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	Proen maintains a comprehensive portfolio of Policies and Procedures mapped to ISO27001 standard. Proen has documented, approved and published Information security policy document required to govern the established ISMS.		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 procedures at least annually.	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	The security policies are reviewed at least annually to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes	CSP-owned	Proen engages with external certifying bodies and independent auditors to review and test the Proen overall control environment.		A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Independent Assessments	
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes	CSP-owned	The audit and assurance assessments are performed according to risk-based plans and policies.		A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	Risk Based Planning Assessment	
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Yes	CSP-owned	Proen annually performs internal and external audits to assess the security and compliance of its services, conform to the requirements of ISO/IEC 27001, ISO 9001 and relevant legislation or regulations.		A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	Requirements Compliance	
A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence?	Yes	CSP-owned	An audit management process is defined and is in place for supporting the audit and other activities. Proen contracts with independent third-parties in accordance with specific audit standards. Yearly audit plans in place as per ISO 27001 certification requirements.		A&A-05	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	Audit Management Process	
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	The risk-based corrective action plan to remediate audit findings is documented and maintained as part of Audit management Process. A detailed plan of action and milestones is used to document and track remediation of identified vulnerabilities and security weaknesses identified through various internal and independent security assessments, open items are reviewed though Corrective and preventive action.		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 status to relevant stakeholders.	Remediation	
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	Yes	CSP-owned	The remediation status of audit findings reviewed and reported to relevant stakeholders, as per the Audit management process and Corrective Action Procedure. The Closure status of findings are reviewed and maintained.					
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?	NA		Proen doesn't have any platform/services which are developed by either in house our outsourced development teams. All our platform/services use commercially of the shelf (COTS) products.		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 security capabilities. Review and update the policies and procedures at least annually.	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?	NA		Proen doesn't have any platform/services which are developed by either in house our outsourced development teams. All our platform/services use commercially of the shelf (COTS) products.					
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	NA		Proen doesn't have any platform/services which are developed by either in house our outsourced development teams. All our platform/services use commercially of the shelf (COTS) products.		AIS-02	Establish, document and maintain baseline requirements for securing different applications.	Application Security Baseline Requirements	
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	NA		Proen doesn't have any platform/services which are developed by either in house our outsourced development teams. All our platform/services use commercially of the shelf (COTS) products.		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?	NA		Proen doesn't have any platform/services which are developed by either in house our outsourced development teams. All our platform/services use commercially of the shelf (COTS) products.		AIS-04	Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	Secure Application Design and Development	
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	NA		Proen doesn't have any platform/services which are developed by either in house our outsourced development teams. All our platform/services use commercially of the shelf (COTS) products.		AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.	Automated Application	

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
AIS-05.2	Is testing automated when applicable and possible?	NA		Proen doesn't have any platform/services which are developed by either in house our outsourced development teams. All our platform/services use commercially of the shelf (COTS) products.		AIS-05		Security Testing	
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	NA		Proen doesn't have any platform/services which are developed by either in house our outsourced development teams. All our platform/services use commercially of the shelf (COTS) products.		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?	NA		Proen doesn't have any platform/services which are developed by either in house our outsourced development teams. All our platform/services use commercially of the shelf (COTS) products.					
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	NA		Proen doesn't have any platform/services which are developed by either in house our outsourced development teams. All our platform/services use commercially of the shelf (COTS) products.		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?	NA		Proen doesn't have any platform/services which are developed by either in house our outsourced development teams. All our platform/services use commercially of the shelf (COTS) products.					
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Proen has documented and implemented policies, processes, procedures and controls ensuring Business Continuity of the services. And Proen performs regular testing of its business continuity plans.		BCR-01	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually.	Business Continuity Management Policy and Procedures	Business Continuity Management and Operational Resilience
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	At least annually, policies and procedures are reviewed and updated to ensure that the most current policy is available to the employees. Proen's business continuity processes are validated frequently by external auditors through assessments including but not limited to ISO27001.					
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes	Shared CSP and 3rd-party	Proen develops, maintains, updates, and disseminates Business Continuity Planning policies and procedures in line to ISO27001 requirements. Criteria are based on annual risk assessments and business impact analysis and related policies and procedures.		BCR-02	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.	Risk Assessment and Impact Analysis	
BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	Yes	Shared CSP and 3rd-party	Proen Cloud Infrastructure Services has developed the Business continuity and operational resilience strategies considering the acceptable limits regarding risk appetite and tolerance. Proen has defined and maintained the BC plan and procedure.		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	Shared CSP and 3rd-party	Proen has defined and maintained the BC plan and procedure.		BCR-04	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.	Business Continuity Planning	
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	Yes	Shared CSP and 3rd-party	Proen develops, maintains, updates, and disseminates Business Continuity Planning policies and procedures in line to ISO27001 requirements.		BCR-05	Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review periodically.	Documentation	
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes	CSP-owned	Documentation is made available internally to Proen authorized personnel.					
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Yes	CSP-owned	At least annually, policies and procedures are reviewed and updated to ensure that the most current policy is available to the employees.					
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	The business and operational resilience plans are exercised annually or upon significant changes or as per the contractual terms and conditions.		BCR-06	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	Business Continuity Exercises	
BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	Yes	CSP-owned	Proen develops, maintains, updates, and disseminates Business Continuity Planning policies and procedures in line to ISO27001 requirements. Stakeholders are identified in accordance with the BC/DR plans.		BCR-07	Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.	Communication	

