Microsoft Azure (All-Up), Dynamics 365 and Other Online Services
ISO/IEC 27001:2013, 27018:2019, 27701:2019
Information Security and Privacy Management Systems - Statement of Applicability

Statement of Applicability (Dated 2/29/2020) v2020.01

ISO/IEC 27001:2013 Clause Number	ISO/IEC 27001:2013 Control Objectives	ISO/IEC 27001:2013 Controls	ISO/IEC 27001:2013 Control Title	ISO 27001:2013 Control	Status	Applicable Yes / No
ISO 27001 Annex A Controls						
A.5 INFORMATION SECURITY POLICIES						
A.5.1 Information security policies	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	A.5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	Implemented	Yes
		A.5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	Implemented	Yes
A.6 ORGANIZATION OF INFORMATION SECURITY						

A.6.1 Internal Organization	To establish a management framework to initiate and control the implementation and operation of information security within the organization.	A.6.1.1	Information security roles and responsibilities	All information security responsibilities shall be clearly defined and allocated.	Implemented	Yes
		A.6.1.2	Segregation of Duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Implemented	Yes
		A.6.1.3	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	Implemented	Yes

		A.6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	Implemented	Yes
		A.6.1.5	Information security in project managemen t	Information security shall be addressed in project management, regardless of the type of the project.	Implemented	Yes
A.6.2 Mobile Devices and teleworking	To ensure the security of teleworking and use of mobile devices.	A.6.2.1	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	Implemented	Yes
		A.6.2.2	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	Implemented	Yes
A.7 Human Resources Security						

A.7.1 Prior to employment	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.	A.7.1.1	Screening	Background verification checks for all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Implemented	Yes
		A.7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	Implemented	Yes
A.7.2 During employment	To ensure that employees and contractors are aware of and fulfil their information security responsibilities	A.7.2.1	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	Implemented	Yes
		A.7.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness training and regular updates in organizational policies and procedures, as	Implemented	Yes

				relevant for their job function.		
		A.7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Implemented	Yes
A.7.3 Termination and change of employment	To protect the organization's interests as part of the process of changing or terminating employment.	A.7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	Implemented	Yes
A.8 ASSET MANAGEMENT						
A.8.1 Responsibility for assets	To identify organizational assets and define appropriate protection responsibilities.	A.8.1.1	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Implemented	Yes
		A.8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned.	Implemented	Yes

		A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information processing facilities shall be identified, documented and implemented	Implemented	Yes
		A.8.1.4	Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Implemented	Yes
A.8.2 Information classification	To ensure that information receives the appropriate level of protection in accordance with its importance to the organization.	A.8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.	Implemented	Yes
		A.8.2.2	Labelling of information	An appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Implemented	Yes
		A.8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Implemented	Yes

A.8.3 Media handling	To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.	A.8.3.1	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Implemented	Yes
		A.8.3.2	Disposal of media	Media shall be disposed of securely and safely when no longer required, using formal procedures.	Implemented	Yes
		A.8.3.3	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Implemented	Yes
A.9 ACCESS CONTROL						
A.9.1 Business requirement of access control	To limit access to information and information processing facilities.	A.9.1.1	Access control policy	An access control policy shall be established, documented, and reviewed based on business and information security requirements.	Implemented	Yes
		A.9.1.2	Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Implemented	Yes

A.9.2 User access management	To ensure authorized user access and to prevent unauthorized access to systems and services.	A.9.2.1	User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Implemented	Yes
		A.9.2.2	User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Implemented	Yes
		A.9.2.3	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	Implemented	Yes
		A.9.2.4	Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	Implemented	Yes
		A.9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals.	Implemented	Yes

		A.9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Implemented	Yes
A.9.3 User responsibilities	To make users accountable for safeguarding their authentication information.	A.9.3.1	Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.	Implemented	Yes
A.9.4 System and application access control	To prevent unauthorized access to systems and applications.	A.9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	Implemented	Yes
		A.9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Implemented	Yes
		A.9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality password.	Implemented	Yes

		A.9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Implemented	Yes
		A.9.4.5	Access control to program source code	Access to program source code shall be restricted.	Implemented	Yes
A.10 CRYPTOGRAPHY						
A.10.1 Cryptographic controls	To ensure the proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.	A.10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	Implemented	Yes
		A.10.1.2	Key Management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Implemented	Yes
A.11 PHYSICAL AND ENVIRONMENTAL SECURITY						
A.11.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.	A.11.1.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Implemented	Yes

