CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	True IDC maintains and implements internal and external audit plans that are performed annually such as ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. following the internal audit procedure.	-
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Yes	CSP-owned	True IDC reviews internal audit proccedure annually.	-
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes	CSP-owned	True IDC conducts independent audit on a annual basis according to internal audit program and external audit plan.	-
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes	CSP-owned	True IDC's independent audit and assurance assessments are performed according to risk management.	-
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. - True IDC conducts information security risk management in accordance with the ISO/IEC 27001 standard and periodically performs information security risk assessment that cover all aspects of information security requirements and take into account the requirements of applicable laws and regulations. - True IDC verifies compliance with the relevant standards applicable to the audit.	-
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	True IDC has established internal audit procedure and performs internal audit annually according to this procedure. The internal audit procedure includes audit planning, risk analysis, security control assessments remediations, reporting, and reviews of past reports/evidence that are performed at least annually to test the efficiency and effectiveness of implemented security controls against the certified standards.	-
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	- True IDC uses an information security risk assessment method for determining risk-based corrective action plan of remediate audit findings. - The risk assessment process is documented, reviewed and conducted annually according to ISO/IEC 27001.	-
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	Yes	CSP-owned	True IDC reports the remediation status of audit findings to relevant stakeholder to review, take corrective and preventive actions.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
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	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes a system and software development policy which supports the organization' s application security.	Cloud customers are responsible for the development and implementation of application security policies and procedures to guide appropriate planning, delivery, and support of their organization's application security capabilities.
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	Cloud customers should review and update policies and procedures at least annually.
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes a system and software development policy which supports the organization' s application security. - True IDC is not an application developer, so True IDC has an application security baseline for internal systems that are outsouced development. - True IDC does not develop any applications on True IDC cloud for cloud customers.	Cloud customers are responsible for establishing baseline requirements to secure different applications within customer environment.
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	No	CSC-owned	True IDC does not develop any applications on True IDC cloud for cloud customers.	Cloud customers should identify their business objectives, security requirements and compliance obligations and then cloud customer should develop proper technical and operational metrics to manage application security.
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes	CSC-owned	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes a system and software development policy which supports the organization' s application security. - True IDC does not develop any applications on True IDC cloud for cloud customers.	Cloud customers should develop an SDLC process and implement it throughout the application development lifecycle.
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	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes a system and software development policy which supports the organization' s application security. - True IDC has UAT (User Acceptance Test) and final acceptance test (FAT) criteria to accept new internal system, upgrades, and new versions. - True IDC does not develop any applications on True IDC cloud for cloud customers.	Cloud customers should develop a testing strategy including criteria for acceptance of new information systems, upgrades and new versions to ensure the security and compliance of application systems are met the delivery objectives and goals of their organization.
AIS-05.2	Is testing automated when applicable and possible?	No	CSC-owned	True IDC does not develop any applications on True IDC cloud for cloud customers.	Cloud customers should develop automation of application security testing when applicable and possible.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	No	CSC-owned	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes a system and software development policy which supports the organization' s application security. - True IDC does not develop any applications on True IDC cloud for cloud customers.	Cloud customers should develop a secure application deployment strategies and capabilities to ensure secure, standardized, and compliance during application code deployment.
AIS-06.2	Is the deployment and integration of application code automated where possible?	No	CSP-owned	True IDC does not develop any applications on True IDC cloud for cloud customers.	Cloud customers should develop automation of secure application deployment where applicable and possible.
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes	Shared CSP and CSC	- Policies and procedures have been established and implemented to vulnerability scan and patch management for True IDC cloud. - True IDC has defined the vulnerability scan schedule for each system including vCenter for True IDC cloud and has defined response times to vulnerability identifications based on severity level of vulnerability (critical, high, medium and low). - Any identified vulnerabilities are categoried and informed to system owners. System owners will remediate in timeline with the severity level of vulnerability (critical, high, medium and low).	Cloud customers are responsible for application vulnerabilities remediation following their application security vulnerability remediation processes.
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	No	CSC-owned	- True IDC does not develop any applications on True IDC cloud for cloud customers. - True IDC application security vulnerabilities are not automated across all environments.	Cloud customers should develop automation of application security vulnerability remediation where applicable and possible.
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	True IDC implements the business continuity plans and incident response plans for our services, reviews and excercises or tests them annually.	-
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	True IDC' s business continuity plans and incident response plans are reviewed 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	True IDC has established criteria for business continuity and operational resiliency strategies and capabilities based on business disruption and risk impacts.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	Yes	CSP-owned	- True IDC Cloud will be located in True IDC data centers with low-risk areas and far away from areas with potential harzards such as floods, hurricanes and earthquakes. - True IDC implements the business continuity plans and incident response plans for our services, reviews and excercises or tests them annually. - True IDC complies with ISO/IEC 27001. Information processing facilities and equipment shall have sufficient redundancy to meet availability requirements.	-
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	The operational resilience strategies are incorporated into the business continuity plans and incident response plans. The annual exercise and test results are documented.	-
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	Yes	CSP-owned	True IDC' s business continuity plans and incident response plans are developed and documented for all critical business processes.	-
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes	CSP-owned	Authorized True IDC employees can access the documents of business continuity plans and incident response plans.	-
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Yes	CSP-owned	True IDC implements the business continuity plans and incident response plans for our services, reviews and excercises or tests them 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	True IDC' s business continuity plans and incident response plans are excercised and tested annually using risk-based approach. When the organization and environment of True IDC cloud changes significant, True IDC' s business continuity plans and incident response plans are also excercised or tested.	-
BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	Yes	CSP-owned	True IDC establishes the call trees for communication with stakeholders.	-
BCR-08.1	Is cloud data periodically backed up?	Yes	Shared CSP and CSC	True IDC provides daily VMs image back up for seven copies.	Cloud customers should periodically back up their cloud data.
BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	Yes	CSC-owned	- True IDC provides daily VMs image back up for seven copies. True IDC restores VMs as per cloud customers request. - True IDC checks backup job daily. - True IDC employees sign non-disclosure agreements and have access to the system only for employees involved in their roles and responsibilities.	Cloud customers are responsible for maintaining the confidentiality, integrity, and availability of their backup data as required by their business.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	Shared CSP and CSC	- True IDC provides daily VMs image back up for seven copies. True IDC restores Vms as per cloud customers request. - True IDC tests backup and restoration annually.	Cloud customers should ensure that their backup data can be completely restored as required by their business.
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	True IDC uses business continuity plans to ensure that services can be recovered in a timely manner in the event of a disaster affecting True IDC cloud (IaaS).	-
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes	CSP-owned	True IDC' s business continuity plans and incident response plans are reviewed annually.	-
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes	CSP-owned	True IDC' s business continuity plans and incident response plans are excercised and tested annually using risk-based approach. When the organization and environment of True IDC cloud changes significant, True IDC' s business continuity plans and incident response plans are also excercised or tested.	-
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	Yes	CSP-owned	- True IDC involve local emergency authorities as needed based on the scenario. - True IDC participates in fire drills every year with the building provider.	-
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	- True IDC Cloud will be located in True IDC data centers with low-risk areas and far away from areas with potential harzards such as floods, hurricanes and earthquakes. - True IDC implements the business continuity plans and incident response plans for our services, reviews and excercises or tests them annually. - True IDC complies with ISO/IEC 27001. Information processing facilities and equipment shall have sufficient redundancy to meet availability requirements.	-
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	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policy and procedure for change management that including risk assessment for the organizational assets changing.	-
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Yes	CSP-owned	True IDC establishes the Method of Procedure (MOP) to identify change implementation plan, change date and time, scenario test, fall back plan etc. Change request must be approved by Change Advisory Board (CAB) before implementation.	-
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	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policy and procedure for change management that including risk assessment for the organizational assets changing. - Change risk is used for approval by Change Advisory Board (CAB).	-
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes	CSP-owned	- True IDC restricts only the authorized person to add, remove, update and manage the organization assets.	-
CCC-05.1	Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs?	Yes	CSP-owned	- True IDC will inform cloud customers in advance when changes impact to cloud customer environments.	-
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes	Shared CSP and CSC	True IDC establishes change management baselines for all relevant authorized changes on internal systems.	Cloud customers should establish a change management baseline to ensure that changes to all assets of customer organization are appropriately approved.
