ISMS06005 Statement of Applicability

Version: v1.6

Dated: 02/25/2020

Security Classification: System High

Document Reference ISMS06005

ISO/IEC 27001:2013 Statement of Applicability				Control applicable?	Control implemented?	Reason for Selection (or justification if not applicable) including	Reference to Control Document/Evidence	Additional Controls Required (if any)
Area	Section	Control	Control Description					
A.5 Information security policies								
	A.5.1 Management direction for	A.5.1.1 Policies for information	A set of policies for information security shall be defined,	1	1	Risk Assessment	POL-ISP-004	
		A.5.1.2 Review of the policies for	The policies for information security shall be reviewed at	1	1	Risk Assessment	SOP-QA-001 Quality	
		Totals:		2	2			
A.6 Organization of information								
	A.6.1 Internal organization	A.6.1.1 Information security roles and	All information security responsibilities shall be defined	1	1	Risk Assessment	POL-ISP-004	
		A.6.1.2 Segregation of duties	Conflicting duties and areas of responsibility shall be	1	1	Risk Assessment	POL-ISP-008 Network and	
		A.6.1.3 Contact with authorities	Appropriate contacts with relevant authorities shall be	1	1	Risk Assessment & Legal	POL-CORP-006 Corporate	
		A.6.1.4 Contact with special interest	Appropriate contacts with special interest groups or other	1	1	Risk Assessment	POL-CORP-006 Corporate	
		A.6.1.5 Information security in project	Information security shall be addressed in project	1	1	Risk Assessment	POL-ISP-010 Systems	
	A.6.2 Mobile devices and teleworking	A.6.2.1 Mobile device policy	A policy and supporting security measures shall be	1	1	Risk Assessment	POL-ISP-014 Mobile Device	
		A.6.2.2 Teleworking	A policy and supporting security measures shall be	1	1	Risk Assessment	POL-ISP-009 Access	
		Totals:		7	7			
A.7 Human resources security								
	A.7.1 Prior to employment	A.7.1.1 Screening	Background verification checks on all candidates for	1	1	Risk Assessment & Legal	Background check reports	
		A.7.1.2 Terms and conditions of	The contractual agreements with employees and	1	1	Risk Assessment	Employee Contract	
	A.7.2 During employment	A.7.2.1 Management responsibilities	Management shall require all employees and contractors	1	1	Risk Assessment	POL-ISP-004	
		A.7.2.2 Information security	All employees of the organization and, where relevant,	1	1	Risk Assessment	POL-ISP-001 Information	
		A.7.2.3 Disciplinary process	There shall be a formal and communicated disciplinary	1	1	Risk Assessment	Employee Handbook	
	A.7.3 Termination and change of	A.7.3.1 Termination or change of	Information security responsibilities and duties that	1	1	Risk Assessment	Employee Handbook	
		Totals:		6	6			
A.8 Asset management								
	A.8.1 Responsibility for assets	A.8.1.1 Inventory of assets	Assets associated with information and information	1	1	Risk Assessment	POL-ISP-006 Asset	
		A.8.1.2 Ownership of assets	Assets maintained in the inventory shall be owned.	1	1	Risk Assessment	POL-ISP-006 Asset	
		A.8.1.3 Acceptable use of assets	Rules for the acceptable use of information and of assets	1	1	Risk Assessment	POL-ISP-006 Asset	
		A.8.1.4 Return of assets	All employees and external party users shall return all of	1	1	Risk Assessment	POL-ISP-006 Asset	
	A.8.2 Information classification	A.8.2.1 Classification of information	Information shall be classified in terms of legal	1	1	Risk Assessment	POL-ISP-006 Asset	
		A.8.2.2 Labeling of information	An appropriate set of procedures for information labeling	1	1	Risk Assessment	POL-ISP-006 Asset	
		A.8.2.3 Handling of assets	Procedures for handling assets shall be developed and	1	1	Risk Assessment	POL-ISP-006 Asset	
	A.8.3 Media Handling	A.8.3.1 Management of removable	Procedures shall be implemented for the management of	1	1	Risk Assessment	POL-ISP-006 Asset	
		A.8.3.2 Disposal of media	Media shall be disposed of securely when no longer	1	1	Risk Assessment	POL-ISP-006 Asset	
		A.8.3.3 Physical media transfer	Media containing information shall be protected against	1	1	Risk Assessment	POL-ISP-006 Asset	
		Totals:		10	10			
A.9 Access control								
	A.9.1 Business requirements of	A.9.1.1 Access control policy	An access control policy shall be established,	1	1	Risk Assessment	POL-ISP-009 Access	
		A.9.1.2 Access to networks and	Users shall only be provided with access to the network	1	1	Risk Assessment	POL-ISP-009 Access	
	A.9.2 User access management	A.9.2.1 User registration and de-	A formal user registration and de-registration process	1	1	Risk Assessment	SOP-HR-005 HR	
		A.9.2.2 User access provisioning	A formal user access provisioning process shall be	1	1	Risk Assessment	SOP-HR-005 HR	
		A.9.2.3 Management of privileged	The allocation and use of privileged access rights shall be	1	1	Risk Assessment	POL-ISP-009 Access	
		A.9.2.4 Management of secret	The allocation of secret authentication information shall	1	1	Risk Assessment	POL-ISP-009 Access	
		A.9.2.5 Review of user access rights	Asset owners shall review users' access rights at regular	1	1	Risk Assessment	POL-ISP-004	
		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.	1	1	Risk Assessment	POL-ISP-007-01 Information Security and Privacy Policy Regarding Staff Members	
	A.9.3 User responsibilities	A.9.3.1 Use of secret authentication	Users shall be required to follow the organization's	1	1	Risk Assessment	POL-ISP-009 Access	
	A.9.4 System and application access	A.9.4.1 Information access restriction	Access to information and application system functions	1	1	Risk Assessment	POL-ISP-009 Access	
		A.9.4.2 Secure log-on procedures	Where required by the access control policy, access to	1	1	Risk Assessment	POL-ISP-009 Access	
		A.9.4.3 Password management	Password management systems shall be interactive and	1	1	Risk Assessment	POL-ISP-009 Access	
		A.9.4.4 Use of privileged utility	The use of utility programs that might be capable of	1	1	Risk Assessment	POL-ISP-009 Access	
		A.9.4.5 Access control to program	Access to program source code shall be restricted.	1	1	Risk Assessment	POL-ISP-009 Access	
		Totals:		14	14			
A.10 Cryptography								