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
BCR-08.1	Is cloud data periodically backed up?	Yes	Shared CSP and CSC	Proen follows a backup process and systems are backed up regularly and back up are restored and tested. All core platform services are configured with backup as per compliance requirements.		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	Shared CSP and CSC	Proen maintains the backup as per the contractual requirements and the necessary security controls are ensured.					
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	Shared CSP and CSC	Proen follows a backup process and systems are backed up regularly and back up are restored and tested. Proen maintains the backup and Backup restoration testing is done as per the contractual requirements and the necessary security controls are ensured.					
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	Shared CSP and 3rd-party	Disaster Recovery Plan is established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters. DR Plan testing is conducted annually or when significant changes occur.		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 significant changes.	Disaster Response Plan	
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes	Shared CSP and 3rd-party	Disaster Recovery Plan is established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters. DR Plan testing is conducted annually or when significant changes occur.					
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes	Shared CSP and 3rd-party	DR Plan reviewed and updated annually or when significant changes occur.		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?	Yes	CSP-owned	Customers are free involve any local emergency authorities for their DR test plan execution.					
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	Proen has identified the business requirements for the availability of information systems and implemented redundant components or architectures when designing information systems.		BCR-11	Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.	Equipment Redundancy	
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	Proen maintains a comprehensive portfolio of Policies and Procedures mapped to the standard ISO27001 requirements. Proen has documented and implemented a Change management process. All changes related to information management systems follow the change management process. Changing organizational assets including applications, systems, infrastructure, configuration, etc. undergo the Change management process established.		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, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.	Change Management Policy and Procedures	Change Control and Configuration Management
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	The security policies at Proen are reviewed atleast annually, to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Yes	CSP-owned	Proen change management process ensures defined quality change control and testing process with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services.		CCC-02	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.	Quality Testing	
CCC-03.1	Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?	Yes	CSP-owned	Changing organizational assets including applications, systems, infrastructure or configuration, undergo the Change management process established. The risks associated with changing organizational assets are Impact analysed, approved and applied.		CCC-03	Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced).	Change Management Technology	
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes	CSP-owned	Change management policies and processes monitors every change and ensure only authorised changes executed on production systems.		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	Shared CSP and CSC	All the provisions to limit changes that impact CSC-owned environments are a part of customer contract.		CCC-05	Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.	Change Agreements	
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes	CSP-owned	Proen change management process ensures defined quality change control and testing process with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services.		CCC-06	Establish change management baselines for all relevant authorized changes on organization assets.	Change Management Baseline	
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Yes	CSP-owned	Proen platform monitoring policies and procedures ensure the proactive monitoring of platform changes.		CCC-07	Implement detection measures with proactive notification in case of changes deviating from the established baseline.	Detection of Baseline Deviation	

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
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes	CSP-owned	Proen has defined the exceptions process.		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	Proen maintains a comprehensive portfolio of Policies and Procedures mapped to the ISO27001 requirements. Exception Process to any policies is defined and implemented at Proen.					
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	Proen change management process takes care of the rollback plan, proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns.		CCC-09	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.	Change Restoration	
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Proen has established and documented encryption policy and procedure.		CEK-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually.	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	CSP-owned	The security policies at Proen are reviewed atleast annually, to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes	CSP-owned	Policies on cryptographic guidelines include roles and responsibilities.		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	Shared CSP and CSC	Encryption is done for data at-rest and in-transit at the platform level. However, customer environment encryption is at their descretion.		CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.	Data Encryption	
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Yes	CSP-owned	Proen has established policies and procedures that govern the use of cryptographic controls. And Proen has an established key management process in place to support the organization's use of cryptographic techniques.		CEK-04	Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.	Encryption Algorithm	
CEK-05.1	Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	Yes	CSP-owned	Proen has established change management policies and procedures which ensures that changes are tested, documented, risk assessed, and authorized in a consistent and timely manner		CEK-05	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.	Encryption Change Management	
CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	Yes	CSP-owned	The changes to policy are reviewed by the compliance/security team. Any changes or updates to the system are reviewed by different stakeholders.		CEK-06	Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.	Encryption Change Cost Benefit Analysis	
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	Yes	CSP-owned	Proen performs a risk assessment for its offerings and the supporting infrastructure in which assets are identified and threats, vulnerabilities, impact, and likelihood are assessed. Cryptography, encryption, and key management related risks are part of it.		CEK-07	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	Encryption Risk Management	
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	NA		Proen Currently does not offer Key Management Services to the customers.		CEK-08	CSPs must provide the capability for CSCs to manage their own data encryption keys.	CSC Key Management Capability	
CEK-09.1	Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event?	Yes	CSP-owned	Encryption key management systems, polices, and procedures are reviewed annually.		CEK-09	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s).	Encryption and Key Management Audit	
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Yes	CSP-owned	Proen conducts Audit on policies, processes, systems annually internally and are validated by external auditors through ISO 27001					
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	Proen cryptographic methods rely on recognized practices and standards for the encryption of data,		CEK-10	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	Key Generation	
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes	CSP-owned	Cryptographic secrets are used and are managed carefully and securely. The use of private keys is generally not supported.		CEK-11	Manage cryptographic secret and private keys that are provisioned for a unique purpose.	Key Purpose	Cryptography, Encryption & Key Management
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Yes	CSP-owned	A key rotation process is in place.		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	CSP-owned	The validity of cryptographic keys is monitored, and keys are replaced before they become invalid.		CEK-13	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.	Key Revocation	
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?	NA		CSC can bring in their own Encryption solutions as per their information security requirements. Encryption and Key management responsibilities are limited only upto platform level.		CEK-14	Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements.	Key Destruction	
CEK-15.1	Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	NA		CSC can bring in their own Encryption solutions as per their information security requirements. Encryption and Key management responsibilities are limited only upto platform level.		CEK-15	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.	Key Activation	