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Yes	CSP-owned	True IDC establishes the security baselines of True IDC systems. The security baselines of True IDC systems are verifed or audited annually.	-
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes	CSP-owned	True IDC will organize risk management process to review the exception cases.	-
CCC-08.2	Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?	Yes	CSP-owned	True IDC has a policy exception process which aligns business requirement and risk management.	-
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	True IDC establishes the Method of Procedure (MOP) to identify change implementation plan, change date and time, scenario test, fall back plan etc. Change request must be approved by Change Advisory Board (CAB) before implementation.	-
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policies and procedures for cryptography, encryption and key management.	Cloud customers should develop policies and procedures for cryptography, encryption and key management.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	Cloud customers should review and update policies and procedures at least annually.
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. - True IDC has set roles and responsibilities for cryptography, encryption, and key management systems and processes.	Cloud customers should define the appropriate roles and responsibilities for cryptography, encryption, and key management of customer environment and data.
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes	Shared CSP and CSC	- True IDC uses HTTPS to encrypt data in-transit when users connect True IDC cloud.	Cloud customers should use cryptographic libraries certified to approved standards for their data at-rest and in-transit.
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Yes	Shared CSP and CSC	- True IDC uses HTTPS to encrypt data in-transit when users connect True IDC cloud. - True IDC defines encryption algorithms in cryptography procedure for internal infrastructure systems and data e.g. SSL 3.0, TLS 1.2 or higher, RSA-2048 or higher, AES-128 bit or higher, SHA-256 etc.	Cloud customers should use appropriate data protection encryption algorithms that consider data classification, associated risks, and encryption technology usability for OS or above layer in True IDC cloud and their data.
CEK-05.1	Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policy and procedure for change management. - Any changes related to cryptography, encryption, and key management technology must be approved according to change management process.	Cloud customers should establish standard change management procedures to accommodate changes from internal and external sources for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.
CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. - Any changes related to cryptography, encryption, and key management technology on True IDC cloud must be approved according to change management process. Risk, cost and benefit analysis are managed and considered during change approval process. - Purchasing department is responsible to compare prices of SSL certificate on True IDC cloud and select vendor, while True IDC security engineer team is responsible to provide vendor lists and conduct risk assessment of vendor annually.	Cloud customers should manage and adopt changes management policies and procudures to cryptography, encryption, and key management technology that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. - True IDC has established the risk assessment and treatment Procedure as part of ISO/IEC 27001. Risk assessments are performed at least annually to ensure appropriate controls are in place to adequately manage the risk for our services. Risk assessment program includes risk management elements such as risk identification, risk analysis, risk evaluation, risk treatment and risk reporting. - The risk assessment covers the encryption and key management processes.	Cloud customers should establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	No	CSP-owned	True IDC sets and manages data encryption keys for True IDC cloud connecting.	-
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	- True IDC has passed the ISO/IEC 27001 certification. - True IDC assigns a standard compliance team to conduct internal audit at least annually for each certified standards. - True IDC develops and maintains an internal audit program to assess the conformanace and effectiveness of standards, policies, procedures, and SLA activities. - True IDC conducts independent audit on a annual basis according to internal audit program and external audit plan.	-
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. - True IDC assigns a standard compliance team to conduct internal audit at least annually for each certified standards. - True IDC develops and maintains an internal audit program to assess the conformanace and effectiveness of standards, policies, procedures, and SLA activities. - True IDC conducts independent audit on a annual basis according to internal audit program and external audit plan.	-
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	True IDC cloud uses SSL certificates for True IDC cloud web portal. SSL certificates are issued by SSL certificate provider and have a 2048-bit key size with validity for one year. True IDC renews SSL certificates every year according to change management process.	-
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes	CSP-owned	After key-pair generation, private key file is protected before distributing to management system of True IDC cloud.	-
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Yes	CSP-owned	True IDC cloud uses SSL certificates for True IDC cloud web portal. SSL certificates are issued by SSL certificate provider and have a 2048-bit key size with validity for one year. True IDC renews SSL certificates every year according to change management process.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
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	- Cryptographic keys are revoked and removed before the end of its established cryptoperiod when key is compromised or key is no longer part of True IDC. Incident ticket will be created to issue new certificate and perform according to change management process. - The public CA updates the CRL to include revoked certificate.	-
CEK-14.1	Are processes, procedures and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions?	Yes	CSP-owned	After SSL certificate expired or revoked, new SSL will replaced in system. True IDC security engineer team reviews backed up SSL certificate and destroys unused SSL certificate with key annually.	-
CEK-15.1	Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSP-owned	After True IDC generated key pairs, True IDC send it to CA for certificate signing. SSL certificate installation is performed according to change management process.	-
CEK-16.1	Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	CSP-owned	True IDC does not have key suspension process because cryptographic keys are revoked and removed before the end of its established cryptoperiod when key is compromised or key is no longer part of True IDC. Then True IDC will replace it with new cryptographic key.	-
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSP-owned	True IDC establishes a cryptography procedure that covers key deactivation at the time of its expiration date or revocation.	-
CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSP-owned	True IDC archives SSL certificate in centralized repository. Repository is limited access for the autorized person.	-
CEK-19.1	Are processes, procedures, and technical measures to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSP-owned	- True IDC cloud (IaaS) does not access cloud customer data. - Cryptographic keys are revoked and removed before the end of its established cryptoperiod when key is compromised or key is no longer part of True IDC. Incident ticket will be created to issue new certificate and perform according to change management process.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
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	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. - True IDC has established the risk assessment and treatment Procedure as part of ISO/IEC 27001. Risk assessments are performed at least annually to ensure appropriate controls are in place to adequately manage the risk for our services. Risk assessment program includes risk management elements such as risk identification, risk analysis, risk evaluation, risk treatment and risk reporting. - The risk assessment covers the encryption and key management processes. - True IDC archives SSL certificate in centralized repository. Repository is limited access for the autorized person. Key recovery is performed according to change management process.	Cloud customers should establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.
CEK-21.1	Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions?	Yes	Shared CSP and CSC	True IDC tracks and reports all key and cryptography detail and status from True IDC key management record.	Cloud customers should define, implement, and evaluate processes, procedures, and technical measures to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions.