Document Reference ISMS06005

ISO/IEC 27001:2013 Statement of Applicability				Control applicable?	Control implemented?	Reason for Selection (or justification if not applicable) including	Reference to Control Document/Evidence	Additional Controls Required (if any)
Area	Section	Control	Control Description					
	A.10.1 Cryptographic controls	A.10.1.1 Policy on the use of	A policy on the use of cryptographic controls for	1	1	Risk Assessment	POL-ISP-010 Systems	
		A.10.1.2 Key management	A policy on the use, protection and lifetime of	1	1	Risk Assessment	POL-ISP-010 Systems	
		Totals:		2	2			
A.11 Physical and environmental								
	A.11.1 Secure areas	A.11.1.1 Physical security perimeter	Security perimeters shall be defined and used to protect	1	1	Risk Assessment	POL-ISP-005 Physical and	
		A.11.1.2 Physical entry controls	Secure areas shall be protected by appropriate entry	1	1	Risk Assessment	POL-ISP-005 Physical and	
		A.11.1.3 Securing offices, rooms and	Physical security for offices, rooms and facilities shall be	1	1	Risk Assessment	POL-ISP-005 Physical and	
		A.11.1.4 Protecting against external	Physical protection against natural disasters, malicious	1	1	Risk Assessment	POL-ISP-005 Physical and	
		A.11.1.5 Working in secure areas	Procedures for working in secure areas shall be designed	1	1	Risk Assessment	POL-ISP-005 Physical and	
		A.11.1.6 Delivery and loading areas	Access points such as delivery and loading areas and	1	1	Risk Assessment	POL-ISP-005 Physical and	
	A.11.2 Equipment	A.11.2.1 Equipment siting and	Equipment shall be sited and protected to reduce the	1	1	Risk Assessment	POL-ISP-005 Physical and	
		A.11.2.2 Supporting utilities	Equipment shall be protected from power failures and	1	1	Risk Assessment	POL-ISP-005 Physical and	
		A.11.2.3 Cabling security	Power and telecommunications cabling carrying data or	1	1	Risk Assessment	POL-ISP-005 Physical and	
		A.11.2.4 Equipment maintenance	Equipment shall be correctly maintained to ensure its	1	1	Risk Assessment	POL-ISP-005 Physical and	
		A.11.2.5 Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	1	1	Risk Assessment	SOP-CORP-010 Operations Change Management	
		A.11.2.6 Security of equipment and	Security shall be applied to off-site assets taking into	1	1	Risk Assessment	N/A No off-site assets	
		A.11.2.7 Secure disposal or reuse of	All items of equipment containing storage media shall be	1	1	Risk Assessment	OTHER-ITH-040 Data	
		A.11.2.8 Unattended user equipment	Users shall ensure that unattended equipment has	1	1	Risk Assessment	POL-ISP-005 Physical and	
		A.11.2.9 Clear desk and clear screen	A clear desk policy for papers and removable storage	1	1	Risk Assessment	POL-ISP-005 Physical and	
		Totals:		15	15			
A.12 Operations security								
	A.12.1 Operational procedures and	A.12.1.1 Documented operating	Operating procedures shall be documented and made	1	1	Risk Assessment	Medidata Policies-SOPs	
		A.12.1.2 Change management	Changes to the organization, business processes,	1	1	Risk Assessment	SOP-CORP-010 Operations	
		A.12.1.3 Capacity management	The use of resources shall be monitored, tuned and	1	1	Risk Assessment	SOP-IT-043-00 Capacity	
		A.12.1.4 Separation of development,	Development, testing, and operational environments shall	1	1	Risk Assessment	POL-ISP-008 Network and	
	A.12.2 Protection from malware	A.12.2.1 Controls against malware	Detection, prevention and recovery controls to protect	1	1	Risk Assessment	POL-ISP-008 Network and	
	A.12.3 Backup	A.12.3.1 Information backup	Backup copies of information, software and system	1	1	Risk Assessment	OTHER-ITH-040 Data	
	A.12.4 Logging and monitoring	A.12.4.1 Event logging	Event logs recording user activities, exceptions, faults	1	1	Risk Assessment	SOP-IT-038-04 Event	
		A.12.4.2 Protection of log information	Logging facilities and log information shall be protected	1	1	Risk Assessment	SOP-IT-038-04 Event	
		A.12.4.3 Administrator and operator	System administrator and system operator activities shall	1	1	Risk Assessment	SOP-IT-038-04 Event	
		A.12.4.4 Clock synchronization	The clocks of all relevant information processing systems	1	1	Risk Assessment	OTHER-ITH-040 Data	
	A.12.5 Control of operational software	A.12.5.1 Installation of software on	Procedures shall be implemented to control the	1	1	Risk Assessment	SOP-CORP-010 Operations	
	A.12.6 Technical vulnerability	A.12.6.1 Management of technical	Information about technical vulnerabilities of information	1	1	Risk Assessment	SOP-ISP-004 Penetration	
		A.12.6.2 Restrictions on software	Rules governing the installation of software by users shall	1	1	Risk Assessment	SOP-CORP-010 Operations	
	A.12.7 Information systems audit	A.12.7.1 Information systems audit	Audit requirements and activities involving verification of	1	1	Risk Assessment	SOP-CORP-010 Operations	
		Totals:		14	14			
A.13 Communications security								
	A.13.1 Network security management	A.13.1.1 Network controls	Networks shall be managed and controlled to protect	1	1	Risk Assessment	POL-ISP-008 Network and	
		A.13.1.2 Security of network	Security mechanisms, service levels and management	1	1	Risk Assessment	POL-ISP-008 Network and	
		A.13.1.3 Segregation in networks	Groups of information services, users and information	1	1	Risk Assessment	POL-ISP-008 Network and	
	A.13.2 Information transfer	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.	1	1	Risk Assessment	POL-ISP-001 Information Security and Data Privacy POL-ISP-008 Network and Computer Operations Security Policy POL-ISP-013 Compliance Security	
		A.13.2.2 Agreements on information	Agreements shall address the secure transfer of business	1	1	Risk Assessment	Client Master Service	
		A.13.2.3 Electronic messaging	Information involved in electronic messaging shall be	1	1	Risk Assessment	POL-ISP-008 Network and	
		A.13.2.4 Confidentiality or	Requirements for confidentiality or non-disclosure	1	1	Risk Assessment	POL-ISP-004	
		Totals:		7	7			
A.14 System acquisition,								

