CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2
Creative Force Ltd (November 2022)

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	Creative Force is ISO/IEC 27001 certified and fully compliant with PCI-DSS. Both certificates are accessible via our public security page and updated annually. In addition, we manage a comprehensive information security management system (ISMS) which is also reviewed and maintained, at least annually.		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						
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes	Shared CSP and 3rd-party	Apart from regular internal assessments, Creative Force engages several 3rd party vendors to help, advise, and audit our ISMS, at least annually.		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	Shared CSP and 3rd-party			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			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			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			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						
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities?	Yes	CSP-owned	All our policies and controls are implemented through ISO/IEC 27001, which includes an annual external audit to ensure Creative Force is applying its policies accurately and effectively.		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?	Yes	CSP-owned						
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes	CSP-owned	To support these baseline requirements, each of our applications go through rigourous security testing, including external vulnerability and penetration testing at least twice a year.		AIS-02	Establish, document and maintain baseline requirements for securing different applications.	Application Security Baseline Requirements	
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes	CSP-owned			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?	No	CSP-owned	Our flexible SDLC process has established processes and workflows to maintain our security requirements, most notably within our automated testing, code review and deployment strategies.		AIS-04	Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	Secure Application Design and Development	
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Yes	CSP-owned			AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.	Automated Application Security Testing	
AIS-05.2	Is testing automated when applicable and possible?	Yes	CSP-owned	Tests are automated whenever possible.					
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes	CSP-owned	We have a CI/CD pipeline that has been developed and improved over multiple years. It currently manages deployments to a number of regions for multiple applications.		AIS-06	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Automated Secure Application Deployment	
AIS-06.2	Is the deployment and integration of application code automated where possible?	Yes	CSP-owned	All deployments are entirely automated.					
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes	Shared CSP and 3rd-party	If vulnerabilities are discovered, these are logged as new tasks and depending on their severity are resolved either immediately or as part of our defined engineering process.		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?	Yes	CSP-owned						Remediation	
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Creative Force has a well-considered BC & DR plan in place and tested monthly. Reports available on request.		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	As per our ISO/IEC 27001 requirements, all policies are reviewed at least annually.					
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes	CSP-owned	Most of our BC & DR policies revolve around our in-house applications and their longevity, as these are the highest-risk areas were they to be affected by any disaster.		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 CSC	We are risk averse and our strategy is heavily informed by it.	Where necessary, CSC should evaluate and determine use of our software based on their own risk appetite.	BCR-03	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.	Business Continuity Strategy	
BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	Yes	CSP-owned			BCR-04	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.	Business Continuity Planning	
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	Yes	CSP-owned			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						
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Yes	CSP-owned	As part of our ISO/IEC 27001 certification, all policies, including our business continuity and disaster recovery process are reviewed at least annually.					
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	Yes	CSP-owned	Yes, please see above.		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			BCR-07	Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.	Communication	
BCR-08.1	Is cloud data periodically backed up?	Yes	Shared CSP and CSC	Cloud data is backed up multiple times a day.	CSC should back up their data should their risk appetite determine its necessity, outside of our own backup solutions and methods.	BCR-08	Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.	Backup	
BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	Yes	CSP-owned	Backups are exclusively visible to our DevOps team for recovery purposes. These backups are integrity and availability tested daily. The backups are also used to setup test environments within the same region for BC & DR testing which is conducted on a monthly basis.					
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	CSP-owned						
BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	Yes	CSP-owned	Both natural and man-made disasters are included in our disaster response plan.		BCR-09	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.	Disaster Response Plan	
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes	CSP-owned	At least annually. And immediately when a significant change occurs.					
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes	CSP-owned	Our plan is exercised on a monthly basis, and reports can be provided on request.		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?	NA		Creative Force does not have any brick-and-mortar locations. Our work force is fully remote and as such, we have no official office. The monthly BC & DR testing does not include local emergency authorities but these are stipulated in our plan should a real-world event impact on individuals or infrastructure.					
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			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			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	
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	All of our policies and procedure execution are reviewed annually, at a minimum.					

CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Yes	CSP-owned		CCC-02	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.	Quality Testing	Change Control and Configuration Management
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	Risks are reviewed regularly and if not covered by our current policies, will either be updated to include new risks, or added to the risk register and mitigated.	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		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?	NA		Changes that may be of concern to CSCs (e.g. adding a sub-processor) are notified in advance, though no authorisation is requested.	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		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?	No			CCC-07	Implement detection measures with proactive notification in case of changes deviating from the established baseline.	Detection of Baseline Deviation	
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes	CSP-owned		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					
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		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		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					
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes	CSP-owned	Only 3 individuals have access, including our Technical Director and DevOps team.	CEK-02	Define and implement cryptographic, encryption and key management roles and responsibilities.	CEK Roles and Responsibilities	
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes	CSP-owned	We use AES-256 encryption for all data at rest, and SSL1.3 for all data during transfer.	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		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?	No		We do not have a change management procedure for cryptography controls and implementation, primarily because it happens so rarely. In the lifetime of the Creative Force business, we've necessarily updated our encryption approach from TLS 1.2 to 1.3, as 1.3 was clearly more secure.	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?	No		As per above.	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?	No		We have not created a separate risk program for this as our approach is clear and straightforward. Only three staff have access and change opportunities are minimal when considering we implement the highest standards.	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?	No		This is not currently possible on our platform, but is a feature that we are considering implementing in the future. We'd be happy to explore this with both existing and new clients on a case-by-case basis.	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		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	All of our processes and policies are externally audited, at least annually. We conduct regular internal reviews much more frequently.				

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			CEK-10	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	Key Generation	Cryptography, Encryption & Key Management
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes	CSP-owned	All keys are utilised for specific purposes and not shared. Additionally, all our keys are kept secret and physically separated from our environments.		CEK-11	Manage cryptographic secret and private keys that are provisioned for a unique purpose.	Key Purpose	
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	No	CSP-owned	We're not currently able to rotate cryptographic keys based on a calculated cryptoperiod. This is due to how our data is currently encrypted. However, we aim to have this resolved in 2023 with a new encryption system which would allow for regular key rotation.		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			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		We do not use hardware keys as part of the organisation, and the soft keys we do use are regularly reviewed, as well as part of staff exiting the company.		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		Our keys are generated when necessary, and never beforehand. When keys are generated, they are provided to the authorised individuals as soon as possible (usually within minutes).		CEK-15	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.	Key Activation	
CEK-16.1	Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	NA		We do not believe this actually applies to our work and services offered.		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?	NA				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?	NA		Keys are never archived, they are simply removed when no longer needed.		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?	NA		We do not generate specific scenario keys. Our keys have general uses in our platform.		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			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?	NA				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			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	If equipment is not destroyed, they are remotely wiped.					
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						
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				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.		

DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	Yes	CSP-owned			DCS-02	Review and update the policies and procedures at least annually.	Off-Site Transfer Authorization Policy and Procedures	Datacenter Security
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						
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	As a remote business, we have no physical offices or facilities to secure. Our personnel are responsible for physical security of their own working environments.		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?	NA							
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	Yes	CSP-owned			DCS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually.	Secure Media Transportation Policy and Procedures	
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	Yes	CSP-owned						
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	NA		This is applicable to, and deferred to - AWS, our hosting partner.		DCS-05	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.	Assets Classification	
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	NA	3rd-party outsourced			DCS-06	Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.	Assets Cataloguing and Tracking	
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	Yes	Shared CSP and 3rd-party	As a remote business, we have no physical offices or facilities to secure. Our application infrastructure is physically secured by our cloud infrastructure provider, AWS. Our personnel are responsible for physical security of their own working environments.		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?	NA		This is not relevant to our business as a remote-working organisation. Additionally, our platform is serviced by Amazon Web Services (AWS) in the cloud, and so we defer our information security policies and certification in respect to storage and processing facilities to their ISO 27001 certification (and others).					
DCS-08.1	Is equipment identification used as a method for connection authentication?	No				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?	NA		Controlled by AWS for our application infrastructure. We otherwise have no server infrastructure of our own.		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?	NA		Controlled by AWS for our application infrastructure. We otherwise have no server infrastructure of our own.					