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	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policies and procedures for the secure disposal of equipment used outside the organization's premises.	-
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policies and procedures for the secure disposal of equipment used outside the organization's premises. - Data and media are destroyed according to data classification and disposal method that defined by True IDC policies and procedures.	-
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	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	-
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	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. - All changes to True IDC assets for the the relocation or transfer to an alternate location must follow the change management policy and procedure.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	Yes	CSP-owned	All changes to True IDC assets for the the relocation or transfer to an alternate location must follow the change management policy and procedure.	-
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	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	-
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	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the procedure for security zones and matrix for data centers to ensure security zones are maintained.	-
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Yes	CSP-owned	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	-
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	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policies and procedures for the secure transportation of physical media incase cloud customers request the export virtual machine. - True IDC assets entering or leaving a data center must be inspected by data center staff to ensure that they are properly recorded and that the methods of transport are appropriate.	-
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	Yes	CSP-owned	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	-
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. - True IDC information is classified according to Data Classification and Data handling procedure. Information assets are classified based on legal, regulation, standard, value and inportant of information including the organizational business risk. - True IDC assets are registered and assigned ownership in asset inventory system.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. - True IDC assets are registered and assigned ownership in asset inventory system. - True IDC systems access are restricted based on least privilege.	-
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. - True IDC provides the physical security perimeters to safeguard personnel, data, and information systems such as CCTV, access card, mantraps, access system, security guards and barriers which are used to monitor ingress and egress at the various physical security zones in a data center and to ensure that only authorized personnel are allowed access.	-
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. - True IDC establishes the procedure for security zones and matrix for data centers to ensure security zones are maintained. - True IDC provides the physical security perimeters to safeguard personnel, data, and information systems such as CCTV, access card, mantraps, access system, security guards and barriers which are used to monitor ingress and egress at the various physical security zones in a data center and to ensure that only authorized personnel are allowed access.	-
DCS-08.1	Is equipment identification used as a method for connection authentication?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. - True IDC assets are identified in asset inventory system and True IDC audits inventory of assets every year.	-
DCS-09.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. - True IDC establishes the procedure for security zones and matrix for data centers to ensure security zones are maintained. - True IDC provides the physical security perimeters to safeguard personnel, data, and information systems such as CCTV, access card, mantraps, access system, security guards and barriers which are used to monitor ingress and egress at the various physical security zones in a data center and to ensure that only authorized personnel are allowed access.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Yes	CSP-owned	- True IDC data center access control records are retained according to the specified retention time based on legal, regulation and operational business need. - True IDC data center staffs are responsible for reviewing data center access records on monthly basis i.e. access control system log and CCTV log.	-
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. - True IDC data centers provide the surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts. - True IDC data center staffs are responsible for reviewing data center access records on monthly basis i.e. access control system log and CCTV log.	-
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	Yes	CSP-owned	True IDC data center staffs are trained to respond to unauthorized access or egress attempts.	-
DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the procedures and technical measures for protection of power and telecommunication cables from interception, interference, or damage.	-
DCS-13.1	Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. - True IDC provides Building Management System (BMS) to monitor temperature, humidity, water and power, and realtime alerts when conditions are not within accepted standards.	-
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. - True IDC data center utility services are monitored, maintained and tested at planned intervals.	-
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	Yes	CSP-owned	- True IDC Cloud will be located in True IDC data centers with low-risk areas and far away from areas with potential harzards such as floods, hurricanes and earthquakes. - True IDC complies with ISO/IEC 27001. Information processing facilities and equipment shall have sufficient redundancy to meet availability requirements.	-
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policy and procedure for data classification and data handling throughout its lifecycle according to all applicable laws and regulations, standards, and risk level.	Cloud customers should develop policies and procedures for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	Cloud customers should review and update policies and procedures at least annually.
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the procedure for data and media disposal that identify the secure data disposal method from media or storage according with data classification. If data or information classification is "Confidential" or "Restricted", disposal method of such data or information must be not recoverable.	Cloud customers should use industry-recognized methods to secure dispose of data or information in media or storage so that data or information cannot be recovered by any forensic means.
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Yes	Shared CSP and CSC	- True IDC complies with Thailand's personal data protection act BE 2562 (PDPA). - True IDC has a data inventory of sensitive and personal data and True IDC reviews and updates such inventory annually or significant changes.	Cloud customers should create and maintain a data inventory that includes at least sensitive and personal data.
DSP-04.1	Is data classified according to type and sensitivity levels?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policy and procedure for data classification and data handling throughout its lifecycle according to all applicable laws and regulations, standards, and risk level. - True IDC data is classified according to data types and sensitivity levels to ensure that data is properly handled in secure method.	Cloud customers should classify data based on data types and sensitivity levels.
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Yes	Shared CSP and CSC	- True IDC has documented a data flow of True IDC cloud. - True IDC cloud (IaaS) does not access cloud customer data so cloud customers are responsible for data flow documentation to identify what data is processed, stored or transmitted where.	Cloud customers are responsible for data flow documentation to identify what data is processed, stored or transmitted where.
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Yes	Shared CSP and CSC	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	Cloud customers should review and update data flow documentation at least annually or after changes.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Yes	Shared CSP and CSC	- True IDC complies with Thailand's personal data protection act BE 2562 (PDPA). - True IDC has a data inventory of sensitive and personal data and True IDC reviews and updates such inventory annually or significant changes. - True IDC data inventory of sensitive and personal data is identified the ownership (data subject such as customer, staff, vendor) and data accountability person or business unit of all relevant personal and sensitive data.	Cloud customers should document the ownership and stewardship of all relevant personal and sensitive data in True IDC cloud.
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	Yes	Shared CSP and CSC	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	Cloud customers should review the data ownership and stewardship documentation at least annually.
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Yes	Shared CSP and CSC	- True IDC complies with Thailand's personal data protection act BE 2562 (PDPA). - True IDC has processes in place to ensure security requirements and privacy requirements are taken into account in all stages of True IDC system development.	Cloud customers should develop systems and products based on a principle of security and privacy by design and industry best practices.
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Yes	Shared CSP and CSC	- True IDC complies with Thailand's personal data protection act BE 2562 (PDPA). - True IDC has processes in place to ensure security requirements and privacy requirements are taken into account in all stages of True IDC system development.	Cloud customers should develop systems and products based on a principle of security and privacy by design and industry best practices.
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	Yes	Shared CSP and CSC	- True IDC complies with Thailand's personal data protection act BE 2562 (PDPA). - True IDC has processes in place to ensure security requirements and privacy requirements are taken into account in all stages of True IDC system development. - Privacy by default setting of True IDC system is configured according to applicable privacy laws and regulations.	Cloud customers should configure privacy by default for their systems' settings according to all applicable laws and regulations.
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	Shared CSP and CSC	- True IDC complies with Thailand's personal data protection act BE 2562 (PDPA). - True IDC establishes the procedure for a data protection impact assessment (DPIA).	Cloud customers should 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.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification and complies with Thailand's personal data protection act BE 2562 (PDPA). - True IDC establishes procedures and technical measures to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope or agreement.	Cloud customers are responsible for the development and implementation of their own processes, procedures and technical measures to ensure any transfer of personal or sensitive data of thier applications or systems is protected from unauthorized access and only processed within thier scope as permitted by the respective laws and regulations.
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification and complies with Thailand's personal data protection act BE 2562 (PDPA). - True IDC establishes procedures and technical measures to enable data subjects to request access to, modify, or delete personal data according to Thailand's personal data protection act BE 2562 (PDPA). - Cloud customers who are data subject can initiate a request through the email address of True IDC customer service. Then True IDC will respond and handle as per request of data subject rights according to PDPA law and regulation.	- Cloud customers are the data controller so they should define, implement, and evaluate processes, procedures, and technical measures to enable data subjects to request access to, modify, or delete personal data in accordance with applicable laws and regulations.
DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification and complies with Thailand's personal data protection act BE 2562 (PDPA). - True IDC collects personal data for the purposes disclosed in the True IDC privacy policy statement.	- Cloud customers should 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.
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)?	N/A	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification and complies with Thailand's personal data protection act BE 2562 (PDPA). - True IDC Cloud located at True IDC data center in Thailand and True IDC cloud (IaaS) does not access cloud customer data so True IDC cloud is data processor for cloud customer data in terms storage.	- Cloud customers should define, implement, and evaluate processes, procedures, and technical measures for the transfer and sub-processing of personal data within the service supply chain in accordance with applicable laws and regulations.
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?	N/A	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification and complies with Thailand's personal data protection act BE 2562 (PDPA). - True IDC Cloud which is located at True IDC data center in Thailand does not access cloud customer data so True IDC cloud is data processor for cloud customer data in storage terms.	- Cloud customers should 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.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification and complies with Thailand's personal data protection act BE 2562 (PDPA). - True IDC establishes a system and software development policy which supports the organization' s application security. By this policy, production data shall be not used in test or development.	Cloud customers should ensure that they obtain authorization from data owner and manage the associated risks before replicating or using production data in non-production environments.
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification and complies with Thailand's personal data protection act BE 2562 (PDPA). - True IDC establishes data retention document to identify data retention period based on business requirements, applicable laws, and regulations. Once the data has been stored for a specified retention time, True IDC will securely dispose it following data classification.	Cloud customers should manage data retention, archiving, and deletion in accordance with their business requirements and applicable laws and regulations.
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification and complies with Thailand's personal data protection act BE 2562 (PDPA). True IDC establishes the policy and procedure for data classification and data handling throughout its lifecycle according to all applicable laws and regulations, standards, and risk level. - True IDC data is handled and protected sensitive data throughout its lifecycle.	Cloud customers should develop policies and procedures for the classification, protection, and handling of data including sensitive data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level.
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	- True IDC has passed the ISO/IEC 27001 certification and complies with Thailand's personal data protection act BE 2562 (PDPA). - True IDC has announced True IDC privacy policy on True IDC website to communicate with customers. - True IDC establishes cloud service agreement which identifies the retention, use and disclosure of customer information. - True IDC establishes the data subject rights procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
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	- True IDC has passed the ISO/IEC 27001 certification and complies with Thailand's personal data protection act BE 2562 (PDPA). - True IDC has announced True IDC privacy policy on True IDC website to communicate with customers. - True IDC establishes cloud service agreement which identifies the retention, use and disclosure of customer information. - True IDC will notify the customers in advance of any action in accordance with True IDC policies, procedures, applicable laws and regulations unless prohibited by law.	-
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	Yes	Shared CSP and CSC	- True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. - True IDC has data centers in Thailand which identifies location for True IDC cloud service. - True IDC provides daily VMs image back up for seven copies. - True IDC has a data inventory of sensitive and personal data and True IDC reviews and updates such inventory annually or significant changes.	- Cloud customers should define, implement, and evaluate processes, procedures, and technical measures to specify and document the physical locations of data processing and backup.
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	- True IDC has passed the ISO/IEC 27001 certification. - The information security policy and procedure are made available to all True IDC employees. All policy and procedures are reviewed annually or significant changes.	-
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. - The information security policy and procedure are made available to all True IDC employees. All policy and procedures are reviewed annually or significant changes.	-
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	True IDC has established the risk assessment and treatment Procedure as part of ISO/IEC 27001. Risk assessments are performed at least annually to ensure appropriate controls are in place to adequately manage the risk for our services. Risk assessment program includes risk management elements such as risk identification, risk analysis, risk evaluation, risk treatment and risk reporting.	-
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	True IDC policies and procedures are reviewed at least annually, or when significant changes occur.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Yes	CSP-owned	True IDC establishes the exception process for our services that aligns with the acceptable risk to the organization.	-
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. - True IDC implements and maintains the information security management plan which covers all CCM control domains.	-
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes	CSP-owned	- As part of the ISO/IEC 27001 certified, True IDC Compliance Committee Assignment are documented and approved by top management. - True IDC establishes a RACI matrix to assign an individual or team responsible for the processes, e.g. data center operation, Incident and Service Request Management, internal audit etc.	-
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Yes	CSP-owned	True IDC complies with the relevant standards, regulations, law, and privacy requirements which are applicable to the organization.	-
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	Yes	CSP-owned	- True IDC maintains contact in iDesk system. - True IDC cloud engineers are responsible to maintain the contact with special interested groups or processional associations to receive early warnings and advice regarding new threats, vulnerabilities, and news updates.	-
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	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the procedure for human resource security that including prior to employment, during employment and termination or change of employment. - True IDC performs background checks on new hires that consists of a review of criminal records, credit reviews, and verification of the information provided on the application including employment experience and educational credentials. - Third parties or contractors are either screened by project owner of True IDC, screen as a condition of contract, or verified as screened by the contractor following a True IDC approved screening process.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
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	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the procedure for human resource security that including prior to employment, during employment and termination or change of employment. - True IDC performs background checks on new hires that consists of a review of criminal records, credit reviews, and verification of the information provided on the application including employment experience and educational credentials. - Third parties or contractors are either screened by project owner of True IDC, screen as a condition of contract, or verified as screened by the contractor following a True IDC approved screening process.	-
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	-
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	True IDC has defined the acceptable use guidelines of information and assets in True IDC Acceptable Use Policy and related procedures. Theses documents are reviewed and updated annually or significant changes.	-
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	True IDC has defined the acceptable use guidelines of information and assets in True IDC Acceptable Use Policy and related procedures. Theses documents are reviewed and updated annually or significant changes.	-
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	True IDC has passed the ISO/IEC 27001 certification. True IDC security policies and procedures specify requirements for secure work areas and unattended equipment.	-
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes	CSP-owned	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	-
HRS-04.1	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	True IDC has a remote work and access procedure and practices of secure environment for working remotely.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	Yes	CSP-owned	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	-
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the procedure for human resource security that including offboarding procedure to ensure that all organizationally-owned assets are returned upon employee or contractor termination.	-
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the procedure for human resource security that defining roles and responsibilities concerning changes or termination in employment.	-
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Yes	CSP-owned	True IDC employees are required to sign employment agreements and non-disclosure agreements before granting users access to True IDC system, resources and assets.	-
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes	CSP-owned	True IDC employees are required to sign employment agreements and non-disclosure agreements. In additional, True IDC employees must acknowledge True IDC information security policies and procedures on e-learning system every year.	-
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the procedure for human resource security that defining information security roles and responsibilities.	-
HRS-10.1	Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?	Yes	CSP-owned	True IDC reviews the details of the non-disclosure agreement annually or significant changes.	-
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	True IDC provides security and privacy awareness training for all employees every year which includes, but is not limited to, e-learning system, email, meeting.	-
HRS-11.2	Are regular security awareness training updates provided?	Yes	CSP-owned	True IDC has process in place for security and privacy awareness training content reviews and refreshes annually.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	CSP-owned	True IDC provides security and privacy awareness training for all employees every year which includes, but is not limited to, e-learning system, email, meeting.	-
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	- True IDC has process in place for security and privacy awareness training content reviews and refreshes annually. - True IDC user access to sensitive organizational and personal data is based on least-privilege, need-to-know or need-to-use principles.	-
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	- True IDC provides security and privacy awareness training for all employees every year which includes, but is not limited to, e-learning system, email, meeting. - All True IDC personnel are made aware of their roles nad responsibilities through the use of multiple methods including on the job training, e-learning system, document management system (share file to announce policies, procedure and other documents releted the standard and organization).	-
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policies and procedures for identity and access management.	Cloud customers should develop policies and procedures for identity and access management of their environment.