Document Reference ISMS06005

ISO/IEC 27001:2013 Statement of Applicability				Control applicable?	Control implemented?	Reason for Selection (or justification if not applicable) including	Reference to Control Document/Evidence	Additional Controls Required (if any)
Area	Section	Control	Control Description					
	A.14.1 Security requirements of	A.14.1.1 Information security	The information security related requirements shall be	1	1	Risk Assessment	POL-ISP-010 Systems	
		A.14.1.2 Securing application	Information involved in application services passing over	1	1	Risk Assessment	SOP-CORP-010 Operations	
		A.14.1.3 Protecting application	Information involved in application service transactions	1	1	Risk Assessment	N/A No application service	
	A.14.2 Security in development and	A.14.2.1 Secure development policy	Rules for the development of software and systems shall	1	1	Risk Assessment	POL-ISP-010 Systems	
		A.14.2.2 System change control	Changes to systems within the development lifecycle	1	1	Risk Assessment	SOP-CORP-010 Operations	
		A.14.2.3 Technical review of	When operating platforms are changed, business critical	1	1	Risk Assessment	SOP-CORP-010 Operations	
		A.14.2.4 Restrictions on changes to	Modifications to software packages shall be discouraged,	1	1	Risk Assessment	SOP-CORP-010 Operations	
		A.14.2.5 Secure system engineering	Principles for engineering secure systems shall be	1	1	Risk Assessment	POL-ISP-010 Systems	
		A.14.2.6 Secure development	Organizations shall establish and appropriately protect	1	1	Risk Assessment	SOP-CORP-010 Operations	
		A.14.2.7 Outsourced development	The organization shall supervise and monitor the activity	1	1	Risk Assessment	N/A No outsourced	
		A.14.2.8 System security testing	Testing of security functionality shall be carried out during	1	1	Risk Assessment	POL-ISP-010 Systems	
		A.14.2.9 System acceptance testing	Acceptance testing programs and related criteria shall be	1	1	Risk Assessment	POL-ISP-010 Systems	
	A.14.3 Test data	A.14.3.1 Protection of test data	Test data shall be selected carefully, protected and	1	1	Risk Assessment	POL-ISP-010 Systems	
		Totals:		13	13			
A.15 Supplier relationships								
	A.15.1 Information security in supplier	A.15.1.1 Information security policy for	Information security requirements for mitigating the risks	1	1	Risk Assessment	SOP-QA-002 Supplier	
		A.15.1.2 Addressing security within	All relevant information security requirements shall be	1	1	Risk Assessment	Client Master Service	
		A.15.1.3 Information and	Agreements with suppliers shall include requirements to	1	1	Risk Assessment	SOP-QA-002 Supplier	
	A.15.2 Supplier service delivery	A.15.2.1 Monitoring and review of	Organizations shall regularly monitor, review and audit	1	1	Risk Assessment	SOP-QA-002 Supplier	
		A.15.2.2 Managing changes to	Changes to the provision of services by suppliers,	1	1	Risk Assessment	SOP-QA-002 Supplier	
		Totals:		5	5			
A.16 Information security incident								
	A.16.1 Management of information	A.16.1.1 Responsibilities and	Management responsibilities and procedures shall be	1	1	Risk Assessment	q	
		A.16.1.2 Reporting information	Information security events shall be reported through	1	1	Risk Assessment	POL-CORP-006 Corporate	
		A.16.1.3 Reporting information	Employees and contractors using the organization’s	1	1	Risk Assessment	POL-CORP-006 Corporate	
		A.16.1.4 Assessment of and decision	Information security events shall be assessed and it shall	1	1	Risk Assessment	POL-CORP-006 Corporate	
		A.16.1.5 Response to information	Information security incidents shall be responded to in	1	1	Risk Assessment	POL-CORP-006 Corporate	
		A.16.1.6 Learning from information	Knowledge gained from analyzing and resolving	1	1	Risk Assessment	POL-CORP-006 Corporate	
		A.16.1.7 Collection of evidence	The organization shall define and apply procedures for	1	1	Risk Assessment	POL-ISP-013 Compliance	
		Totals:		7	7			
A.17 Information security aspects								
	A.17.1 Information security continuity	A.17.1.1 Planning information security	The organization shall determine its requirements for	1	1	Risk Assessment	POL-CORP-006 Corporate	
		A.17.1.2 Implementing information	The organization shall establish, document, implement	1	1	Risk Assessment	OTHER-CORP-017	
		A.17.1.3 Verify, review and evaluate	The organization shall verify the established and	1	1	Risk Assessment	OTHER-CORP-017	
	A.17.2 Redundancies	A.17.2.1 Availability of information	Information processing facilities shall be implemented	1	1	Risk Assessment	OTHER-CORP-017	
		Totals:		4	4			
A.18 Compliance								
	A.18.1 Compliance with legal and	A.18.1.1 Identification of applicable	All relevant legislative statutory, regulatory, contractual	1	1	Risk Assessment	POL-ISP-013 Compliance	
		A.18.1.2 Intellectual property rights	Appropriate procedures shall be implemented to ensure	1	1	Risk Assessment	POL-ISP-013 Compliance	
		A.18.1.3 Protection of records	Records shall be protected from loss, destruction,	1	1	Risk Assessment	POL-QA-008-04 Quality	
		A.18.1.4 Privacy and protection of	Privacy and protection of personally identifiable	1	1	Risk Assessment	POL-ISP-013 Compliance	
		A.18.1.5 Regulation of cryptographic	Cryptographic controls shall be used in compliance with	1	1	Risk Assessment	Letter from Bureau of	
	A.18.2 Information security reviews	A.18.2.1 Independent review of	The organization’s approach to managing information	1	1	Risk Assessment	SOC2 - Description of	
		A.18.2.2 Compliance with security	Managers shall regularly review the compliance of	1	1	Risk Assessment	Internal QS Audit Report for	
		A.18.2.3 Technical compliance review	Information systems shall be regularly reviewed for	1	1	Risk Assessment	Internal QS Audit Report for	
		Totals:		8	8			