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	NA		Controlled by AWS for our application infrastructure. We otherwise have no server infrastructure of our own.		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?	NA		Controlled by AWS for our application infrastructure. We otherwise have no server infrastructure of our own.		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?	NA		Controlled by AWS for our application infrastructure. We otherwise have no server infrastructure of our own.		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?	NA		Controlled by AWS for our application infrastructure. We otherwise have no server infrastructure of our own.		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?	NA		Controlled by AWS for our application infrastructure. We otherwise have no server infrastructure of our own.		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?	NA		Although this is not specifically applicable to our business, our BC & DR plan does indeed cover scenarios whereby complete and total disaster of a given region applies to our services. In such instances, we are able to recover to full operational capacity within 24 hours in a nearby region.		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?	No				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	Data Security and Privacy Lifecycle Management
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes	CSP-owned						
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Yes				DSP-02	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.	Secure Disposal	
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Yes	CSP-owned			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?	No				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?	No		This will be resolved in the very near future as we're currently altering a number of products, services and endpoints and so this will change dramatically. Once complete, full data flow documentation will be available.		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?	No							
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	No		We do not currently have specific ownership over personal and sensitive data, but we will have policies and procedures on this in the very near future as we intend on becoming ISO / IEC 27701 certified.		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?	No		As above.					
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Yes	CSP-owned			DSP-07	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.	Data Protection by Design and Default	
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Yes	CSP-owned			DSP-08	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	Data Privacy by Design and Default	
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	No	CSP-owned						
DSP-09.1	Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations and industry best practices?	Yes	CSC-owned		Origin, nature, particularity and severity relates to data being collected as determined by CSC, so DPIA responsibility is largely with CSC.	DSP-09	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.	Data Protection Impact Assessment	
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	Yes	CSP-owned	In part. Despite having no processes or policies around this, we do implement a number of technical solutions to satisfy this control, by storing all data at rest securely, as well as in transit, by using TLS1.3, and encrypting all data at rest using AES-256 encryption.		DSP-10	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Sensitive Data Transfer	
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	Yes	CSP-owned			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)?	No				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)?	Yes				DSP-13	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	Personal Data Sub-processing	
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	Yes				DSP-14	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.	Disclosure of Data Sub-processors	

DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	Yes		Data rarely leaves our production environment. It is technically impossible to retrieve this data by our engineering team(s), as any use of production data is automatically sanitised and/or pseudonymised before use in other environments, such as when requiring such data for evaluating solutions for bug fixes. In respect to other departments, authorisation is obtained through our client success team.		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				DSP-16	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	Data Retention and Deletion	
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Yes	Shared CSP and CSC	This is documented in Schedule B of our DPA "Technical & organisational measures"	CSC as the data controllers must implement their own processes and procedures around the data lifecycle, as some elements of it will begin outside of the Creative Force domain boundary.	DSP-17	Define and implement, processes, procedures and technical measures to protect sensitive data throughout it's lifecycle.	Sensitive Data Protection	
DSP-18.1	Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations?	Yes	CSP-owned	You can see our documentation on this here.		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 of a law enforcement investigation.	Disclosure Notification	
DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?	Yes	CSP-owned	Our privacy policy can be found here					
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	Yes	CSP-owned	Covered in Schedule A of our DPA		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			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						
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	This is covered under ISO 27001 as part of our risk identification and mitigation procedures.		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			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?	NA		Deviations cannot occur, either the risk is identified and mitigated, or added to our risk register.		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	We have implemented policies in accordance with ISO 27001, which is reviewed and audited annually.		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			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			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?	No				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			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						
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes	CSP-owned						
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			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	

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			HRS-02		Technology Policy and Procedures	
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Although yes, we do establish this, for the most part it is non-applicable to our organisation, and really only applies when workspaces change to public locations (such as when staff work from a cafe).		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	
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes	CSP-owned						
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?	NA				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?	NA							
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	CSP-owned			HRS-05	Establish and document procedures for the return of organization-owned assets by terminated employees.	Asset returns	Human Resources
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Yes	CSP-owned			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			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			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			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?	NA		Such changes are so rare for our organisation that we have not organised or planned, regular reviews. As our organisation grows we will revisit this requirement.		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			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						
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	CSP-owned			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	All employee access is strictly controlled and monitored, particularly when it comes to sensitive private information.					