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
CEK-16.1	Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSP-owned	A policy for the use of cryptographic methods is defined and implemented.		CEK-16	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.	Key Suspension	
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSP-owned	A key management process is defined.		CEK-17	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.	Key Deactivation	
CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSP-owned	Proen follows formal practices for key generation, distribution, storage, and access that are in line with industry best practices as per the defined Key LifeCycle Management Procedure for the platform services.		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	CSP-owned	Proen has policies in place for scenarios in which data must be encrypted, along with additional legal, compliance, or security requirements.		CEK-19	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.	Key Compromise	
CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSP-owned	Proen performs a risk assessment for its offerings and the supporting infrastructure in which assets are identified and threats, vulnerabilities, impact, and likelihood are assessed. Cryptography, encryption, and key management related risks are part of it.		CEK-20	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.	Key Recovery	
CEK-21.1	Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions?	Yes	CSP-owned	Proen maintains the list of cryptographic keys used for its operations and services; tracks and reports all cryptographic materials and status changes.		CEK-21	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.	Key Inventory Management	
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	Proen maintains a comprehensive portfolio of Policies and Procedures mapped to the ISO27001 requirements. Removal of any asset including equipment, information or software will not be permitted without prior approvals. Proen ensures that all storage media in any equipment are securely disposed by cleaning using methods including degaussing, shredding or appropriate destruction methods.		DCS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually.	Off-Site Equipment Disposal Policy and Procedures	
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Yes	CSP-owned	Proen ensures that all storage media in any equipment are securely disposed by data destruction using methods including degaussing and/or shredding or appropriate destruction methods.					
DCS-01.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually?	Yes	CSP-owned	The security policies are reviewed at least annually, to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					
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	Procedures for All Equipment move in and move out are defined and practised as per Asset management Policy and needs to follow relevant approval processes.		DCS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually.	Off-Site Transfer Authorization Policy and Procedures	
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	Yes	CSP-owned	Inventory relocation/transfer is approved and tracked as per Asset management Policy.					
DCS-02.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually?	Yes	CSP-owned	The security policies are reviewed atleast annually, to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					
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	All platform assets are hosted in a secure Tier3 Design certified Datacenters, which ensures the safe and secure environment/ facilities as per the defined policies and procedures.		DCS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually.	Secure Area Policy and Procedures	
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Yes	CSP-owned	The security policies are reviewed at defined intervals to ensure the continuing suitability, adequacy and effectiveness of the information security policies. Datacenter policies and procedures are also periodically reviewed.					
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	NA		No removable Media transfer applicable.		DCS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually.	Secure Media Transportation Policy and Procedures	
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	NA		No removable Media transfer applicable.					
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Yes	CSP-owned	Proen identified owners and classifications are designated for each of the processes and assets necessary for Proen Cloud operation in line to ISO27001 standard.		DCS-05	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.	Assets Classification	

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
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Yes	CSP-owned	Proen maintains asset inventories and assigns ownership for managing its critical resources. Assets have the labels with details of the assets and connections.		DCS-06	Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.	Assets Cataloguing and Tracking	Datacenter Security
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	Yes	CSP-owned	All controls for safeguarding the personnel, data and information systems are in place.		DCS-07	Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas.	Controlled Access Points	
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	Yes	CSP-owned	Physical security perimeters are defined and established between administrative and business areas, data storage, and processing facilities.					
DCS-08.1	Is equipment identification used as a method for connection authentication?	Yes	CSP-owned	Proen uses ACLs to achieve authentication integrity.		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	CSP-owned	Data Center Access Policies and Procedures and controls are in place to ensure only authorized personnel access the secure areas.		DCS-09	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.	Secure Area Authorization	
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Yes	CSP-owned	All Employee locations as well DCs are equipped with CCTV cameras, IDs as well checkpoints. Access control records are retained periodically as per the regulatory and contractual requirements.					
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Yes	CSP-owned	All Employee locations as well DCs are equipped with CCTV cameras, IDs as well checkpoints. Proen Data centers maintain secure external perimeter protections.		DCS-10	Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.	Surveillance System	
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	Yes	CSP-owned	All platform assets are hosted in a secure Tier3 Design and ISO 27001 certified Datacenters, which ensures the safe and secure environment/ facilities and Employee Awareness Building controls.		DCS-11	Train datacenter personnel to respond to unauthorized ingress or egress attempts.	Unauthorized Access Response Training	
DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	Yes	CSP-owned	All platform assets are hosted in secure Tier3 Design and ISO 27001 certified Datacenters, which ensures the safe and secure environment/ facilities and processes, procedures, and technical measures are 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.		DCS-12	Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.	Cabling Security	
DCS-13.1	Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?	Yes	CSP-owned	All platform assets are hosted in secure Tier3 Design and ISO 27001 certified Datacenters, which ensures the safe and secure environment/ facilities and data center environmental control systems are designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained.		DCS-13	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	Environmental Systems	
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	Yes	CSP-owned	All platform assets are hosted in secure Tier3 Design and ISO 27001 certified Datacenters, which ensures the safe and secure environment/ facilities and data center utility services are secured, monitored, maintained, and tested at planned intervals for continual effectiveness.		DCS-14	Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.	Secure Utilities	
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	Yes	CSP-owned	All platform assets are hosted in secure Tier3 Design and ISO 27001 certified Datacenters, which ensures the safe and secure environment/ facilities. Proen separates and takes care of Business critical equipment from locations subject to a high probability of environmental risk events		DCS-15	Keep business-critical equipment away from locations subject to high probability for environmental risk events.	Equipment Location	
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	Proen maintains a comprehensive portfolio of Policies and Procedures mapped to the ISO27001 requirements, which includes the policy and standard for classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level.		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, standards, and risk level. Review and update the policies and procedures at least annually.	Security and Privacy Policy and Procedures	
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	The security policies are reviewed at defined intervals to ensure the continuing suitability, adequacy and effectiveness of the information security policies. Proen security controls are maintained through frequent internal audits and are validated by external auditors through assessments including but not limited to ISO27001					