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	Cloud customers should review and update policies and procedures at least annually.
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policies and procedures for strong password.	Cloud customers should develop policies and procedures for strong password.
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	Cloud customers should review and update policies and procedures at least annually.
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. - True IDC defines system identity information and access level based on need-to-know, need-to-use and least-privilege principles such as role-based access control and segregation of duties.	Cloud customers are responsible for managing, keeping and review system identity information and levels of access of their environment.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. - True IDC defines system identity information and access level based on need-to-know, need-to-use and least-privilege principles such as role-based access control and segregation of duties.	Cloud customers should apply the separation of duties principle when implementing or grant access rights for information systems of their environment.
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. - True IDC defines system identity information and access level based on need-to-know, need-to-use and least-privilege principles such as role-based access control and segregation of duties.	Cloud customers should apply the least privilege principle when implementing or when grant access rights for information systems of their environment.
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. - True IDC has processes in place which define the steps of user access provisioning. The system owners or admins consider user permissions based on need-to-know, need-to-use and least-privilege principles such as role-based access control and segregation of duties. After the system owners or admin grant user access rights, they will record the user permissions in user authoruzed matrix.	Cloud customers should define and implement a user access provisioning process which authorizes, records, and communicates access changes to their data and assets.
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	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. - When employees and other third parties change their status, such as termination or transfer, the user's logical access rights are revoked or changed the access rights following their new job functions. - True IDC periodically reviews access lists and removes access that is no longer required.	Cloud customers should revoke or change the access rights of their employees and other third parties who have terminated or changed their positions in a timely manner to comply with the access management control policies established by their company.
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	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. - True IDC periodically reviews access lists and removes access that is no longer required.	Cloud customers should periodically review and revalidation of user access to meet the least privilege and separation of duties. The frequency of access review or revalidation should be algned with the organizational risk tolerance.
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. - True IDC privileged accounts are strictly limited to business justification for use and segregated from accounts for general business use. - True IDC has processes in place which define the steps of user access provisioning. The system owners or admins consider user permissions based on need-to-know, need-to-use and least-privilege principles such as role-based access control and segregation of duties. After the system owners or admin grant user access rights, they will record the user permissions in user authoruzed matrix.	Cloud customers should develop, implement and evaluate policies, procedures and technical measures for the segregation of privileged access roles.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. - True IDC defines system identity information and access level based on need-to-know, need-to-use and least-privilege principles such as role-based access control and segregation of duties. - True IDC privileged accounts are strictly limited to business justification for use and segregated from accounts for general business use. - True IDC periodically reviews access lists and removes access that is no longer required.	Cloud customers should develop a grant user access process for privileged accounts and permissions and define the validity period.
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. - True IDC defines system identity information and access level based on need-to-know, need-to-use and least-privilege principles such as role-based access control and segregation of duties. - True IDC privileged accounts are strictly limited to business justification for use and segregated from accounts for general business use. - True IDC periodically reviews access lists and removes access that is no longer required.	Cloud customers should implement procedures to prevent the culmination of segregated privileged access such as monitoring for suspicious activity.
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?	No	Shared CSP and CSC	True IDC can not access CSCs' operating system after delivery.	Cloud customers are responsible for managing access to systems or applications or databases etc. within their cloud environment.
IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated?	Yes	CSP-owned	True IDC has the centralized log sysem. The collected log is in read-only mode and is restricted to only authorized staff to access the centralized log system.	-
IAM-12.2	Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. - Changes to configuration of logging system cannot be made without approval as per True IDC change management process.	-
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	Shared CSP and CSC	True IDC cloud staffs use the unique user accounts for access to True IDC cloud management system through Active Directory (AD).	Cloud customers should use the unique user accounts for access to their systems or applications.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
IAM-14.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?	Yes	Shared CSP and CSC	- True IDC has processes, procedures and technical measures for authenticating access to systems, application, and data assets. - True IDC cloud staffs shall access via VPN which used highly complex password to True IDC cloud management system and authenticate by AD user IDs. - True IDC provides two-factors authentication for some internal systems.	Cloud customers sholud develop identity authentication management mechanisms for their managed systems, applications, and data assets such as two-factors authentication mechanisms for privileged users or sensitive data access.
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Yes	Shared CSP and CSC	True IDC cloud system use digital certificate with RSA-2048 bit keys that issue by public PKI trusted CA.	Cloud customers should provide authentication for their systems by using digital certificates or alternatives that achieve an equivalent security level as required.
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the password management policy to enforce the secure management of password for True IDC systems.	Cloud customers should develop processes, procedures and technical measures for the secure management of passwords for their systems as per required.
IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes access control policies and procedures based on need-to-know, need-to-use and least-privilege principles. - True IDC periodically reviews access lists and removes access that is no longer required.	Cloud customers should develop processes, procedures and technical measures to verify the data and system functions access are properly authorized, defined, implemented and evaluated.
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	N/A	CSC-owned	- True IDC establishes the interoperability and portability procedure but True IDC cloud is not delivered API to cloud customers.	Cloud customers should develop policies and procedures for interoperability and portability including requirements of communication between application services.
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Yes	CSC-owned	- True IDC establishes the interoperability and portability procedure but True IDC cloud is not delivered API to cloud customers.	Cloud customers should develop policies and procedures for information processing interoperability.
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	N/A	CSC-owned	- True IDC establishes the interoperability and portability procedure but True IDC cloud is not delivered API to cloud customers.	Cloud customers should develop policies and procedures for application development portability.
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	N/A	CSC-owned	- True IDC establishes the interoperability and portability procedure but True IDC cloud is not delivered API to cloud customers and can not access customer data in customer tenent.	Cloud customers should develop policies and procedures for information/data exchange, usage, portability, integrity, and persistence.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	N/A	CSC-owned	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	Cloud customers should review and update policies and procedures at least annually.
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	No	CSC-owned	True IDC cloud is not delivered API to cloud customers.	- Cloud customers should periodically back up their cloud data and ensure that their backup data can be completely restored as required by their business. - Cloud customers shall inform True IDC customer service if they require their VMs image back up.
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	Yes	Shared CSP and CSC	- True IDC defines encryption protocols for the management. - Communication traffic of cloud customer's VM are following as below: 1) True IDC internal network does not encrypt physical connection. 2) True IDC allows private link connectivity to cloud customer's subnet. 3) True IDC provides IPSec connectivity between Cloud customer site and Cloud customer subnet incase cloud customer uses TIDC firewall as a service.	Cloud customers should encrypt their data to manage, import, and exit cloud services using standardized network protocols.
IPY-04.1	Do agreements include provisions specifying CSC data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Yes	Shared CSP and CSC	True IDC stores customer data in True IDC cloud for 14 days after contract termination, then True IDC will delete that data.	Cloud customers should remove all data that stored in True IDC cloud before service termination date.
IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the infrastructure and virtualization security management policies and procedures.	-
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
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 CSC	- True IDC complies with ISO/IEC 27001 and ISO/IEC20000-1. - True IDC establishes the demand and capacity management plan for all True IDC services. True IDC reports capacity in operation meeting and report to management. - True IDC continuously monitors services to meet the contractual and regulatory obligations.	Cloud customers should plan and monitor the availability, quality, and capacity of cloud resources based on their business requirements.
IVS-03.1	Are communications between environments monitored?	Yes	Shared CSP and CSC	- True IDC monitors availability of network link (24x7) between network infrastructure and cloud service. - True IDC monitors international banwidth usage for cloud customer. - True IDC provides username and password for True IDC cloud login for cloud customers. - True IDC cloud encrypted by wildcard certification and kept activity log.	- Cloud customers should monitor network communications of OS level and application level. - Cloud customers should create log server to keep their activity log for their applications.
IVS-03.2	Are communications between environments encrypted?	Yes	Shared CSP and CSC	- True IDC uses TLS to encrypt True IDC cloud. - True IDC network is not encrypted data at rest for cloud customers. - True IDC encrypts and authenticates uplink between True IDC and True IDC provider. - True IDC provides username and password for True IDC cloud login for cloud customers. - True IDC cloud encrypted by wildcard certification and kept activity log.	Cloud customers should encrypt communications between their environments.
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes	Shared CSP and CSC	- True IDC network communications are restricted to only authenticated and authorized connections. All access to True IDC informations and systems shall be authorized to protect against unauthorized access, disclosure and modification. - After True IDC provisions True IDC cloud for cloud customers, True IDC will send cloud configuration document to our customers for True IDC cloud access.	Cloud customers should restrict communications between environments to only authenticated and authorized connections, as justified by their business.
IVS-03.4	Are network configurations reviewed at least annually?	Yes	Shared CSP and CSC	True IDC network configurations and firewall rulesets are reviwed at least annually.	Cloud customers should review their network configuration at least annually.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Yes	Shared CSP and CSC	- True IDC has a network engineer team to manage, support and update network diagram and network equipment configuration. Any changes to network equipment must be followed the change management policy and procedure. - True IDC does not block any services, protocols and ports. But True IDC allows and defines services, protocols and ports for True IDC cloud staff to access True IDC cloud management. - True IDC establishes the security baseline and security hardening baseline documents e.g. new Windows Server, VMware Infrastructure, Firewall configuration, network switches and routers etc.	Cloud customers should define all allowed services, protocols, ports, and compensating controls that can support network configurations.
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	Shared CSP and CSC	- True IDC establishes the security baseline and security hardenin baseline documents e.g. new Windows Server, VMware Infrastructure, Firewall configuration, network switches and routers etc. - True IDC uses references such as NIST, the Center for Internet Security (CIS) and product proprietary to document for securing and hardenung network and system equipments.	Cloud customers are responsible for hardening of their guest OS.
IVS-05.1	Are production and non-production environments separated?	Yes	CSP-owned	Production and non-production of True IDC infrastructure are physically or logically separated.	-
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	Yes	Shared CSP and CSC	- True IDC user access is appropriately segregated, restricted and reviwed. - True IDC infrastructure and internal systems are separated from customer systems. - True IDC cloud for customers are logically segregated to prevent unauthorized access them.	- Cloud customers should isolate cloud resources based on their business requirements or services. - Cloud customers should consider hardware and software firewall options for security implementation.
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	Shared CSP and CSC	True IDC cloud engineer migrates customers' servers, services, applications, or data to True IDC cloud using OVF or OVA templates.	Cloud customers should export the VMs as OVF or OVA templates from the old cloud environment and send the encrypted templates to True IDC cloud engineer for cloud migration.
IVS-08.1	Are high-risk environments identified and documented?	Yes	CSP-owned	True IDC maintains and updates network architecture diagram.	-
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	Shared CSP and CSC	True IDC uses network next-generation firewall to prevent True IDC Cloud infrastructure.	- Cloud customers should consider to implement virtual firewall in option. Cloud customer should manage virtual firewall that is True IDC service and should configure host based on firewall and host base on IPS by themselves or using True IDC managed service.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policy and procedure for logging and monitoring.	Cloud customers should develop policies and procedures for logging and monitoring of their environment.
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	Cloud customers should review and update policies and procedures at least annually.
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policy and procedure for logging and monitoring. - True IDC logs are stored in centralized log systems that restricted to authorized personnel only. True IDC keeps logs at least period as defined by regulation.	Cloud customers should develop policies, procedures and technical measures to ensure the security of logs and meet their identidication retention periods.
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes	Shared CSP and CSC	- True IDC employs a monitoring and alerting infrstructure allowing for the identification of security-related events. A system can be defined and implemented to generate alerts to responsible stakeholders. - True IDC customer service team performs 24x7 monitoring for system availability and support for incident management.	Cloud customers are responsible for employing a security monitoring and alerting of their applications to identify events that may cause security incidents.
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	Yes	Shared CSP and CSC	- True IDC employs a monitoring and alerting infrstructure allowing for the identification of security-related events. A system can be defined and implemented to generate alerts to responsible stakeholders. - True IDC customer service team performs 24x7 monitoring for system availability and support for incident management.	Cloud customers should notify to responsible stakeholders based on security events and their corresponding metrics of applications.
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policy and procedure for logging and monitoring. - True IDC logs are stored in centralized log systems that restricted to authorized personnel only. The authorized personnel who access the centralized log systems must be granted access with unique user account.	Cloud customers should ensure that the authorized personnel have access to audit logs and that access is recorded to ensure unique access accountability.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Yes	Shared CSP and CSC	- True IDC employs a monitoring and alerting infrstructure allowing for the identification of security-related events. A system can be defined and implemented to generate alerts to responsible stakeholders. - True IDC customer service team performs 24x7 monitoring for system availability and support for incident management. - True IDC establishes the policy and procedure for security incident management, e-discovery, and cloud forensics to manage and response to security incident in a timely manner on detected anomalies.	Cloud customers should continuously monitor security audit logs to detect activity outside of typical or expected patterns and take appropriate and timely actions on detected anomalies.
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes	Shared CSP and CSC	- True IDC employs a monitoring and alerting infrstructure allowing for the identification of security-related events. A system can be defined and implemented to generate alerts to responsible stakeholders. - True IDC customer service team performs 24x7 monitoring for system availability and support for incident management. - True IDC establishes the policy and procedure for security incident management, e-discovery, and cloud forensics to manage and response to security incident in a timely manner on detected anomalies.	Cloud customers should continuously monitor security audit logs to detect activity outside of typical or expected patterns and take appropriate and timely actions on detected anomalies.
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. - True IDC uses the Network Time Protocol (NTP) to synchronize with the reference time source. This ensure that all relevant information processing systems have a reliable time source.	Cloud customers are responsible to use a reliable time source across all their relevant information processing systems.
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policy and procedure for logging and monitoring. - True IDC defines logging requirements for information system events. Logged events include information such as identity of users (user ID), timestamp and the action that was taken.	Cloud customers should define logging scope of their applications or systems within customer environment.
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	Yes	Shared CSP and CSC	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	Cloud customers should review and update policies and procedures at least annually.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
LOG-08.1	Are audit records generated, and do they contain relevant security information?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policy and procedure for logging and monitoring. - True IDC defines logging requirements for information system events. Logged events include information such as identity of users (user ID), timestamp and the action that was taken. - True IDC has the centralized log sysem. The collected log is in read-only mode and is restricted to only authorized staff to access the centralized log system.	Cloud customers should ensure that the stored audit logs contain the relevant security information.
