters Kluwer employees or customers, or critical Assets, it is required that appropriate security controls are in place. Access by vendors is required to be limited to only the access required to provide the contracted-for services. Security controls are required to be implemented to ensure that vendor access is limited appropriately. Periodic reviews of vendors, including third-party security audits, may be used to confirm whether vendors are adhering to their obligations and maintaining appropriate security measures. In particular, before the third party can access to personal, sensitive or critical data, Wolters Kluwer performs a qualification process to veruty that the vendor possesses tje security reqyurements requested by Wolters Kluwer. The qualification process is defined in compliance with the ISO 9001 norm. The following further qualification requirements are necessary for cloud service providers: - verification that the management procedures for secret authentication information for the services in perimeter of the contract are in line with the organization requirements; - verification that the services included in the Contract allows a profilation: at Cloud service level; at level of specific fuctions of the service; at level of informtion. - verification that logging criteria defined from the Cloud Service Provider are in line with the organization requirements; - verification that the services provided by the Cloud Service Provider satisfy the organization requirements in terms of environments segregations (tenants).	STA-04	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.	SSRM Control Ownership	Supply Chain Management, Transparency, and Accountability
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Yes	CSP-owned	The internal documentation is periodically reviewed and validated in reference to the processes for periodic reviews of vendors, including third-party security audits that may be used to confirm whether vendors are adhering to their obligations and maintaining appropriate security measures.	STA-05	Review and validate SSRM documentation for all cloud services offerings	SSRM Documentation Review	
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes	CSP-owned	Wolters Kluwer maintains a vendor risk management program that assesses all vendors that access, store, process, or transmit Wolters Kluwer information and customers' information for appropriate security and privacy controls and business disciplines. Periodic reviews of vendors, including third-party security audits, may be used to confirm whether vendors are adhering to their obligations and maintaining appropriate security measures.	STA-06	Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.	SSRM Control Implementation	
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	Yes	CSP-owned	The development and delivery process and the resources involved in the process are defined in the development process management documents drawn up according to ISO 27001 certification, as well as asset management.	STA-07	Develop and maintain an inventory of all supply chain	Supply Chain Inventory	
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Yes	CSP-owned	As described in the answer to STA-06.1 question, Wolters Kluwer maintains a vendor risk management program that assesses all vendors that access, store, process, or transmit Wolters Kluwer information and customers' information for appropriate security and privacy controls and business disciplines. Periodic reviews of vendors, including third-party security audits, may be used to confirm whether vendors are adhering to their obligations and maintaining appropriate security measures. In addition, at least once per calendar year, Wolters Kluwer obtains an assessment against the referred standards and audit methodologies by an independent third-party auditor.	STA-08	CSPs periodically review risk factors associated with all organizations within their supply chain.	Supply Chain Risk Management	
STA-09.1	Do service agreements between CSPs and CSCs (tenants) incorporate at least the following mutually agreed upon provisions and/or terms? • Scope, characteristics, and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third-party assessment • Service termination • Interoperability and portability requirements • Data privacy	Yes	CSP-owned	The Contracts between CSP and the CSC cointains, regulates and describes all the terms present in the requirement	STA-09	Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process	Primary Service and Contractual Agreement	
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	Yes	CSP-owned	Wolters Kluwer Italia reviews annually the terms and conditions to be used in the contracts with clients	STA-10	Review supply chain agreements between CSPs and CSCs at least	Supply Chain Agreement Review	
STA-11.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	Yes	CSP-owned	The internal assessment is carried out at least once a year upstream of the audits for ISO/IEC 27001, 27017 and 27018 certification.	STA-11	Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of	Internal Compliance Testing	
STA-12.1	Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Yes	CSP-owned	Wolters Kluwer maintains a vendor risk management program that assesses all vendors that access, store, process, or transmit Wolters Kluwer information and customers' information for appropriate security and privacy controls and business disciplines. Before Wolters Kluwer provides a vendor with access to personal information or any other sensitive information of Wolters Kluwer employees or customers, or critical Assets, it is required that appropriate security controls are in place. Access by vendors is required to be limited to only the access required to provide the contracted-for services. Security controls are required to be implemented to ensure that vendor access is limited appropriately. Periodic reviews of vendors, including third-party security audits, may be used to confirm whether vendors are adhering to their obligations and maintaining appropriate security measures.	STA-12	Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy	Supply Chain Service Agreement Compliance	
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.	STA-13	Periodically review the organization's supply chain partners' IT	Supply Chain Governance Review	

STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	Yes	CSP-owned	Wolters Kluwer Italy is ISO/IEC 27001, 27017 and 27018 certified, audits and inspections are performed annually by external assessor.	STA-14	Define and implement a process for conducting security assessments periodically for all	Supply Chain Data Security Assessment	
TVM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation?	Yes	CSP-owned	The Wolters Kluwer vulnerability management program is focused on the collection, analysis, summarization, tracking and reporting of identifiable vulnerabilities in applications, infrastructure, endpoint systems and networks. Remediation are schedule in accordance with established vulnerability management procedure policy and standards.	TVM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability	Threat and Vulnerability Management Policy and Procedures	Threat & Vulnerability Management
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council (“Security Council”), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.				
