Databricks ISO 27001 / 27018 / 27017 / 27701 Statement of Applicability.

ISMS and PIMS
Last updated: 3/23/2023 version 7
Company Confidential. If printed, this is not the authoritative version.
Note: "n/a" implies a new requirement specifically for ISO 27001:2022 so there is no correspondence of the ISO 27001:2022 standanrd with ISO 27018:2019 and ISO 27017:2015.

			ISO 27001:2022		ISO 27018:2019		ISO 27017:2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion or exclusion
A.5	Organizational controls								
A.5.1	Policies for information security	Control Information security policy and topic-specific policies shall be de- fined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	yes	yes	yes	yes	yes	yes	legal risk assessment business requirement best practice
A.5.2	Information security roles and responsibilities	Control Information security roles and responsibilities shall be defined and allocated according to the organization needs.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.5.3	Segregation of duties	Control Conflicting duties and conflicting areas of responsibility shall be seg- regated.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.5.4	Management responsibilities	Control Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.5.5	Contact with authorities	Control The organization shall establish and maintain contact with relevant authorities.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.5.6	Contact with special interest groups	Control The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.5.7	Threat intelligence	Control Information relating to information security threats shall be collected and analysed to produce threat intelligence.	yes	yes	n/a - This is new for ISO 27001:2022. There is no correspondence of the ISO 27001:2022 standard with ISO 27018:2019 and ISO 27017:2015.				risk assessment best practice
A.5.8	Information security in project management	Control Information security shall be integrated into project management.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.5.9	Inventory of information and other associated assets	Control Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	yes	yes	yes	yes	yes	yes	business requirement best practice risk assessment
A.5.10	Acceptable use of information and other associated assets	Control Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	yes	yes	yes	yes	yes	yes	business requirement best practice risk assessment

Databricks ISO 27001 / 27018 / 27017 / 27701 Statement of Applicability.

ISMS and PIMS
Last updated: 3/23/2023 version 7
Company Confidential. If printed, this is not the authoritative version.
Note: "n/a" implies a new requirement specifically for ISO 27001:2022 so there is no correspondence of the ISO 27001:2022 standanrd with ISO 27018:2019 and ISO 27017:2015.

			ISO 27001:2022		ISO 27018:2019		ISO 27017:2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion or exclusion
A.5.11	Return of assets	Control Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	yes	yes	yes	yes	yes	yes	business requirement best practice risk assessment
A.5.12	Classification of information	Control Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	yes	yes	yes	yes	yes	yes	business requirement best practice risk assessment
A.5.13	Labelling of information	Control An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information clas- sification scheme adopted by the organization.	yes	yes	yes	yes	yes	yes	business requirement best practice risk assessment
A.5.14	Information transfer	Control Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice
A.5.15	Access control	Control Rules to control physical and logical access to information and other associated assets shall be established and implemented based on busi- ness and information security requirements.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice business requirement
A.5.16	Identity management	Control The full life cycle of identities shall be managed.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.5.17	Authentication information	Control Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.5.18	Access rights	Control Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	yes	yes	yes	yes	yes	yes	risk assessment legal best practice business requirement
A.5.19	Information security in supplier relationships	Control Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	yes	yes	yes	yes	yes	yes	best practice risk assessment

Databricks ISO 27001 / 27018 / 27017 / 27701 Statement of Applicability.

ISMS and PIMS
Last updated: 3/23/2023 version 7
Company Confidential. If printed, this is not the authoritative version.
Note: "n/a" implies a new requirement specifically for ISO 27001:2022 so there is no correspondence of the ISO 27001:2022 standanrd with ISO 27018:2019 and ISO 27017:2015.

			ISO 27001:2022		**ISO 27018:2019**		**ISO 27017:2015**		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion or exclusion
A.5.20	Addressing information security within supplier agreements	Control Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	yes	yes	yes	yes	yes	yes	legal best practice business requirement risk assessment
A.5.21	Managing information security in the information and commu- nication technology (ICT) supply chain	Control Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.5.22	Monitoring, review and change management of supplier services	Control The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.5.23	Information security for use of cloud services	Control Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	yes	yes	n/a - This is new for ISO 27001:2022. There is no correspondence of the ISO 27001:2022 standard with ISO 27018:2019 and ISO 27017:2015.				legal risk assessment business requirement best practice
A.5.24	Information security incident management planning and prepa- ration	Control The organization shall plan and prepare for managing information secu- rity incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.5.25	Assessment and decision on in- formation security events	Control The organization shall assess information security events and decide if they are to be categorized as information security incidents.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.5.26	Response to information security incidents	Control Information security incidents shall be responded to in accordance with the documented procedures.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.5.27	Learning from information se- curity incidents	Control Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.5.28	Collection of evidence	Control The organization shall establish and implement procedures for the iden- tification, collection, acquisition and preservation of evidence related to information security events.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment

Databricks ISO 27001 / 27018 / 27017 / 27701 Statement of Applicability.