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
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	CSP-owned	The procedure for secure data disposal from storage media is defined.		DSP-02	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.	Secure Disposal	
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.		DSP-03	Create and maintain a data inventory, at least for any sensitive data and personal data.	Data Inventory	
DSP-04.1	Is data classified according to type and sensitivity levels?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.		DSP-04	Classify data according to its type and sensitivity level.	Data Classification	
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.		DSP-05	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.	Data Flow Documentation	
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.					
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.		DSP-06	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.	Data Ownership and Stewardship	
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.					
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.		DSP-07	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.	Data Protection by Design and Default	
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.		DSP-08	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	Data Privacy by Design and Default	Data Security and Privacy Lifecycle Management
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.					
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?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.		DSP-09	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.	Data Protection Impact Assessment	
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.		DSP-10	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Sensitive Data Transfer	
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.		DSP-11	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.	Personal Data Access, Reversal, Rectification and Deletion	
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)?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.		DSP-12	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	Limitation of Purpose in Personal Data Processing	
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.		DSP-13	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	Personal Data Sub-processing	
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.		DSP-14	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.	Disclosure of Data Sub-processors	
DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.		DSP-15	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.	Limitation of Production Data Use	
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes	CSP-owned	Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.		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?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.		DSP-17	Define and implement, processes, procedures and technical measures to protect sensitive data throughout it's lifecycle.	Sensitive Data Protection	
DSP-18.1	Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.		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 to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality	Disclosure Notification	

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
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?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.		DSP-18	of a law enforcement investigation.	Disclosure Notification	
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	NA		Proen does not classify data uploaded and stored by customers. Customer DATA security as per the contract is customer's own responsibility.		DSP-19	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.	Data Location	
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	Proen maintains a comprehensive portfolio of Policies and Procedures mapped to the ISO27001. The information governance program policies and procedures sponsored by organizational leadership are established.		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 organization. Review and update the policies and procedures at least annually.	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	The security policies and procedures at Proen are reviewed at defined intervals to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					
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	Proen has developed and maintains risk assessment processes aligned with the ISO27001 standard. Including risk assessments being performed at least annually. The risk management policy is defined taking into account all aspects business requirement.		GRC-02	Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.	Risk Management Program	
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Yes	CSP-owned	The security policies and procedures at Proen are reviewed at defined intervals to ensure the continuing suitability, adequacy and effectiveness of the information security policies.		GRC-03	Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.	Organizational Policy Reviews	
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Yes	CSP-owned	An approved exception process mandated by the governance program is established and followed. The Exception process defined for every policies and procedures.		GRC-04	Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.	Policy Exception Process	
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Yes	CSP-owned	Proen maintains a comprehensive portfolio of Policies and Procedures mapped to the ISO27001. The information governance program policies and procedures sponsored by organizational leadership are established.		GRC-05	Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.	Information Security Program	
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes	CSP-owned	The security roles and responsibilities for planning, implementing, operating, assessing, and improving Information Security governance programs are defined and documented by Proen as part of ISO 27001 standard requirements.		GRC-06	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	Governance Responsibility Model	
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Yes	CSP-owned	Proen constantly monitors changing regulatory requirements and subscribes to sources for additional updates. Any changes to the regulatory environment are identified, reviewed and addressed accordingly.		GRC-07	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.	Information System Regulatory Mapping	
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	Yes	CSP-owned	Proen maintains contact with relevant stakeholders.		GRC-08	Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.	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	CSP-owned	Proen maintains a comprehensive portfolio of Policies and Procedures mapped to the ISO27001. Proen has established HR Policies and procedures which takes care of background verification during onboarding process		HRS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually.	Background Screening Policy and Procedures	
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	Proen has established HR Policies and procedures according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk, which takes care of background verification during onboarding process.					
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	The security policies and procedures are reviewed at defined intervals to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					
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	The Acceptable Usage policies and procedures are in place to take care of acceptable use of organizationally owned or managed assets.		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 annually.	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	The security policies and procedures are reviewed at defined intervals to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					