Document Reference ISMS06005

ISO/IEC 27018:2014 Statement of Applicability				Control applicable?	Control implemented?	Reason for Selection (or justification if not applicable) including risk reference	Reference to Control Document/Evidence	Additional Controls Required (if any)
Area	Section	Control	Control Description					
A.1 Obligation to co-operate regarding PII principals' rights								
	A.1.1 Obligation to co-operate regarding PII principals' rights	A.5.1.1 Policies for information security	Specified informational and technical measures are specific in the contract with the cloud processor	1	1	Risk Assessment	POL-IS-01-06 Information Security Policy Amazon Contract	
A.2 Purpose legitimacy and specification								
		A.2.1 Public cloud II processors purpose	Instruction in the contract between the public cloud PII process and the cloud service customer including objective goal for the service, for the purpose of measuring conformity	1	1	Risk Assessment	Amazon Contract	
		A.2.2 Public cloud PII processors' commercial use	PII not processed without customer consent	1	1	Risk Assessment	MPO-01-01 Data Governance Policy	
	A.3	A.3 Collection Limitation	Rely on ISO 27001	0	0	N/A	N/A	
A.4 Data Minimization								
		A.4.1 Secure erasure of temporary files	Medidata performs audit on the scope and application of FIPS 800-88 sanitation of all media that has the potential to store or transmit PII	1	1	Risk Assessment	POL-IS-01-06 Information Security Policy	
A.5 Use, retention and disclosure limitation								
		A.5.1 PII disclosure notification	Public cloud processor shall notify Medidata of any legitimate request for disclosure of PII by law enforcement	1	1	Risk Assessment	Amazon Contract	
		A.5.2 Recording of PII Disclosures	Disclosure of all PII is recorded via the MPO tracking program	1	1	Risk Assessment	MPO-01-01 Data Governance Policy	
A.6 Accuracy and quality								
		A.6 Accuracy and Quality	Rely on ISO 27001	0	0	N/A	N/A	
A.7 Openness, transparency and notice								
		A.7.1 Disclosure of sub-contracted PII processing	Disclosure of subcontractor information is define within the Master Services Agreement	1	1	Risk Assessment	Medidata Standard Managed Service Agreement	
A.8 Individual participation and access								
		A.8 Individual Participation and access	Rely on ISO 27001	0	0	N/A	N/A	
A.9 Accountability								
		A.9.1 Notification of a data breach involving PII	Data breach notification requirements are including in Medidata Master Service Agreement; consistent with Medidata Incident Response protocols which include description, time period, consequences, impact and remediation steps				POL-IS-01-06 Information Security Policy	
		A.9.2 Retention period for administrative security policies and guidelines	Policies shall be kept in a Electronic Document Management System (EDMS) in accordance with the Medidata Data Retention Policy				Data Retention Policy	
		A.9.3 PII return, transfer ad disposal	Policy shall exist for the deposition of PII and should be available for the customer.				End of Study Work Instruction	
A.10 Information Security								
		A.10.1 Confidentiality or non-disclosure agreements	Confidentiality agreements between public cloud processor, its employees and agents) which ensure that disclosure outside of Medidata's instructions; terms of which shall be survivable in perpetuity.	1	1	Risk Assessment	Amazon Contract	
		A.10.2 Restriction of creation of hardcopy material	Rely on ISO 27001	0	0	N/A	N/A	
		A.10.3 Control and logging of data restoration	Manual data restoration processes shall include task, description of stored data, person responsible and date.	1	1	Risk Assessment	MPO-01-01 Data Governance Policy	
		A.10.4 Protecting data on storage media leaving the premises.	Medida contain PII shall be subject to an authorization procedure and should not be accessible to anyone other than authorized data.	1	1	Risk Assessment	MPO-01-01 Data Governance Policy	
		A.10.5 Use of unencrypted portable storage media and devices	Portable physical media and portable devices that do not permit encryption are prohibited.	1	1	Risk Assessment	POL-IS-01-06 Information Security Policy	