		A.11.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Implemented	Yes
		A.11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	Implemented	Yes
		A.11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	Implemented	Yes
		A.11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and applied.	Implemented	Yes
		A.11.1.6	Delivering and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	Implemented	Yes
A.11.2 Equipment	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	A.11.2.1	Equipment sitting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Implemented	Yes

		A.11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Implemented	Yes
		A.11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	Implemented	Yes
		A.11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Implemented	Yes
		A.11.2.5	Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	Implemented	Yes
		A.11.2.6	Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Implemented	Yes
		A.11.2.7	Secure disposal or re-use of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Implemented	Yes

		A.11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	Implemented	Yes
		A.11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	Implemented	Yes
A.12 OPERATIONS SECURITY						
A.12.1 Operational procedures and responsibilities	To ensure correct and secure operations of information processing facilities.	A.12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.	Implemented	Yes
		A.12.1.2	Change management	Changes to organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Implemented	Yes
		A.12.1.3	Capacity management	The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.	Implemented	Yes

		A.12.1.4	Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	Implemented	Yes
A.12.2 Protection from malware	To ensure that information and information processing facilities are protected against malware.	A.12.2.1	Controls against malware	Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Implemented	Yes
A.12.3 Back-up	To protect against the loss of data.	A.12.3.1	Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Implemented	Yes
A.12.4 Logging and Monitoring	TO record events and generate evidence	A.12.4.1	Event Logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Implemented	Yes
		A.12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Implemented	Yes

		A.12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Implemented	Yes
		A.12.4.4	Clock Synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.	Implemented	Yes
A.12.5 Control Of Operational software	To ensure the integrity of operational systems	A.12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	Implemented	Yes
A.12.6 Technical vulnerability management	To prevent exploitation of technical vulnerabilities.	A.12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Implemented	Yes

		A.12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	Implemented	Yes
A.12.7 Information systems audit considerations	To minimize the impact of audit activities on operational systems.	A.12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.	Implemented	Yes
A.13 COMMUNICATIONS SECURITY						
A.13.1 Network security management	To ensure the protection of information in networks and its supporting information processing facilities.	A.13.1.1	Network controls	Networks shall be managed and controlled to protect information in systems and applications.	Implemented	Yes
		A.13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Implemented	Yes

		A.13.1.3	Segregation of networks	Groups of information services, users, and information systems shall be segregated on networks.	Implemented	Yes
A.13.2 Information transfer	To maintain the security of information transferred within an organization and with any external entity.	A.13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Implemented	Yes
		A.13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	Implemented	Yes
		A.13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	Implemented	Yes
		A.13.2.4	Confidentiality or non-disclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	Implemented	Yes
A.14 SYSTEM ACQUISITION, DEVELOPMENT						

AND MAINTENANCE						
A.14.1 Security requirements of information systems	To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.	A.14.1.1	Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Implemented	Yes
		A.14.1.2	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Implemented	Yes
		A.14.1.3	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	Implemented	Yes
A.14.2 Security in development and support processes.	To ensure that information security is designed and implemented within the development	A.14.2.1	Secure development policy	Rules for the development of software and systems shall be established and applied to developments	Implemented	Yes

	lifecycle of information systems.			within the organization.		
		A.14.2.2	System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	Implemented	Yes
		A.14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Implemented	Yes
		A.14.2.4	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Implemented	Yes
		A.14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system	Implemented	Yes

				implementation efforts.		
		A.14.2.6	Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Implemented	Yes
		A.14.2.7	Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	N/A	N/A
		A.14.2.8	System security testing	Testing of security functionality shall be carried out during development.	Implemented	Yes
		A.14.2.9	System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Implemented	Yes
A.14.3 Test data	To ensure the protection of data used for testing.	A.14.3.1	Protection of test data	Test data shall be selected carefully, protected and controlled.	Implemented	Yes
A.15 SUPPLIER RELATIONSHIPS						
A.15.1.1 Information security in supplier relationships	To ensure protection of the organization's assets that is accessible by suppliers	A.15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the	Implemented	Yes