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policy and procedure for logging and monitoring. - True IDC logs are stored in centralized log systems that restricted to authorized personnel only and set in read-only mode. The authorized personnel who access the centralized log systems must be granted access with unique user account.	Cloud customers should ensure that audit logs of their information systems are not accessed, modified or deleted without authorization.
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	Yes	Shared CSP and CSC	- True IDC cloud (IaaS) does not access cloud customer data - Cryptographic keys are revoked and removed before the end of its established cryptoperiod when key is compromised or key is no longer part of True IDC. Incident ticket will be created to issue new certificate and perform according to change management process.	Cloud customers should develop the monitoring and internal reporting policies, processes and procedures to control accross the encryption and key management lifecycle.
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Yes	Shared CSP and CSC	True IDC tracks and reports all key and cryptography detail and status from True IDC key management record.	Cloud customers should develop the monitoring and internal reporting policies, processes and procedures to control accross the encryption and key management lifecycle.
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. - True IDC provides the physical security perimeters to safeguard personnel, data, and information systems such as CCTV, access card, mantraps, access system, security guards and barriers which are used to monitor ingress and egress at the various physical security zones in a data center and to ensure that only authorized personnel are allowed access. - True IDC data center staffs are responsible for reviewing data center access records on monthly basis i.e. access control system log and CCTV log.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the process and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the relavant stakeholders. - True IDC customer service team performs 24x7 monitoring for system availability and support for incident management.	Cloud customers should develop processes and technical measures to report anomalies and failures of the monitoring system for their environment and provide notification to the related stakeholders immediately.
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. - True IDC customer service team performs 24x7 monitoring for system availability and support for incident management. True IDC has defined the incident escalation to notify the responsible stakeholders based on incident response matrix.	Cloud customers should develop processes and technical measures to report anomalies and failures of the monitoring system for their environment and provide notification to the related stakeholders immediately.
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	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policy and procedure for security incident management, e-discovery, and cloud forensics.	Cloud customers should develop policies and procedures for security incident management, e-discovery, and cloud forensics of their environment.
SEF-01.2	Are policies and procedures reviewed and updated annually?	Yes	Shared CSP and CSC	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	Cloud customers should review and update policies and procedures at least annually.
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policy and procedure for security incident management, e-discovery, and cloud forensics. - True IDC customer service team performs 24x7 monitoring for incident management.	Cloud customers should develop policies and procedures for security incident management, e-discovery, and cloud forensics of their environment.
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Yes	Shared CSP and CSC	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	Cloud customers should review and update policies and procedures at least annually.
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	- True IDC implements the business continuity plans and incident response plans for our services, reviews and excercises or tests them annually. - True IDC informs customers when incident occurs and has impact to them.	-
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	- True IDC implements the business continuity plans and incident response plans for our services, reviews and excercises or tests them annually.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
SEF-05.1	Are information security incident metrics established and monitored?	Yes	CSP-owned	- True IDC customer service team performs 24x7 monitoring for incident management. - True IDC summarizes and analyzes the quarterly security incident report to determine volume of security incidents, incidents by product etc.	-
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Yes	CSP-owned	- True IDC has passed the ISO/IEC 27001 certification. True IDC has the incident management procedure to support the assessment of security-related events that define the incident severity and security impact.	-
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes	CSP-owned	True IDC security incident notifications are made available to potential impacted stakeholders in accordance with policies, procedures and applicable laws and regulations.	-
SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	Yes	CSP-owned	True IDC security breaches and assumed security breaches are reported following BCP call tree, call tree list or related regulator. Incase security breaches and assumed security breaches affect to the customers, True IDC will report the related customers in line with incident management procedure.	-
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Yes	CSP-owned	True IDC maintains points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities. Contact details are documented in True IDC documentation or system.	-
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	True IDC establishes the shared security responsibility model (SSRM) for True IDC cloud that including roles and responsibilities between True IDC and cloud customer.	-
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Yes	CSP-owned	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	-
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes	CSP-owned	- True IDC establishes the shared security responsibility model (SSRM) for True IDC cloud that including roles and responsibilities between True IDC and cloud customer. - True IDC has a supplier management procedure to manage supplier or vendor from the selection process to the service delivery.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	Yes	CSP-owned	- True IDC establishes the shared security responsibility model (SSRM) for True IDC cloud that including roles and responsibilities between True IDC and cloud customer. - SSRM guidance of True IDC is carried out the certified standards e.g. ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc.	-
STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	Yes	CSP-owned	True IDC defines CAIQ v4 that including the shared ownership and applicability of all CSA CCM controls.	-
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Yes	CSP-owned	- True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes. - CAIQ v4 is a part of True IDC documentation so True IDC reviews and validates annually.	-
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes	Shared CSP and CSC	- True IDC undergoes accredited certification audits yearly for information security management (ISO/IEC 27001) and CSA STAR to assess the efficiency and effectiveness of implemented security controls. - The portions of the SSRM that the organization is responsible for are implemented, operated, audited, and assessed. True IDC conducts the internal audit at least annually for each certified standards.	Cloud customers should implement, operate, and audit or assess the portions of the SSRM which their organizations are responsible for.
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	Yes	CSP-owned	True IDC maintains an inventory of supplier relationships. List of suppliers are reviewed and updated periodically.	-
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Yes	CSP-owned	True IDC periodically reviews the risk factors associated with all True IDC services within the supply chain. This includes third-party suppliers and their associated risks. Risk assessments are performed at least annually to ensure appropriate controls are in place to adequately manage the risk for our services.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
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	True IDC cloud service agreement contains the following terms: - Scope, characteristics, and location of business relationship and services - Information security requirements (including SSRM) - Change management process - Logging and monitoring capability - Incident management and communication procedures - Right to audit - Service termination - Interoperability and portability requirements -> data import & export - Data privacy	-
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	N/A	CSP-owned	True IDC does not have supply chain agreements with True IDC cloud customers.	-
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	- True IDC assigns a standard compliance team to conduct internal audit at least annually for each certified standards. - True IDC develops and maintains an internal audit program to assess the conformanace and effectiveness of standards, policies, procedures, and SLA activities. - True IDC conducts independent audit on a annual basis according to internal audit program and external audit plan.	-
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	- True IDC complies with ISO/IEC 27001 so all True IDC policies that require all supplly chain True IDC to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards. - True IDC has a supplier management procedure to manage supplier or vendor from the selection process to the service delivery.	-
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	Yes	CSP-owned	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	-

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	Yes	CSP-owned	- True IDC has a supplier management procedure to manage supplier or vendor from the selection process to the service delivery. - True IDC periodically reviews the risk factors associated with all True IDC services within the supply chain. This includes third-party suppliers and their associated risks. Risk assessments are performed at least annually to ensure appropriate controls are in place to adequately manage the risk for our services.	-
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	Shared CSP and CSC	Policies and procedures have been established and implemented to vulnerability scan and patch management for True IDC cloud.	Cloud customers are responsible for the development and implementation of their own policies and procedures to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation for their OS and application on True IDC cloud or customer environment.
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	Cloud customers should review and update policies and procedures at least annually.
TVM-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	True IDC has policies and procedures in place to protect against malware on all organizationally-owned assets (computers, notebooks and servers).	Cloud customers are responsible for the development and implementation of their own policies and procedures to protect managed assets from malware.
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	Cloud customers should review and update policies and procedures at least annually.