Document Reference ISMS06005

ISO/IEC 27018:2014 Statement of Applicability				Control applicable?	Control implemented?	Reason for Selection (or justification if not applicable) including risk reference	Reference to Control Document/Evidence	Additional Controls Required (if any)
Area	Section	Control	Control Description					
		A.10.6 Encryption of PII transmitted over public data-transmission networks	PII transmitted over public data-transmission networks should be encrypted prior to transmission	1	1	Risk Assessment	POL-IS-01-06 Information Security Policy	
		A.10.7 Secure Disposal of hardcopy materials	Where hardcopy materials are destroyed, they should be destroyed security using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.	1	1	Risk Assessment	POL-IS-01-06 Information Security Policy	
		A.10.8 Unique user of user IDs	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.	1	1	Risk Assessment	POL-IS-01-06 Information Security Policy	
		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	1	1	Risk Assessment	POL-IS-01-06 Information Security Policy	
		A.10.10 User ID management	De-activated or expired user ID's should not be granted to other individuals	1	1	Risk Assessment	POL-IS-01-06 Information Security Policy	
		A.10.11 Contract measures	Contracts between the cloud service customer and the public cloud PII process should specific minimum technical and organization measures to ensure that the contract security arrangements are in place and the data is 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 processor.	1	1	Risk Assessment	Amazon Contract	
		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's security and PII protection obligations of the public cloud processor. Such measures should not be subject to unilateral reductions by the sub-contractor.	1	1	Risk Assessment	POL-IS-01-06 Information Security Policy	
		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 assignee to a cloud service customer; any data previously residing on the storage space in not visible to that cloud service customer.	1	1	Risk Assessment	Amazon Contract	
A.11 Privacy compliance								
		A.11.1 Geographical Location of PII	The public cloud PII process should specific and document the countries in which PII might possibly be stored.	1	1	Risk Assessment	Medidata Standard Managed Service Agreement	
		A.11.2 Intended destination of PII	PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that the data reaches it's destination.	1	1	Risk Assessment	POL-IS-01-06 Information Security Policy	
		Totals:		21	21			