				organization's assets shall be agreed with the supplier and documented.		
		A.15.1.2	Addressing security within supplier agreement	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	Implemented	Yes
		A.15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Implemented	Yes
A.15.2 Supplier service delivery management	To maintain an agreed level of information security and service delivery in line with supplier agreements.	A.15.2.1	Monitoring and review of supplier services	Organizations shall be regularly monitor, review and audit supplier service delivery.	Implemented	Yes
		A.15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking	Implemented	Yes

				account of the criticality of business information, systems and processes involved and re-assessment of risks.		
A.16 INFORMATION SECURITY INCIDENT MANAGEMENT						
A.16.1 Management of information security incidents and improvements	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Implemented	Yes
		A.16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	Implemented	Yes
		A.16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	Implemented	Yes
		A.16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information	Implemented	Yes

				security incidents.		
		A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Implemented	Yes
		A.16.1.6	Learning from information security incidents	Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Implemented	Yes
		A.16.1.7	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information which can serve as evidence.	Implemented	Yes
A.17 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT						
A.17.1 Information security continuity	Information security continuity shall be embedded in the organization's business continuity management systems.	A.17.1.1	Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Implemented	Yes

		A.17.1.2	Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Implemented	Yes
		A.17.1.3	Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	Implemented	Yes
A.17.2 Redundancies	To ensure availability of information processing facilities.	A.17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Implemented	Yes
A.18 COMPLIANCE						
A.18.1 Compliance with legal and contractual requirements	To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.	A.18.1.1	Identification applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	Implemented	Yes

		A.18.1.2	Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and use of proprietary software products.	Implemented	Yes
		A.18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.	Implemented	Yes
		A.18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Implemented	Yes
		A.18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Implemented	Yes
A.18.2 Information security reviews	To ensure that information security is implemented and operated in accordance with the organizational	A.18.2.1	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control	Implemented	Yes

	policies and procedures.			objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes occur.		
		A.18.2.2	Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Implemented	Yes
		A.18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	Implemented	Yes
Azure Added Privacy and Data Protection Controls (NOT PART OF ISO 27001 Annex A Controls)						
A.19 PRIVACY						
A.19.1 Information system privacy considerations	**A.19.1 Information system privacy considerations** **Control objective: to ensure compliance of systems with divisional privacy requirements.**	A.19.1.1	Privacy Reviews	Every major release of Azure Features must go through a privacy review	Implemented	Yes
		A.19.1.2	Illegal content or usage	All Azure Features must be able to respond to illegal content or use, including notices for copyrighted material.	Implemented	Yes
		A.19.1.3	Privacy Disclosure	All Azure Features must conform to the Azure Privacy Statement or obtain approval from the Privacy Manager and	Implemented	Yes

				CELA for an alternative Privacy Statement		
		A.19.1.4	Terms of Use	All Azure Features must comply with the Azure agreement terms or obtain approval from CELA for an alternative contract	Implemented	Yes
		A.19.1.5	Privacy Statement updates	Any revision to the Azure Privacy Statement must be approved by Privacy Manager and the CELA contact.	Implemented	Yes
		A.19.1.6	Customer privacy inquires	All Azure Features must have procedures for escalation of privacy inquires and requests from customers.	Implemented	Yes
		A.19.1.7	Customer control of end user data	All Azure Features must allow Customers to control end user access to customer data.	Implemented	Yes
		A.19.1.8	Cookie inventory	All Azure Features must maintain an inventory of cookies and their functions, designed to ensure that no cookies are utilized in an unauthorized manner.	Implemented	Yes
		A.19.1.9	Privacy Incident Response	All Azure Features must follow the Azure Privacy Incident Response plan or obtain approval from the Privacy Manager and CELA for an alternative plan.	Implemented	Yes