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
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	The policies and procedures requiring unattended workspaces to conceal confidential data are established.		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 policies and procedures at least annually.	Clean Desk Policy and Procedures	Human Resources
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes	CSP-owned	The security policies and procedures are reviewed at defined intervals to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					
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	The policies and procedures to protect information accessed, processed, or stored at remote sites and locations are established.		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 procedures at least annually.	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	The security policies and procedures are reviewed at defined intervals to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	CSP-owned	The return procedures of organizationally-owned assets by terminated employees are established. Change of employment processes are in place and followed by Human Resources. These processes are maintained through internal audits and validated by independent auditors.		HRS-05	Establish and document procedures for the return of organization-owned assets by terminated employees.	Asset returns	
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Yes	CSP-owned	The procedures outlining the roles and responsibilities concerning changes in employment are established.		HRS-06	Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment.	Employment Termination	
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Yes	CSP-owned	The Access provisioning procedures to organizational information systems, resources, and assets are established.		HRS-07	Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.	Employment Agreement Process	
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes	CSP-owned	Proen hiring processes are in place and followed by Human Resources inline to the ISO 27001 security requirements. The provisions and terms for adherence to established information governance and security policies included within employment agreements. As part of onboarding induction training/awareness sessions are conducted on information security and governance perspective.		HRS-08	The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.	Employment Agreement Content	
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Yes	CSP-owned	Proen maintains employee roles and responsibilities relating to information assets and security. These responsibilities are supplemented, where necessary, with more detailed guidance for specific sites and information processing facilities.		HRS-09	Document and communicate roles and responsibilities of employees, as they relate to information assets and security.	Personnel Roles and Responsibilities	
HRS-10.1	Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?	Yes	CSP-owned	The NDA/Confidentiality agreement is reviewed at planned intervals		HRS-10	Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details.	Non-Disclosure Agreements	
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Yes	CSP-owned	The regular security training/awareness sessions are conducted to ensure that employees are up to date with best security practices.		HRS-11	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.	Security Awareness Training	
HRS-11.2	Are regular security awareness training updates provided?	Yes	CSP-owned	The regular security training/awareness sessions are conducted to ensure that employees are up to date with best security practices.					
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	CSP-owned	The security awareness program addresses all groups of different information and data sensitivity levels.		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 function relative to the organization.	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	Standard Operating Procedures are periodically reviewed or updated, for employees granted access to sensitive organizational and personal data.					
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	The employees are notified on their roles and responsibilities to maintain awareness and compliance with established policies and other legal/regulatory obligations.		HRS-13	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.	Compliance User Responsibility	
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	Proen identifies and maintains all requirements for access within the Access Control Policy which is based on least privilege and best practices. Platform does provide all the necessary capability to control the accesses based on least privilege role based access control and segregation of duties.		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	The security policies and procedures are reviewed at defined intervals to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					

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
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	Password policy is defined and implemented. Policies and standards have been established and implemented for password expiration, length, complexity.		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	Identity & Access Management
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	The security policies and procedures are reviewed at defined intervals to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes	CSP-owned	System identities are centrally maintained and access to the systems are controlled and periodically reviewed.		IAM-03	Manage, store, and review the information of system identities, and level of access.	Identity Inventory	
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes	CSP-owned	Separation of Duties is governed by the Access Control Policy; Proen provides all the necessary capability to control accesses based on least privilege role based access control and segregation of duties.		IAM-04	Employ the separation of duties principle when implementing information system access.	Separation of Duties	
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes	CSP-owned	Platform does provide all the necessary capability to control accesses based on least privilege role based access control and segregation of duties. Necessary user guides are provided up on request.		IAM-05	Employ the least privilege principle when implementing information system access.	Least Privilege	
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes	CSP-owned	A procedure for assigning user access rights for access to assets is defined in guidelines and implemented accordingly.		IAM-06	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	User Access Provisioning	
IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	Yes	CSP-owned	The Access control policy addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews.		IAM-07	De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.	User Access Changes and Revocation	
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	Proen carefully monitors effective access rights to minimise the risk of over-privileged accounts. Proen regularly conducts access reviews.		IAM-08	Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.	User Access Review	
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	Yes	CSP-owned	Administrative access is limited to the necessary minimum by default.		IAM-09	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated.	Segregation of Privileged Access Roles	
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Yes	CSP-owned	The process is defined and implemented to ensure privileged access roles and rights are granted for a limited period.		IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.	Management of Privileged Access Roles	
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	Yes	CSP-owned	Proen maintains and regularly verifies a separation of duties matrix to document the organizational roles established within the organization.					
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?	NA		Privileged access roles onto the Customer environments are managed by the CSC itself.		IAM-11	Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.	CSCs Approval for Agreed Privileged Access Roles	
IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated?	Yes	CSP-owned	Log data is preserved separately in protected areas and accessible for authorized admins only.		IAM-12	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.	Safeguard Logs Integrity	
IAM-12.2	Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?	Yes	CSP-owned	Proen operates a controlled and managed role-based access principle for granting access rights. The possibility of changing rights is limited to dedicated administrators who other administrators also monitor.					
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	Each account is assigned a unique ID. The use of shared accounts is not permitted.		IAM-13	Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.	Uniquely Identifiable Users	
IAM-14.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?	Yes	CSP-owned	Proen defines and implements processes, procedures, and technical measures that ensure users are identifiable through unique identification.		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 data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	Strong Authentication	
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Yes	CSP-owned	Different passwords are used for accessing different security levels of information					
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Yes	CSP-owned	Policies defining the secure use of passwords are in place		IAM-15	Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.	Passwords Management	
IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Yes	CSP-owned	Authorizations control in place for every applications/services as a mandatory requirement. Logical Access to Proen Cloud systems is protected via authentication requirements and restricted to the least access necessary.		IAM-16	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	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)?	NA		Proen customers are responsible for their data and have the ability to decide the method used to communicate between applications.			Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces		