TVM-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Wolters Kluwer implements and maintains security mechanisms on endpoints, including firewalls, Threat detection solution and full disk encryption. Wolters Kluwer restricts personnel from disabling security mechanisms, in accordance with established endpoint protection procedure policy and standards.	TVM-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies	Malware Protection Policy and Procedures	
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council (“Security Council”), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.				
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk)?	Yes	CSP-owned	Emergency responses to vulnerability follow the remediation schedule in accordance with established vulnerability management standards.	TVM-03	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and	Vulnerability Remediation Schedule	
TVM-04.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	Yes	CSP-owned	Wolters Kluwer implements and maintains security mechanisms on endpoints, including firewalls, Threat detection solution and full disk encryption. Wolters Kluwer restricts personnel from disabling security mechanisms, in accordance with established endpoint protection procedure policy and standards.	TVM-04	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat	Detection Updates	
TVM-05.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the organization's vulnerability management policy)?	Yes	CSP-owned	Wolters Kluwer standards and process defines the steps that must be taken prior to each use of OSS (Open Source Software). This policy applies to any new use of open source software in any of its forms and considers vulnerability and license risk related to the use of OSS.	TVM-05	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party	External Library Vulnerabilities	
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Yes	Shared CSP and 3rd-party	Third-party penetration tests are performed annually.	TVM-06	Define, implement and evaluate processes, procedures and technical measures for the	Penetration Testing	
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Yes	CSP-owned	Monthly vulnerability external and internal scans are conducted. Application code security scans (SAST) and docker image scans are performed at each new release.	TVM-07	Define, implement and evaluate processes, procedures and technical measures for the detection of	Vulnerability Identification	
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	Yes	CSP-owned	Vulnerability remediation follow the remediation schedule in accordance with established vulnerability management standards.	TVM-08	Use a risk-based model for effective prioritization of vulnerability	Vulnerability Prioritization	
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes	CSP-owned	Wolters Kluwer vulnerability management program provide accurate visibility of remediation and risk across the organization.	TVM-09	Define and implement a process for tracking and reporting vulnerability identification and	Vulnerability Management Reporting	
TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Yes	CSP-owned	Wolters Kluwer vulnerability management program provide accurate visibility of remediation and risk across the organization.	TVM-10	Establish, monitor and report metrics for vulnerability identification	Vulnerability Management Metrics	
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes	CSP-owned	Wolters Kluwer implements and maintains security mechanisms on End User Computing (EUC) systems both physical and virtual, including firewalls, automated locking of devices after a specified period of inactivity, updated anti-virus, an advanced endpoint detection and response (EDR) solution, and full disk encryption. Wolters Kluwer restricts personnel from disabling security mechanisms.	UEM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least	Endpoint Devices Policy and Procedures	
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Wolters Kluwer updates all security policies and standards governing the Security Program annually by the Wolters Kluwer Security Council (“Security Council”), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.				