A.20 CUSTOMER DATA PROTECTION						
A.20.1 Information system customer data protection considerations	**A.20.1 Information system customer data protection considerations** **Control objective: to ensure compliance of systems with EU Model Clauses and related agreements and regulations.**	A.20.1.1	Reproduction of customer data	Azure Personnel must not reproduce Customer Data on removable media or paper without Customer or CELA approval	Implemented	Yes
		A.20.1.2	Customer data transfer over public networks	Azure must not transmit non-public Customer Data over public networks without encryption	Implemented	Yes
		A.20.1.3	Identify personnel accessing customer data systems	Azure must identify personnel who are authorized to access systems that contain Customer Data	Implemented	Yes
ISO 27018 Annex A Controls (Appended to current SOA as part of the PII and Data Protection Control review)						
A.21 - 27018 CONSENT AND CHOICE						
A.21.1	Obligation to co-operate regarding PII principals' rights	A.1.1	Obligation to co-operate regarding PII principals' rights	The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfill their obligation to facilitate the exercise of PII principals' rights to access, correct, and/or erase PII pertaining to them.	Implemented	Yes
A.22 - 27018 PURPOSE LEGITIMACY						

AND SPECIFICATION						
A.22.1	Public Cloud PII controller's purpose	A.2.1	Public Cloud PII controller's purpose	PII to be processed under a contract should not be processed for any purpose independent of the instructions of the cloud service customer.	Implemented	Yes
A.22.2	Public Cloud PII processor's commercial use	A.2.2	Public Cloud PII processor's commercial use	PII processed under a contract should not be used by the public cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.	Implemented	Yes
A.23 - 27018 DATA MINIMIZATION						
A.23.1	Secure erasure of temporary files	A.4.1	Secure erasure of temporary files	Temporary files and documents are erased or destroyed within a specified, documented period.	Implemented	Yes
A.24 - 27018 USE, DISCLOSURE and RETENTION INFORMATION						

A.24.1	PII Disclosure Notification	A.5.1	PII Disclosure Notification	The contract between the public cloud PII processor and the cloud service customer should require the public cloud PII processor to notify the cloud service customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited.	Implemented	Yes
A.24.2	Recording of PII Disclosures	A.5.2	Recording of PII Disclosures	Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time.	Implemented	Yes
A.25 - 27018 OPENNESS, TRANSPARENCY AND NOTICE						
A.25.1	Disclosure of Sub-Contracted PII processing	A.7.1	Disclosure of Sub-Contracted PII processing	The use of sub-contractors by the public cloud PII processor to process PII should be disclosed to the relevant PII cloud service customers before their use.	Implemented	Yes
A.26 - 27018 ACCOUNTABILITY						

A.26.1	Notification of a data breach involving PII	A.9.1	Notification of a data breach involving PII	The public cloud PII processor should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII, or unauthorized access to processing equipment or facilities resulting in loss, disclosure, or alteration of PII.	Implemented	Yes
A.26.2	Retention period for administrative security policies and guidelines	A.9.2	Retention period for administrative security policies and guidelines	Copies of security policies and operating procedures should be retained for a specified, documented period upon replacement (including updating).	Implemented	Yes
A.26.3	PII Return, transfer and disposal	A.9.3	PII Return, transfer and disposal	The public cloud PII processor should have a policy in respect of the return, transfer, and/or disposal of PII and should make this policy available to the cloud service customer.	Implemented	Yes
A.27 - 27018 INFORMATION SECURITY						
A.27.1	Confidentiality or non-disclosure agreements	A.10.1	Confidentiality or non-disclosure agreements	Individuals under the public cloud PII processor's control with access to PII should be subject to a confidentiality obligation.	Implemented	Yes
A.27.2	Restriction of creation of hard copy material	A.10.2	Restriction of creation of hard copy material	The creation of hardcopy material displaying PII	Implemented	Yes

				should be restricted.		
A.27.3	Control and logging of data restoration	A.10.3	Control and logging of data restoration	There should be is a procedure for, and a log of, data restoration efforts.	Implemented	Yes
A.27.4	Protecting data on storage media leaving the premises	A.10.4	Protecting data on storage media leaving the premises	PII on media leaving the organization's premises should be subject to an authorization procedure and should not accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).	Implemented	Yes
A.27.5	Use of unencrypted storage media	A.10.5	Use of unencrypted storage media	Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented.	Implemented	Yes
A.27.6	Encryption of PII transmitted over public networks	A.10.6	Encryption of PII transmitted over public networks	PII that is transmitted over public data transmission networks should be encrypted prior to transmission.	Implemented	Yes
A.27.7	Secure disposal of hardcopy materials	A.10.7	Secure disposal of hardcopy materials	Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.	Implemented	Yes