ISMS and PIMS
Last updated: 3/23/2023 version 7
Company Confidential. If printed, this is not the authoritative version.
Note: "n/a" implies a new requirement specifically for ISO 27001:2022 so there is no correspondence of the ISO 27001:2022 standanrd with ISO 27018:2019 and ISO 27017:2015.

			ISO 27001:2022		ISO 27018:2019		ISO 27017:2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion or exclusion
A.5.29	Information security during disruption	Control The organization shall plan how to maintain information security at an appropriate level during disruption.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice business requirement
A.5.30	ICT readiness for business con- tinuity	Control ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	yes	yes	n/a - This is new for ISO 27001:2022. There is no correspondence of the ISO 27001:2022 standard with ISO 27018:2019 and ISO 27017:2015.				risk assessment business requirement best practice
A.5.31	Legal, statutory, regulatory and contractual requirements	Control Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice business requirement
A.5.32	Intellectual property rights	Control The organization shall implement appropriate procedures to protect intellectual property rights.	yes	yes	yes	yes	yes	yes	legal best practice risk assessment
A.5.33	Protection of records	Control Records shall be protected from loss, destruction, falsification, unau- thorized access and unauthorized release.	yes	yes	yes	yes	yes	yes	legal best practice risk assessment
A.5.34	Privacy and protection of person- al identifiable information (PII)	Control The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	yes	yes	yes	yes	yes	yes	legal best practice business requirement risk assessment
A.5.35	Independent review of informa- tion security	Control The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.5.36	Compliance with policies, rules and standards for information security	Control Compliance with the organization's information security policy, top- ic-specific policies, rules and standards shall be regularly reviewed.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.5.37	Documented operating proce- dures	Control Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.6	People controls								

Databricks ISO 27001 / 27018 / 27017 / 27701 Statement of Applicability.

ISMS and PIMS
Last updated: 3/23/2023 version 7
Company Confidential. If printed, this is not the authoritative version.
Note: "n/a" implies a new requirement specifically for ISO 27001:2022 so there is no correspondence of the ISO 27001:2022 standanrd with ISO 27018:2019 and ISO 27017:2015.

			ISO 27001:2022		**ISO 27018:2019**		**ISO 27017:2015**		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion or exclusion
A.6.1	Screening	Control Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	yes	yes	yes	yes	yes	yes	legal risk assessment business requirement best practice
A.6.2	Terms and conditions of employment	Control The employment contractual agreements shall state the personnel’s and the organization’s responsibilities for information security.	yes	yes	yes	yes	yes	yes	legal business requirement best practice risk assessment
A.6.3	Information security awareness, education and training	Control Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice risk assessment
A.6.4	Disciplinary process	Control A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	yes	yes	yes	yes	yes	yes	legal best practice risk assessment
A.6.5	Responsibilities after termination or change of employment	Control Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice
A.6.6	Confidentiality or non-disclosure agreements	Control Confidentiality or non-disclosure agreements reflecting the organ- ization’s needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	yes	yes	yes	yes	yes	yes	legal best practice risk assessment
A.6.7	Remote working	Control Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization’s premises.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment

Databricks ISO 27001 / 27018 / 27017 / 27701 Statement of Applicability.

ISMS and PIMS
Last updated: 3/23/2023 version 7
Company Confidential. If printed, this is not the authoritative version.
Note: "n/a" implies a new requirement specifically for ISO 27001:2022 so there is no correspondence of the ISO 27001:2022 standanrd with ISO 27018:2019 and ISO 27017:2015.