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			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			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						
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned			IAM-02	Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.	Strong Password Policy and Procedures	
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Yes	CSP-owned						
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes	CSP-owned			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			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	Staff are only ever provided as much access as is required to fulfill their roles competently and without delay.		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	See our System and Application access control procedure, as well as our HR procedure.	IAM-06	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	User Access Provisioning	Identity & Access Management
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		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		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		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?	NA		How our company works with specific roles means that time-limited access does not apply. Everyone has a role, and those roles sometimes require certain access privileges. If that staff member exists, or changes roles, then we revisit access permissions.	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?	NA						
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		Customers cannot participate. Ie. Not applicable. However, when using our products, customers can manage their own permissions and access roles.	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?	No		We have technical measures that restrict access to all logging, but no written procedures around this requirement.	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?	No		Although no, this also doesn't really apply. With our logging in place, changes to logging configuration aren't applicable from a read-write perspective.				
IAM-13.1	Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?	Yes			IAM-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		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	All our systems communicate using TLS1.3, and this is true both of internal and external system communications, as well as communication between end-user devices and servers.				
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Yes	CSP-owned		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		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)?	Yes	CSP-owned		IPY-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually.	Interoperability and Portability Policy and Procedures	Interoperability & Portability
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	No						
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	NA		Our software is designed to work within a very set range of environments (namely AWS), and these are documented as part of our devops processes and infrastructre. Because this is all automated, the documentation of this is not necessary.				
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						
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	NA						

IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes	Shared CSP and CSC	Clients can work with our public API to retrieve all data they may need for portability.	All CSCs must establish their own software solutions when working with our APIs.	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	CSP-owned			IPY-03	Implement cryptographically secure and standardized network protocols for the management, import and export of data.	Secure Interoperability and Portability Management		
IPY-04.1	Do agreements include provisions specifying CSC data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Yes	CSP-owned	These are covered more generally under sections 5 and 16 of our DPA (Data retention agreement).		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?	No		Our infrastructure (virtualisation does not apply) is all automated and so once in place, rarely (if ever) changes. As such we have not established any policies or procedures around this aspect.		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?	NA								
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	Shared CSP and 3rd-party	Yes, and this is all automated - all of our systems scale up and down automatically as required.		IVS-02	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	Capacity and Resource Planning		
IVS-03.1	Are communications between environments monitored?	Yes	CSP-owned	We use various tools, such as TrendMicro Cloud One as well as working toward some other solutions to monitor all traffic. We also use ESET to monitor traffic on our internal network.		IVS-03	Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.	Network Security		
IVS-03.2	Are communications between environments encrypted?	Yes	CSP-owned	All communications use TLS1.3 for encrypted connections between all endpoints.						
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes	CSP-owned	In addition to this, MFA/2FA is enforced internally in case connections are hijacked or spoofed.						
IVS-03.4	Are network configurations reviewed at least annually?	No		We have a VPN for all staff to connect to, this is the only network that we manage and this is not yet included as part of any policy or procedure.						
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	No		Due to the limited network access required, and the fact that we access mostly SaaS systems, our requirement around network configuration policies and procedures is minimal.						
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 end-user systems must be protected using ESET Cloud protect, and every one of our server hosts as part of the infrastructure are protected using Trend Micro Cloud One.		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	We have several environments, each of which is separated logically and physically.		IVS-05	Separate production and non-production environments.	Production and Non-Production Environments		
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	Yes	CSP-owned	Client data is logically separated within the same region, and physically separated when compared to tenant data in other regions. Furthermore, each of our deployment processes is also segmented logically.		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	TLS1.3 is enforced at every level of our infrastructure.		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?	No		We have not taken this step in respect to our enviornments.		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			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?	No		We do not yet have any specifc logging or monitoring policies, but are currently looking at various solutions to close this gap.		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		
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	No		We do not yet currently have any policies around logging and monitoring.						
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?			We do not yet have any specifc logging or monitoring policies, but are currently looking at various solutions to close this gap.		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	We have a security identification policy and procedure, which includes identification, monitoring and closing.	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	Logging and Monitoring
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	We have several tools that upon irregular or erroneous activity, immediately alert the entire company to a potential problem. This is done and managed via various Cloudwatch alerts in AWS, as well as Newrelic. We're also looking to expand this in the very near future.				