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
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	NA		Proen customers are responsible for their data and have the ability to decide the method used to communicate between applications.		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-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	NA		Customers are responsible for their data and have the ability to decide the method used to migrate applications to and from Proen.					
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	NA		Customers are responsible for their data and have the ability to decide the method used to migrate applications to and from Proen.					
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	NA		Proen customers are responsible for their data and have the ability to decide the method used to communicate between applications.					
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes	Shared CSP and CSC	The list of all standard APIs available in the service are published. Proen uses an industry-recognized virtualization platform and standard virtualization formats (e.g., QCOW2) to ensure interoperability and portability.		IPY-02	Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability.	Application Interface Availability	
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	Yes	Shared CSP and CSC	All data import/export is over an SSL/TLS enabled channel.		IPY-03	Implement cryptographically secure and standardized network protocols for the management, import and export of data.	Secure Interoperability and Portability Management	
IPY-04.1	Do agreements include provisions specifying CSC data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Yes	Shared CSP and CSC	Proen Cloud's customer contract Service Schedule include provisions specifying CSC data access upon contract termination, which is an additional service to be purchased by the CSC.		IPY-04	Agreements must include provisions specifying CSCs access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Data Portability Contractual Obligations	
IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Proen maintains security requirements for the configuration and management of devices connecting to corporate services. The policies also apply to infrastructure and virtual instances.		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	The security policies and procedures are reviewed at defined intervals to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					
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	Proen maintains capacity and resource planning in alignment with ISO27001 and monitors system processing capacity and usage and corrective actions to address changing requirements, if applicable, and documents, in accordance with the defined policy.		IVS-02	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	Capacity and Resource Planning	
IVS-03.1	Are communications between environments monitored?	Yes	Shared CSP and CSC	Customer environments are totally isolated. No network communication is allowed between the customer environments in the cloud platform. However, customer can control the communications as per their business requirements.		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	Shared CSP and CSC	Communication channels are logically isolated from other networks. Customer configuration information supplied through the management portal is protected while in transit and at rest.					
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes	Shared CSP and CSC	Proen allows only Business justified Network communications and requires authorization.					
IVS-03.4	Are network configurations reviewed at least annually?	Yes	CSP-owned	The security policies and procedures are reviewed at defined intervals to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Yes	Shared CSP and CSC	Baseline configurations come with vendor defaults disabled, and only necessary ports and protocols enabled. System configurations have a baseline agreed upon with the customer and include all necessary service configurations within the image. Customers then have the opportunity to enable configurations that their tenancies need to operate.					
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 resources provided are hardened and subject to baseline configurations for security.		IVS-04	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.	OS Hardening and Base Controls	
IVS-05.1	Are production and non-production environments separated?	Yes	CSP-owned	Customers have the ability and responsibility to implement separate environments for production and test processes. Customers should develop production and non-production environments in compliance with their defined compliance goals.		IVS-05	Separate production and non-production environments.	Production and Non-Production Environments	

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
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	CSP-owned	Customer environments are logically segregated to prevent customers from accessing resources not assigned to them.		IVS-06	Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants.	Segmentation and Segregation	
IVS-07.1	Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?	Yes	CSP-owned	Data in transit is protected via encryption according to industry standards.		IVS-07	Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.	Migration to Cloud Environments	
IVS-08.1	Are high-risk environments identified and documented?	Yes	CSP-owned	The overall risk management program of the ISMS identifies and documents high-risk 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	Intrusion and anomaly detection systems are installed (based on customer agreement) to provide insight into attack activities and provide adequate information to respond to incidents.		IVS-09	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.	Network Defense	
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	The logging and monitoring policies and procedures are established, documented.		LOG-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.	Logging and Monitoring Policy and Procedures	Logging and Monitoring
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	The security policies and procedures are reviewed at defined intervals to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Yes	CSP-owned	The processes and procedures to ensure audit log security and retention have been defined, documented and implemented. Logs stored are only accessible to authorised users.		LOG-02	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.	Audit Logs Protection	
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes	CSP-owned	A comprehensive event monitoring and event management system is in place.		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 such events and corresponding metrics.	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	Proen reacts to events and communicates with its stakeholders depending on severity.					
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes	CSP-owned	Proen restricts physical and logical access to audit logs to authorized users only.		LOG-04	Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.	Audit Logs Access and Accountability	
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Yes	CSP-owned	A comprehensive cloud platform monitoring system is in place to detect abnormalities and anomalies.		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 actions on detected anomalies.	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	The process to review and take appropriate actions on detected incidents is established and maintained.					
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes	CSP-owned	All systems in eitc are synchronised with the NTP Server .		LOG-06	Use a reliable time source across all relevant information processing systems.	Clock Synchronization	
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Yes	Shared CSP and CSC	Proen does not access, modify, delete, or retain data outside of the terms of the customer service agreement. Optional Managed Security services can be opted by the customer, else the customer data or meta data is not logged by Proen as part of Event logging.		LOG-07	Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment.	Logging Scope	
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	Scope of System events logging and monitoring is reviewed at least annually.					
LOG-08.1	Are audit records generated, and do they contain relevant security information?	Yes	CSP-owned	Proen maintains an automated log collection and analysis tool to review and analyse log events.		LOG-08	Generate audit records containing relevant security information.	Log Records	
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Yes	CSP-owned	The processes and procedures to ensure audit log security and retention have been defined, documented and implemented. Audit logs are retained and reviewed regularly. Logs stored are only accessible to authorised users. Logs are protected against tampering and unauthorized access.		LOG-09	The information system protects audit records from unauthorized access, modification, and deletion.	Log Protection	
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	Yes	CSP-owned	The collection of log data applies to all systems of the cloud platform. This includes events related to cryptographic operations.		LOG-10	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.	Encryption Monitoring and Reporting	
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Yes	CSP-owned	Events related to cryptographic key management are recorded and evaluated.		LOG-11	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.	Transaction/Activity Logging	
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	Yes	CSP-owned	Authorized personnel are able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms, at datacenters. Access log review of Datacenter is conducted periodically.		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	Log-monitoring system is configured to generate the alerts to be reported to responsible stakeholders.			Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.		