Document Reference ISMS06005

ISO/IEC 27701:2019 Statement of Applicability				Control applicable?	Control implemented?	Reason for Selection (or justification if not applicable) including risk reference	Reference to Control Document/Evidence	Additional Controls Required (if any)
Area	Section	Control	Control Description					
B.8.2 Conditions for collection and processing			To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.					
		B.8.2.1 Customer agreement	The organization shall ensure that PII processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer.	1	1	Risk Assessment	POL-MPO-003-00 Global Privacy Policy	
		B.8.2.2 Organization's purposes	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).	1	1	Risk Assessment	POL-MPO-003-00 Global Privacy Policy	
		B.8.2.3 Marketing and advertising use	The organization shall not use PII processed under a contract for the 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.	1	1	Risk Assessment	POL-MPO-003-00 Global Privacy Policy	
		B.8.2.4 Infringing instruction	The organization shall inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation.	1	1	Risk Assessment	POL-MPO-003-00 Global Privacy Policy	
		B.8.2.5 Customer obligations	The organization shall provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations.	1	1	Risk Assessment	POL-MPO-003-00 Global Privacy Policy	
		B.8.2.6 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.	1	1	Risk Assessment	POL-MPO-003-00 Global Privacy Policy	
B.8.3 Obligations to PII principals			To ensure that PII principals are provided with the appropriate information about the processing of their PII, and to meet any other applicable obligations to PII principals related to the processing of their PII.					
		B.8.3.1 Obligations to PII principals	The organization shall provide the customer with the means to comply with its obligations related to PII principals.	1	1	Risk Assessment	POL-MPO-003-00 Global Privacy Policy	
B.8.4 Privacy by design and privacy by default			To ensure that processes and systems are designed such that the collection and processing of PII (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.					
		B.8.4.1 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.	1	1	Risk Assessment	POL-MPO-003-00 Global Privacy Policy	
		B.8.4.2 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 available to the customer.	1	1	Risk Assessment	POL-MPO-003-00 Global Privacy Policy	
		B.8.4.3 PII transmission controls	The organization shall subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.	1	1	Risk Assessment	POL-MPO-003-00 Global Privacy Policy	
B.8.5 PII sharing, transfer and disclosure			To determine whether and document when PII is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.					
		B.8.5.1 Basis for PII transfer between jurisdictions	The organization shall inform the customer in a timely manner of 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.	1	1	Risk Assessment	POL-MPO-003-00 Global Privacy Policy	