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes	CSP-owned	Log access is limited to engineers 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?	No		We do not yet have security audit logs.	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	This is covered as part of our Incident Management procedure.				
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes	CSP-owned	All systems are expected to sync with the world clock daily.	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?	No		We do not yet have any policies or procedures around logging for information meta/data systems.	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?	No		We do not yet have any policies or procedures around logging requirements.				
LOG-08.1	Are audit records generated, and do they contain relevant security information?	No		We do not yet have any policies or procedures around logging for information meta/data systems.	LOG-08	Generate audit records containing relevant security information.	Log Records	
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Yes	CSP-owned	Logs can only be accessed, and only by selected individuals within the organisation.	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?	No			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?	NA		We do not yet use key rotation within our systems so this is not applicable. We are investigating how to apply this to our platform in the near future.	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?	NA		We are a 100% remote-working company so this does not apply to us.	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-13	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.	Failures and Anomalies Reporting	
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Yes	CSP-owned					
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	For the SEF controls, we have a Security Incident policy and procedure, that is approved by our ISO 27001 certification.	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					
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned		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					
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		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		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?	NA		We have not yet defined any metrics to specific to security incidents that we we monitor. In all honesty, our security incident pattern is so irregular and rare that such metrics are not yet useful to us.	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			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	The Office of the Australian Information Commissioner (responsible for the Privacy Act) publish a guide to handling personal information security breaches. In the case of a privacy breach, we will follow this guide: Part 3: Responding to data breaches — four key steps (part 3 of of the Data breach preparation and response guide). See: https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response		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	Shared CSP and 3rd-party						
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	No				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	We do yet have a defined Shared Security Responsibility Model, however there are many aspects of a good SSRM that we have established and evaluate regularly.		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	Supply Chain Management, Transparency, and Accountability
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	No							
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes	CSP-owned			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	Shared CSP and 3rd-party			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?	No				STA-04	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.	SSRM Control Ownership	
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Yes	CSP-owned			STA-05	Review and validate SSRM documentation for all cloud services offerings the organization uses.	SSRM Documentation Review	
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	No				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			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			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			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?	No		We review these semi-regularly, usually when a large organisational or security change is required.		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			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			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?	NA				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			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		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					
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	Along with our policies we also implement ESET Cloud protect organisation-wide for end-user devices, as well as Trend Micro Cloud One for our all our servers.	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	All our policies and procedures are reviewed annually as per our ISO 27001 certification.				
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	All vulnerabilities identified are evaluated immediately and then resolved based on the risk profile. Any vulnerability determined to be of medium risk or higher goes straight to our engineering teams to resolve, anything lower may or may not be resolved depending on the nature of the vulnerability (some may be identified but have no impact).	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		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		No processes per se, but we do have tools in place that automatically detect whether updates are available and/or when security vulnerabilities are present. This helps us to stay ahead of any issues that may be present and these are resolved immediately.	TVM-05	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.	External Library Vulnerabilities	
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Yes	CSP-owned	We have 3rd party pentests executed at least once every 6 months.	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	ESET Cloud protect manages this aspect of the policy for us, automatically.	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?	No			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?	NA			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?	NA		This is managed automatically by tools such as ESET Cloud Protect and Trend Micro cloud one. No policy applied, but the technical solution has been place for some time.	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		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	
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned					
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	We have a list of approved applications, though many machines our staff use are also personal machines so there is some leeway provided. This is mitigated somewhat by our enforced use of endpoint protection mechanisms such as ESET Cloud Protect.	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?	No			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		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		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		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?	NA		This is managed automatically by ESET. We enforce this and when an endpoint gets too far behind, we will investigate further and enforce if necessary. Sometimes updates can take a while (particularly major release versions) as this may create conflicts with existing software.		UEM-07	Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.	Operating Systems	Universal Endpoint Management
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	Yes	CSP-owned			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			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	Firewalls are enforced on every endpoint.		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?	No		We're currently looking into DLP technologies to help facilitate our growing protection solutions.		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?	No				UEM-12	Enable remote geo-location capabilities for all managed mobile endpoints.	Remote Locate	
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	Yes	CSP-owned			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?	NA				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									