A.27.8	Unique use of identifiers	A.10.8	Unique use of identifiers	If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication and authorization purposes.	Implemented	Yes
A.27.9	Records of authorized users	A.10.9	Records of authorized users	An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained.	Implemented	Yes
A.27.10	Identifier Management	A.10.10	Identifier Management	De-activated or expired user IDs should not be granted to other individuals.	Implemented	Yes
A.27.11	Contract Measures	A.10.11	Contract Measures	Contracts between the cloud service customer and the public cloud PII processor should specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor.	Implemented	Yes

A.27.12	Sub-Contracted PII Processing	A.10.12	Sub-Contracted PII Processing	Contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor.	Implemented	Yes
A.27.13	Access to data on pre-used data storage space	A.10.13	Access to data on pre-used data storage space	The public cloud PII processor should ensure that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer.	Implemented	Yes
A.28 - 27018 PRIVACY COMPLIANCE						
A.28.1	Geographical Location of PII	A.11.1	Geographical Location of PII	The public cloud PII processor should specify and document the countries in which PII might possibly be stored.	Implemented	Yes
A.28.2	Intended Destination of PII	A.11.2	Intended Destination of PII	PII transmitted using a data-transmission network should be subject to appropriate controls designed	Implemented	Yes

				to ensure that data reaches its intended destination.		
Microsoft-Defined GDPR Controls						
A.29 - GDPR COMPLIANCE						
A.29.1	Data Protection Impact Assessment | Processor		Data Protection Impact Assessment | Processor	Microsoft C&AI performs a Data Protection Impact Assessment for customer facing services where Microsoft is the Data Processor.	Implemented	Yes
A.29.2	Data Protection Impact Assessment | Customer Enablement		Data Protection Impact Assessment | Customer Enablement	Microsoft C&AI maintains documentation to enable customers to complete a Data Protection Impact Assessment.	Implemented	Yes
A.29.3	Data Subject Request Logging		Data Subject Request Logging	Data subject requests received from customers through Microsoft's administrative console are logged and retained per corporate guidelines.	Implemented	Yes
A.29.4	MINIMIZATION OF PERSONALLY INFORMATION		Minimization of Personal Information	Microsoft C&AI has defined a Data Protection Policy to manage customer data and to reduce the sensitivity and risk resulting from disclosure.	Implemented	Yes
A.29.5	Data Retention and Disposal		Data Retention and Disposal	Microsoft C&AI customer data is retained and removed per the defined terms within the Microsoft Online Services Terms (OST), when a customer's subscription	Implemented	Yes

				expires or is terminated.		
A.29.6	Identification and Authentication (Non-Organizational Users) | Data Subject Requests		Identification and Authentication (Non-Organizational Users) | Data Subject Requests	Microsoft C&AI provides a mechanism for authorized admins to authenticate prior to initiating a data subject request.	Implemented	Yes
A.29.7	PERSONAL DATA | INDIVIDUAL ACCESS		Personal Data | Individual Access, Delete and Export	Microsoft C&AI maintains a mechansim that enables authorized admins to directly access/export and delete personal data as per the Microsoft Privacy Policy.	Implemented	Yes
A.29.8	Data Residency, Transfer, Protection, Incident Response Policy		Data Residency, Transfer, Protection, Incident Response Policy	Microsoft C&AI maintains documentation and makes publicly available through organizational websites or otherwise: 1) Privacy program information, including data protection policies and instructions to action on a data subject request; 2) Data residency and transfer policy (including abstracted data flow maps, legal safeguards and justification for transfer); 3) Data protection policy description	Implemented	Yes

				including security, processor/controller commitment, privacy by design and default, backup and restore, and business continuity. The policy includes pointers to service capabilities that customer can use to support data protection and security; and 4) Incident management process.		
A.29.9	Information Sharing Agreement | First Parties		Information Sharing Agreement | First Parties	Microsoft C&AI will share personal data with other Microsoft teams in pursuant to Standard Operating Procedures for data protection and privacy.	Implemented	Yes
A.29.10	External Information System Services		External Information System Services	Microsoft C&AI maintains a list of subcontractors permitted to obtain customer data in the delivery of contracted services. Subcontractors are added to the list after the contractual notification period.	Implemented	Yes
A.29.11	Supplier Security and Privacy Assurance (SSPA) Program		Supplier Security and Privacy Assurance (SSPA) Program	To ensure subcontractor accountability, all Microsoft vendors who handle customer personal information are required to join	Implemented	Yes