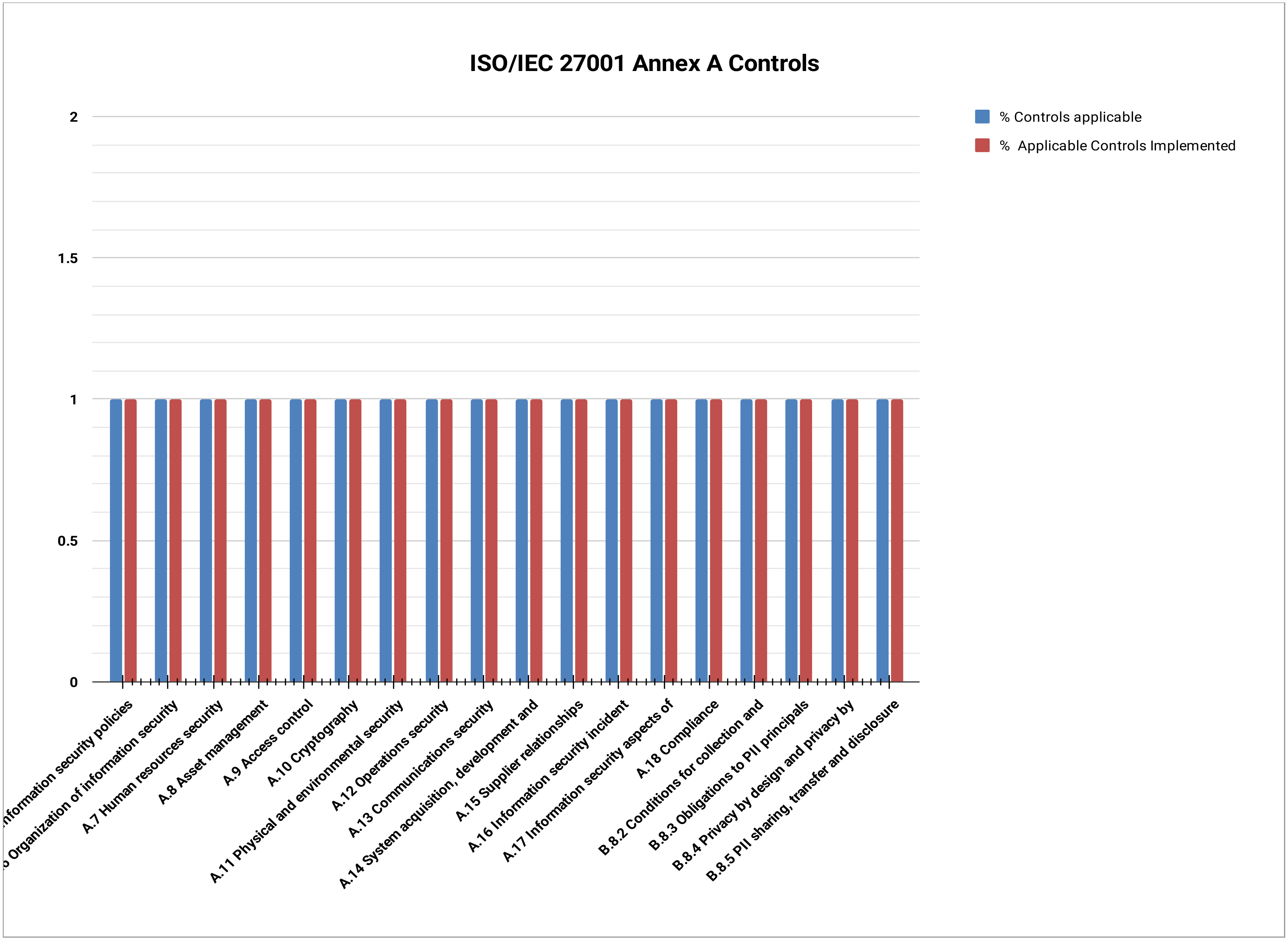
Document Reference ISMS06005

ISO/IEC 27701:2019 Statement of Applicability				Control applicable?	Control implemented?	Reason for Selection (or justification if not applicable) including risk reference	Reference to Control Document/Evidence	Additional Controls Required (if any)
Area	Section	Control	Control Description					
		B.8.5.2 Countries and international organizations to which PII can be transferred	The organization shall specify and document the countries and international organizations to which PII can possibly be transferred.	1	1	Risk Assessment	POL-MPO-003-00 Global Privacy Policy	
		B.8.5.3 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.	1	1	Risk Assessment	POL-MPO-003-00 Global Privacy Policy	
		B.8.5.4 Notification of PII disclosure requests	The organization shall notify the customer of any legally binding requests for disclosure of PII.	1	1	Risk Assessment	POL-MPO-003-00 Global Privacy Policy	
		B.8.5.5 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 disclosures that are authorized by the corresponding customer.	1	1	Risk Assessment	POL-MPO-003-00 Global Privacy Policy	
		B.8.5.6 Disclosure of subcontractors used to process PII	The organization shall disclose any use of subcontractors to process PII to the customer before use.	1	1	Risk Assessment	POL-MPO-003-00 Global Privacy Policy	
		B.8.5.7 Engagement of a subcontractor to process PII	The organization shall only engage a subcontractor to process PII according to the customer contract.	1	1	Risk Assessment	POL-MPO-003-00 Global Privacy Policy	