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	Shared CSP and CSC	- Policies and procedures have been established and implemented to vulnerability scan and patch management for True IDC cloud. - True IDC has defined the vulnerability scan schedule for each system including vCenter for True IDC cloud and has defined response times to vulnerability identifications based on severity level of vulnerability (critical, high, medium and low).	Cloud customers should define, implement, and evaluate processes, procedures, and technical measures to enable scheduled and emergency responses to vulnerability identifications based on the identified risk.
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	Shared CSP and CSC	True IDC sets anti-malware on company-owned computers (PCs or laptops) to be update hourly and server to be updated daily.	Cloud customers should define, implement, and evaluate processes, procedures, and technical measures on weekly or more frequent basis to update detection tools, threat signatures, and compromise indicators.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
TVM-05.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the organization's vulnerability management policy)?	Yes	Shared CSP and CSC	True IDC cloud is updated according to security patch management.	Cloud customers are responsible for the development and implementation of their own processes, procedures and technical measures to identify vulnerabilities and updates for applications that using third-party or open source libraries.
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	No	CSC-owned	-	Cloud customers should perform penetration testing on customer instances (OS, services or applications).
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Yes	Shared CSP and CSC	- Policies and procedures have been established and implemented to vulnerability scan and patch management for True IDC cloud. Patch checking is performed daily and patch updating is performed according to the severity level and response times.	Cloud customers should perform vulnerability detection on their organizationally managed assets at least monthly.
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	Yes	Shared CSP and CSC	- Policies and procedures have been established and implemented to vulnerability scan and patch management for True IDC cloud. - Vulnerability remediation is prioritized based on the Common Vulnerability Scoring System (CVSS) score.	Cloud customers should prioritize remediation for identified vulnerabilities based on their risk appetite.
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes	Shared CSP and CSC	- Policies and procedures have been established and implemented to vulnerability scan and patch management for True IDC cloud. - True IDC security engineer team yearly scans vulnerabilities. If a vulnerability is detected on True IDC cloud, this team will record and notify the related engineer team to fix or patch this vulnerability. After the vulnerabilties are fixed, True IDC security engineer team will verify the fixing results.	Cloud customers are responsible for the development and implementation of their own policies and procedures to track and report identified vulnerabilities and remediation activities including notifying stakeholders.
TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Yes	Shared CSP and CSC	- Policies and procedures have been established and implemented to vulnerability scan and patch management for True IDC cloud. - True IDC security engineer team yearly scans vulnerabilities. If a vulnerability is detected on True IDC cloud, this team will record and notify the related engineer team to fix or patch this vulnerability. After the vulnerabilties are fixed, True IDC security engineer team will verify the fixing results.	Cloud customers should establish metrics for vulnerability identification and remediation, and monitor and report that metrics at defined intervals.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policy and procedure for mobile security to manage True IDC owned endpoints and BYOD. - True IDC does not permit BYOD to access True IDC cloud management system.	Cloud customers should develop policies and procedures for all their endpoints.
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC	True IDC has passed the certification of ISO/IEC 27001, ISO/IEC 20000-1, ISO27799, CSA STAR etc. True IDC reviews and updates related policies and procedures annually or significant changes.	Cloud customers should review and update policies and procedures at least annually.
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	Shared CSP and CSC	True IDC defines internal software and application whitelist to allow True IDC endpoints to install. Incase softwares or applications are not in such list, True IDC users must request True IDC security engineer team to consider the related risk prior installation.	Cloud customers should develop a list of services, applications and application stores for accessing or storing their organization-managed data.
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	Yes	Shared CSP and CSC	- True IDC has defined the internal software and application whitelist to allow True IDC endpoints to install. Incase softwares or applications are not in such list, True IDC users must request True IDC security engineer team to consider the related risk prior installation.	Cloud customers should develop and implement processes to verify their endpoint device are compatible with operating systems and applications.
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. - True IDC assets are registered and assigned ownership in asset inventory system including True IDC endpoints which used to store and access company data.	Cloud customers should maintain an inventory of all endpoints used to store and access company data.
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	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. True IDC establishes the policy and procedure for mobile security to manage True IDC owned endpoints and BYOD. - True IDC has established the security baseline for PC/Notebook and requied BYOD to install MS Intune. - True IDC does not permit BYOD to access True IDC cloud management system. - True IDC has processes in place which define the steps of user access provisioning. The system owners or admins consider user permissions based on need-to-know, need-to-use and least-privilege principles such as role-based access control and segregation of duties. After the system owners or admin grant user access rights, they will record the user permissions in user authoruzed matrix. True IDC periodically reviews access lists and removes access that is no longer required.	Cloud customers should develop and implement processes, procedures, and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process their organizational data.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. - True IDC has configured all True IDC endpoints for automatic screen lock after a pre-defined period of time.	Cloud customers should configure all thier relevant interactive-use endpoints to require an automatic lock screen.
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	Yes	Shared CSP and CSC	- Change to endpoint operating systems, patch levels, and/or applications of True IDC endpoints (e.g. server, hypervisor, database storage, etc.) must be operated through change management process. - All True IDC endpoints must be updated in the event of the release of updates that include security fixes.	Cloud customers should manage changes to their endpoint operating systems, patch levels, and/or applications according to their change management process.
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	Yes	Shared CSP and CSC	True IDC use storage encryption for True IDC endpoints to protect information from unauthorized disclosure.	Cloud customers should manage their endpoints with storage encryption.
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification. - True IDC has configured all True IDC endpoints with anti-malware and users cannot change the setting. - True IDC has educated and trained employees on security awareness that including malware protection in this training plan.	Cloud customers should deploy anti-malware detection and prevention technology and services for their endpoints.
UEM-10.1	Are software firewalls configured on managed endpoints?	Yes	Shared CSP and CSC	- True IDC has configured all True IDC endpoints with properly configured software firewalls and users cannot change the setting.	Cloud customers should configure the software firewalls on their endpoints.
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	N/A	CSC-owned	- True IDC has passed the ISO/IEC 27001 certification and complies with Thailand's personal data protection act BE 2562 (PDPA). - True IDC cloud (IaaS) does not access cloud customer data so cloud customers are responsible for deploying Data Loss Prevention (DLP) technologies and setting rules per their risk assessement. - True IDC employees sign non-disclosure agreements and have access to the system only for employees involved in their roles and responsibilities.	Cloud customers are responsible for deploying Data Loss Prevention (DLP) technologies and setting rules per their risk assessement.
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	No	CSC-owned	- True IDC does not permit BYOD to access True IDC cloud management system. - True IDC cloud management can perform by True IDC notebook/ PC at anywhere.	Cloud customers are responsible for enabling remote geo-location capabilities for all managed mobile endpoints which access their environment.

Question ID	Consensus Assessments Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	N/A	CSC-owned	- True IDC cloud (IaaS) does not access cloud customer data. - True IDC does not permit BYOD to access True IDC cloud management system. - True IDC establishes the procedures and technical measures for enabling the deletion of company data remotely on managed mobile devices or BYOD.	Cloud customers should enable the function of remotely deleting their organizational data from managed endpoint devices.
UEM-14.1	Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?	Yes	Shared CSP and CSC	- True IDC has passed the ISO/IEC 27001 certification and complies with Thailand's personal data protection act BE 2562 (PDPA). - True IDC does not allow third-party endpoints to access True IDC cloud assets.	Cloud customers should develop processes, procedures and technical measures to maintain proper security of third-party endpoints with access to their organizational assets.