				the Microsoft Supplier Security and Privacy Assurance Program.		
A.29.12	Protection of Information		Protection of Information	Customer Data is stored in customer-specified region and are not replicated outside of the geo in which that region resides as disclosed in public documentation.	Implemented	Yes
ISO 27701 Annex A: PIMS Specific PII Controllers						
B.8.2 Conditions for collection and processing						
B.8.2.1	Customer agreement		Customer agreement	The organization shall ensure, where relevant, that the contract to process PII addresses the organization's role in providing assistance with the customer's obligations, (taking into account the nature of processing and the information available to the organization).	Implemented	Yes
B.8.2.2	Organization's purposes		Organization 's purposes	The organization shall ensure that PII processed on behalf of a cus- tomer are only processed for the purposes expressed in the docu- mented instructions of the customer.	Implemented	Yes
B.8.2.3	Marketing and advertising use		Marketing and advertising use	The organization shall not use PII processed under a contract for the	Implemented	Yes

				purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal. The organization shall not make providing such consent a condition for receiving the service.		
B.8.2.4	Infringing instruction		Infringing instruction	The organization shall inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation.	Implemented	Yes
B.8.2.5	Customer obligations		Customer obligations	The organization shall provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations.	Implemented	Yes
B.8.2.6	Records related to processing PII		Records related to processing PII	The organization shall determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable contract) for the processing of PII carried out on behalf of a customer.	Implemented	Yes
B.8.3 Obligations to PII principals						

B.8.3.1	Obligations to PII principals		Obligations to PII principals	The organization shall provide the customer with the means to com- ply with its obligations related to PII principals.	Implemented	Yes
B.8.4 Privacy by design and privacy by default						
B.8.4.1	Temporary files		Temporary files	The organization shall ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.	Implemented	Yes
B.8.4.2	Return, transfer or disposal of PII		Return, transfer or disposal of PII	The organization shall provide the ability to return, transfer and/or disposal of PII in a secure manner. It shall also make its policy availa- ble to the customer.	Implemented	Yes
B.8.4.3	PII transmission controls		PII transmission controls	The organization shall subject PII transmitted over a data-transmis- sion network to appropriate controls designed to ensure that the data reaches its intended destination.	Implemented	Yes
B.8.5 PII sharing, transfer and disclosure						
B.8.5.1	Basis for PII trans- fer between juris- dictions		Basis for PII trans- fer between juris- dictions	The organization shall inform the customer in a timely manner of	Implemented	Yes

				the basis for PII transfers between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract.		
B.8.5.2	Countries and inter- national organiza- tions to which PII can be transferred		Countries and inter-national organiza-tions to which PII can be transferred	The organization shall specify and document the countries and inter- national organizations to which PII can possibly be transferred.	Implemented	Yes
B.8.5.3	Records of PII disclosure to third parties		Records of PII disclosure to third parties	The organization shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and when.	Implemented	Yes
B.8.5.4	Notification of PII disclosure requests		Notification of PII disclosure requests	The organization shall notify the customer of any legally binding requests for disclosure of PII.	Implemented	Yes
B.8.5.5	Legally binding PII disclosures		Legally binding PII disclosures	The organization shall reject any requests for PII disclosures that are not legally binding, consult the corresponding customer before making any PII disclosures and accepting any contractually agreed requests for PII	Implemented	Yes

				disclosures that are authorized by the corresponding customer.		
B.8.5.6	Disclosure of sub-contractors used to process PII		Disclosure of sub-contractors used to process PII	The organization shall disclose any use of subcontractors to process PII to the customer before use.	Implemented	Yes
B.8.5.7	Engagement of a subcontractor to process PII		Engagement of a subcontractor to process PII	The organization shall only engage a subcontractor to process PII according to the customer contract.	Implemented	Yes
B.8.5.8	Change of subcon- tractor to process PII		Change of subcon-tractor to process PII	The organization shall, in the case of having general written author-ization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, thereby giving the customer the opportunity to object to such changes.	Implemented	Yes