			ISO 27001:2022		ISO 27018:2019		ISO 27017:2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion or exclusion
A.6.8	Information security event reporting	Control The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice
A.7	**Physical controls**								
A.7.1	Physical security perimeters	Control Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.7.2	Physical entry	Control Secure areas shall be protected by appropriate entry controls and access points.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.7.3	Securing offices, rooms and facilities	Control Physical security for offices, rooms and facilities shall be designed and implemented.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.7.4	Physical security monitoring	Control Premises shall be continuously monitored for unauthorized physical access.	yes	yes	n/a - This is new for ISO 27001:2022. There is no correspondence of the ISO 27001:2022 standard with ISO 27018:2019 and ISO 27017:2015.				risk assessment best practice
A.7.5	Protecting against physical and environmental threats	Control Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.7.6	Working in secure areas	Control Security measures for working in secure areas shall be designed and implemented.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.7.7	Clear desk and clear screen	Control Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.7.8	Equipment siting and protection	Control Equipment shall be sited securely and protected.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.7.9	Security of assets off-premises	Control Off-site assets shall be protected.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.7.10	Storage media	Control Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice business requirement

Databricks ISO 27001 / 27018 / 27017 / 27701 Statement of Applicability.

ISMS and PIMS
Last updated: 3/23/2023 version 7
Company Confidential. If printed, this is not the authoritative version.
Note: "n/a" implies a new requirement specifically for ISO 27001:2022 so there is no correspondence of the ISO 27001:2022 standanrd with ISO 27018:2019 and ISO 27017:2015.

			ISO 27001:2022		ISO 27018:2019		ISO 27017:2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion or exclusion
A.7.11	Supporting utilities	Control Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.7.12	Cabling security	Control Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.7.13	Equipment maintenance	Control Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.7.14	Secure disposal or re-use of equipment	Control Items of equipment containing storage media shall be verified to en- sure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	yes	yes	yes	yes	yes	yes	risk assessment best practice
A.8	**Technological controls**								
A.8.1	User end point devices	Control Information stored on, processed by or accessible via user end point devices shall be protected.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.8.2	Privileged access rights	Control The allocation and use of privileged access rights shall be restricted and managed.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice business requirement
A.8.3	Information access restriction	Control Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.8.4	Access to source code	Control Read and write access to source code, development tools and software libraries shall be appropriately managed.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.8.5	Secure authentication	Control Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.8.6	Capacity management	Control The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.8.7	Protection against malware	Control Protection against malware shall be implemented and supported by appropriate user awareness.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement

Databricks ISO 27001 / 27018 / 27017 / 27701 Statement of Applicability.

ISMS and PIMS
Last updated: 3/23/2023 version 7
Company Confidential. If printed, this is not the authoritative version.
Note: "n/a" implies a new requirement specifically for ISO 27001:2022 so there is no correspondence of the ISO 27001:2022 standanrd with ISO 27018:2019 and ISO 27017:2015.

			ISO 27001:2022		**ISO 27018:2019**		**ISO 27017:2015**		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion or exclusion
A.8.8	Management of technical vulnerabilities	Control Information about technical vulnerabilities of information systems in use shall be obtained, the organization’s exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice business requirement
A.8.9	Configuration management	Control Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	yes	yes	n/a - This is new for ISO 27001:2022. There is no correspondence of the ISO 27001:2022 standard with ISO 27018:2019 and ISO 27017:2015.				risk assessment best practice
A.8.10	Information deletion	Control Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	yes	yes	n/a - This is new for ISO 27001:2022. There is no correspondence of the ISO 27001:2022 standard with ISO 27018:2019 and ISO 27017:2015.				legal risk assessment best practice
A.8.11	Data masking	Control Data masking shall be used in accordance with the organization’s topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	yes	yes	n/a - This is new for ISO 27001:2022. There is no correspondence of the ISO 27001:2022 standard with ISO 27018:2019 and ISO 27017:2015.				legal risk assessment best practice
A.8.12	Data leakage prevention	Control Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	yes	yes	n/a - This is new for ISO 27001:2022. There is no correspondence of the ISO 27001:2022 standard with ISO 27018:2019 and ISO 27017:2015.				risk assessment business requirement best practice
A.8.13	Information backup	Control Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.8.14	Redundancy of information processing facilities	Control Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.8.15	Logging	Control Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.8.16	Monitoring activities	Control Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential infor- mation security incidents.	yes	yes	n/a - This is new for ISO 27001:2022. There is no correspondence of the ISO 27001:2022 standard with ISO 27018:2019 and ISO 27017:2015.				risk assessment business requirement best practice

Databricks ISO 27001 / 27018 / 27017 / 27701 Statement of Applicability.