		B.8.5.8 Change of subcontractor to process PII	The organization shall, in the case of having general written authorization, 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.	1	1	Risk Assessment	POL-MPO-003-00 Global Privacy Policy	
		Totals:		13	13			

medidata

Statement of Applicability Summary

Area	Number of ISO/IEC 27001 Controls	Number of Applicable Controls	% Controls applicable	Number of Applicable Controls Implemented	% Applicable Controls Implemented
A.5 Information security policies	2	2	100%	2	100%
A.6 Organization of information security	7	7	100%	7	100%
A.7 Human resources security	6	6	100%	6	100%
A.8 Asset management	10	10	100%	10	100%
A.9 Access control	14	14	100%	14	100%
A.10 Cryptography	2	2	100%	2	100%
A.11 Physical and environmental security	15	15	100%	15	100%
A.12 Operations security	14	14	100%	14	100%
A.13 Communications security	7	7	100%	7	100%
A.14 System acquisition, development and maintenance	13	13	100%	13	100%
A.15 Supplier relationships	5	5	100%	5	100%
A.16 Information security incident management	7	7	100%	7	100%
A.17 Information security aspects of business continuity management	4	4	100%	4	100%
A.18 Compliance	8	8	100%	8	100%
B.8.2 Conditions for collection and processing	6	6	100%	6	100%
B.8.3 Obligations to PII principals	1	1	100%	1	100%
B.8.4 Privacy by design and privacy by default	3	3	100%	3	100%
B.8.5 PII sharing, transfer and disclosure	8	8	100%	8	100%



ISO/IEC 27001 Annex A Controls