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
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Yes	CSP-owned	An internal procedure defines the management of events and, depending on their severity, which accountable parties must be informed or involved.		LOG-13		Failures and Anomalies Reporting	
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	A policy for security incident management is in place. Proen operates a comprehensive process to ensure prompt notification and investigation of incidents.		SEF-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually.	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	The security policies and procedures are reviewed at defined intervals to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Proen maintains incident response procedures to help ensure prompt notification and investigation of incidents. These procedures include guidelines on prioritization based on severity.		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 and procedures at least annually.	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	The security policies and procedures are reviewed at defined intervals to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					
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	Proen incident management addresses all the necessary internal departments and affected stakeholders.		SEF-03	'Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted.'	Incident Response Plans	
SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	Yes	CSP-owned	The security incident response plan is tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes.		SEF-04	Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.	Incident Response Testing	
SEF-05.1	Are information security incident metrics established and monitored?	Yes	CSP-owned	The information security incident metrics are established and monitored. Proen monitors and quantifies the types, volumes, and impacts on all information security incidents.		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	Proen establishes the procedures and supporting business processes and technical measures, to triage security-related events and ensure timely and thorough incident management process.		SEF-06	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.	Event Triage Processes	
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes	CSP-owned	Breaches are reported to required parties according to legal and contractual requirements.		SEF-07	Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.	Security Breach Notification	
SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	Yes	CSP-owned	Incident management at Proen incorporates required process steps for reporting breaches.					
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	Extensive lists for contact information to authorities and offices exist.		SEF-08	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.	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	Proen maintains a comprehensive portfolio of Policies and Procedures mapped to the ISO27001. The Third Party Security Risk Management Policy and Vendor management procedures are established and documented.		STA-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually.	SSRM Policy and Procedures	
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Yes	CSP-owned	The security policies and procedures are reviewed at defined intervals to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes	CSP-owned	Supply Chain processes are managed at the corporate level. Proen's policies and procedures establish the CSP's control ownership and responsibilities as it relates to the service offerings. Relevant information security requirements with suppliers are addressed in supplier agreements. Shared Security responsibilities with CSC are addressed in the customer contract.		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	The guidance about SSRM applicability to CSC has been informed through the service agreement. The Security Roles and Responsibilities with the Vendors are documented and managed through the Vendor Contract Agreement.		STA-03	Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.	SSRM Guidance	
STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	Yes	CSP-owned	The shared ownership and applicability of all CSA CCM controls is delineated according to the SSRM for the cloud service offering, through the service schedule/ contract. This is delineated in the CSA CAIQ and in the Cloud Infrastructure Services Responsibility Matrix		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	