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	Wolters Kluwer evaluate implements and maintains list of approved software on end user computing, that have access to the Wolters Kluwer network, that store and or process any Wolters Kluwer Information, or any system where Wolters Kluwer customer data is stored or processed. The standard shall be applied uniformly independently of the organization deploying and managing these systems, in addition Wolters Kluwer adopt Secure Configuration Management baseline compliant to CIS L1 Standard with approved deviations.		UEM-02	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints	Application and Service Approval	Universal Endpoint Management
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	Yes	CSP-owned	Wolters Kluwer provides, updates and publishes each quarter a technical standard for end user computing. Atlantide is a web application that users access via web browsers; major web browsers are supported.		UEM-03	Define and implement a process for the validation of the endpoint	Compatibility	
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Yes	CSP-owned	Wolters Kluwer maintains an inventory of its assets used within Wolters Kluwer and by any third parties authorized to act on its behalf, and an inventory of all media and equipment where data is stored. An asset is anything that has value to Wolters Kluwer, which includes hardware, software, information, infrastructure, outsourced services and even resources with specific skills and knowledge ("Asset").		UEM-04	Maintain an inventory of all endpoints used to store and access company data	Endpoint Inventory	
UEM-05.1	Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?	Yes	CSP-owned	Wolters Kluwer Secure Configuration Management (SCM) comprises a set of activities focused on establishing and maintaining the integrity of systems through control of the processes for initializing, changing, and monitoring the baseline configurations of those assets.		UEM-05	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints	Endpoint Management	
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	NA	CSC-owned	Wolters Kluwer for end user computing are configured and hardened to the appropriate, most current "Center for Internet Security (CIS) L1 Hardening Standard" with documented deviations.	Atlantide application can be used by most common browsers, this kind of setting cannot be managed by Wolters Kluwer but is the responsibility of the customer.	UEM-06	Configure all relevant interactive-use endpoints to require an automatic	Automatic Lock Screen	
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	Yes	CSP-owned	Wolters Kluwer implements and maintains a Change Management program and the related supporting processes designed for Change Management.		UEM-07	Manage changes to endpoint operating systems, patch levels, and/or applications through	Operating Systems	
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	Yes	CSP-owned	Wolter Kluwer uses industry standard encryption to encrypt data in transit over public networks to the Wolters Kluwer environment and data at rest for systems, applications and services that involve or impact sensitive data.		UEM-08	Protect information from unauthorized disclosure on managed endpoint	Storage Encryption	
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Yes	CSP-owned	Wolters Kluwer implements and maintains security mechanisms for end user computing, including firewalls, automated locking of devices after a specified period of inactivity, updated anti-virus, an advanced endpoint detection and response (EDR) solution, and full disk encryption. Wolters Kluwer restricts personnel from disabling security mechanisms.		UEM-09	Configure managed endpoints with anti-malware detection and prevention	Anti-Malware Detection and Prevention	
UEM-10.1	Are software firewalls configured on managed endpoints?	Yes	CSP-owned	Wolters Kluwer implements and maintains security mechanisms for end user computing, including firewalls, automated locking of devices after a specified period of inactivity, updated anti-virus, an advanced endpoint detection and response (EDR) solution, and full disk encryption. Wolters Kluwer restricts personnel from disabling security mechanisms.		UEM-10	Configure managed endpoints with properly configured software firewalls.	Software Firewall	
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	Yes	CSP-owned	Wolters Kluwer implements and maintains DLP solution for end user computing device to identify data in motion to IM Clients, E-mail clients, Mass shared storage devices etc.		UEM-11	Configure managed endpoints with Data Loss Prevention (DLP) technologies	Data Loss Prevention	
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	Yes	CSP-owned	Wolters Kluwer implements and maintains hardware and software security baseline including geolocation capabilities for enduser mobile device.		UEM-12	Enable remote geo-location capabilities for all managed mobile	Remote Locate	
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	Yes	CSP-owned	Wolters Kluwer implements and maintains hardware and software security baseline including remote company data wipe on end user mobile devices.		UEM-13	Define, implement and evaluate processes, procedures and technical measures to enable the	Remote Wipe	
UEM-14.1	Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?	Yes	Shared CSP and 3rd-party	Wolters Kluwer defined System security setting for end user computing devices across Wolters Kluwer including all divisions, customer units and operating companies. For third-party contractual measure are in place, Virtual WorkSpaces compliant to security setting and managed by Wolters Kluwer is the preferred method for all contractors and contingent workers to access the Wolters Kluwernetwork.		UEM-14	Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain	Third-Party Endpoint Security Posture	

End of Standard