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
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Yes	CSP-owned	Proen defines the roles and responsibilities of Proen and customer/ supplier as part of the onboarding as per the services. The responsibilities are reviewed and validated for all cloud services.		STA-05	Review and validate SSRM documentation for all cloud services offerings the organization uses.	SSRM Documentation Review	Supply Chain Management, Transparency, and Accountability
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes	CSP-owned	The services are established securely against the defined SSRM. Proen's SSRM documentation undergoes periodic review.		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 list of service providers - and services have been maintained with necessary details.		STA-07	Develop and maintain an inventory of all supply chain relationships.	Supply Chain Inventory	
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Yes	CSP-owned	Supply chain risks are reviewed as part of our business continutiy plan review.		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	All contractual commitments with customers are continuously monitored and measured to ensure compliance.		STA-09	Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third party assessment • Service termination • Interoperability and portability requirements • Data privacy	Primary Service and Contractual Agreement	
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	Yes	CSP-owned	All contractual commitments with customers are continuously monitored and measured to ensure compliance. The supply chain agreements between CSPs and CSCs are reviewed at every service renewal stage		STA-10	Review supply chain agreements between CSPs and CSCs at least annually.	Supply Chain Agreement Review	
STA-11.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	Yes	CSP-owned	Regular internal audits are conducted to ensure conformance to compliance of standards, policies, procedures, and SLA activities.		STA-11	Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually.	Internal Compliance Testing	
STA-12.1	Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Yes	CSP-owned	The relevant polices to comply with information security, confidentiality, access control,etc are implemented and monitored. All contractual commitments with partners as well as customers are continuously monitored and measured to ensure compliance.		STA-12	Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards.	Supply Chain Service Agreement Compliance	
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	Yes	CSP-owned	Proen employs a vendor management process that includes contractual requirements and periodic review of vendors to ensure adherence to Proen requirements.		STA-13	Periodically review the organization's supply chain partners' IT governance policies and procedures.	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	Proen has agreements with key third party suppliers with defined expectations and implements relationship management tools where applicable with third-party suppliers. These management mechanisms include frequent validation that the supplier is meeting the expectations as defined in agreements.		STA-14	Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.	Supply Chain Data Security Assessment	
TVM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation?	Yes	CSP-owned	Threat and vulnerability management policies and procedures are defined. The Vulnerability analysis and Penetration testing Scans are carried out by a External party annually.		TVM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually.	Threat and Vulnerability Management Policy and Procedures	Threat & Vulnerability Management
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	The security policies and procedures are reviewed at defined intervals to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					
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	Procedures and guidelines for detecting and protecting malware infections are part of the ISMS policy framework.		TVM-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually.	Malware Protection Policy and Procedures	
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	The security policies and procedures are reviewed at defined intervals to ensure the continuing suitability, adequacy and effectiveness of the information security policies.					
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	The treatment of detected vulnerabilities is carried out according to precise process specifications and prioritisation, considering the severity of a vulnerability.		TVM-03	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.	Vulnerability Remediation Schedule	
TVM-04.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	Yes	CSP-owned	Proen's threat detection systems are continuously updated, based on attack signatures as new signatures are identified		TVM-04	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.	Detection Updates	
TVM-05.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the organization's vulnerability management policy)?	NA		Only COTS products are used by Proen platform. No Software development is done.		TVM-05	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.	External Library Vulnerabilities	

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
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Yes	CSP-owned	Proen coordinates external 3rd party penetration testing using qualified and certified penetration testers at least annually.		TVM-06	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.	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	Proen routinely scans internal and external facing non-customer apps for vulnerabilities.		TVM-07	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.	Vulnerability Identification	
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	Yes	CSP-owned	Vulnerability remediation is prioritized using a risk-based model from CVSS. Proen's Vulnerability Priority Guidelines define how security vulnerability remediation timelines and prioritizations are based on level of risk.		TVM-08	Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.	Vulnerability Prioritization	
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes	CSP-owned	Proen has defined a process to track and report vulnerability identification and remediation activities. If required, Proen notifies the impacted stakeholders.		TVM-09	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.	Vulnerability Management Reporting	
TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Yes	CSP-owned	Proen has established metrics for vulnerability identification and remediation and are being monitored and reported periodically.		TVM-10	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.	Vulnerability Management Metrics	
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes	CSP-owned	The policies and procedures for asset management have been established and maintained.		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 annually.	Endpoint Devices Policy and Procedures	Universal Endpoint Management
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	The security policies and procedures are reviewed at defined intervals to ensure the continuing suitability					
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	The organization has maintained an approved software list that can be used on endpoints.		UEM-02	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.	Application and Service Approval	
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	Yes	CSP-owned	The organization has defined Hardening checklists for the endpoints. The compatibility validation is done as part of the system hardening checklist.		UEM-03	Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.	Compatibility	
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Yes	CSP-owned	The assets that are allowed to store and access company data have been identified and a asset inventory has been maintained.		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	Proen implements a management system, aligned with ISO 27001, to support this policy.		UEM-05	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.	Endpoint Management	
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes	CSP-owned	All endpoints must enforce an automatic screen lock after a certain period of inactivity.		UEM-06	Configure all relevant interactive-use endpoints to require an automatic lock screen.	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	Proen's endpoint devices are continuously patched through system management software as patches become available, which varies by OS and applications.		UEM-07	Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.	Operating Systems	
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	No	CSP-owned	Storage units within endpoints are not encrypted by default.		UEM-08	Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.	Storage Encryption	
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Yes	CSP-owned	Only corporate devices are approved to store information/data pertaining to the company. All corporate devices are by default enabled with anti malware software.		UEM-09	Configure managed endpoints with anti-malware detection and prevention technology and services.	Anti-Malware Detection and Prevention	
UEM-10.1	Are software firewalls configured on managed endpoints?	Yes	CSP-owned	The Endpoints are protected by Firewall. Windows Firewall is used.		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	Proen leverages and enforces DLP via administrative procedures, information classification.		UEM-11	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.	Data Loss Prevention	
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	Yes	CSP-owned	Remote geolocation capabilities are implemented if required and meaningful.		UEM-12	Enable remote geo-location capabilities for all managed mobile endpoints.	Remote Locate	
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	No	CSP-owned	Proen employees are prohibited to store confidential information on endpoints, but capabilities to detect/enforce remote wipe policy are not present.		UEM-13	Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.	Remote Wipe	
UEM-14.1	Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?	Yes	CSP-owned	Third-Party Endpoint Security Posture is ensured through defined procedures, and technical and/or contractual measures. 3rd party endpoint connection requirements - to Proen resource is defined and verified.		UEM-14	Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets.	Third-Party Endpoint Security Posture	

End of Standard