ISMS and PIMS
Last updated: 3/23/2023 version 7
Company Confidential. If printed, this is not the authoritative version.
Note: "n/a" implies a new requirement specifically for ISO 27001:2022 so there is no correspondence of the ISO 27001:2022 standanrd with ISO 27018:2019 and ISO 27017:2015.

			ISO 27001:2022		ISO 27018:2019		ISO 27017:2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion or exclusion
A.8.17	Clock synchronization	Control The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.8.18	Use of privileged utility programs	Control The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.8.19	Installation of software on operational systems	Control Procedures and measures shall be implemented to securely manage software installation on operational systems.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.8.20	Networks security	Control Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.8.21	Security of network services	Control Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.8.22	Segregation of networks	Control Groups of information services, users and information systems shall be segregated in the organization’s networks.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.8.23	Web filtering	Control Access to external websites shall be managed to reduce exposure to malicious content.	yes	yes	n/a - This is new for ISO 27001:2022. There is no correspondence of the ISO 27001:2022 standard with ISO 27018:2019 and ISO 27017:2015.				risk assessment business requirement best practice
A.8.24	Use of cryptography	Control Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.8.25	Secure development life cycle	Control Rules for the secure development of software and systems shall be established and applied.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.8.26	Application security require- ments	Control Information security requirements shall be identified, specified and approved when developing or acquiring applications.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.8.27	Secure system architecture and engineering principles	Control Principles for engineering secure systems shall be established, docu- mented, maintained and applied to any information system development activities.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.8.28	Secure coding	Control Secure coding principles shall be applied to software development.	yes	yes	n/a - This is new for ISO 27001:2022. There is no correspondence of the ISO 27001:2022 standard with ISO 27018:2019 and ISO 27017:2015.				risk assessment business requirement best practice

Databricks ISO 27001 / 27018 / 27017 / 27701 Statement of Applicability.

ISMS and PIMS
Last updated: 3/23/2023 version 7
Company Confidential. If printed, this is not the authoritative version.
Note: "n/a" implies a new requirement specifically for ISO 27001:2022 so there is no correspondence of the ISO 27001:2022 standanrd with ISO 27018:2019 and ISO 27017:2015.

			ISO 27001:2022		**ISO 27018:2019**		**ISO 27017:2015**		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion or exclusion
A.8.29	Security testing in development and acceptance	Control Security testing processes shall be defined and implemented in the development life cycle.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.8.30	Outsourced development	Control The organization shall direct, monitor and review the activities related to outsourced system development.	no	no	no	no	no	no	system or software development is not outsourced, thus the requirement is not applicable for Datacbricks. risk assessment
A.8.31	Separation of development, test and production environments	Control Development, testing and production environments shall be separated and secured.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.8.32	Change management	Control Changes to information processing facilities and information systems shall be subject to change management procedures.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.8.33	Test information	Control Test information shall be appropriately selected, protected and managed.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.8.34	Protection of information sys- tems during audit testing	Control Audit tests and other assurance activities involving assessment of op- erational systems shall be planned and agreed between the tester and appropriate management.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement

Databricks ISO 27018 Appendix A Statement of Applicability. Public cloud PII processor extended control set for PII protection.

ISMS
Last updated: 3/23/202 version 7
Company Confidential. If printed, this is not the authoritative version.

			ISO 27018:2019 Appendix A		
Section	Section Title	Section Objective	Included	Implemented	Justification for
A.2	**Consent and Choice**				
A.2.1	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 fulfil their obligation to facilitate the exercise of PII principals’ rights to access, correct and/or erase PII pertaining to them.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.3	**Purpose Legitimacy and Specification**				
A.3.1	Public cloud PII processor’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.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.3.2	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.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.5	**Data Minimization**				
A.5.1	Secure erasure of temporary files	Temporary files and documents should be erased or destroyed within a specified, documented period.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.6	**Use, Retention and Disclosure Limitation**				

Databricks ISO 27018 Appendix A Statement of Applicability. Public cloud PII processor extended control set for PII protection.

ISMS
Last updated: 3/23/202 version 7
Company Confidential. If printed, this is not the authoritative version.

			ISO 27018:2019 Appendix A		
Section	Section Title	Section Objective	Included	Implemented	Justification for
A.6.1	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.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.6.2	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.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.8	**Openness, Transparency and Notice**				
A.8.1	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 cloud service customers before their use.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.10	**Accountability**				
A.10.1	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.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.10.2	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).	Yes	Yes	Public cloud PII processor extended control set for PII protection

Databricks ISO 27018 Appendix A Statement of Applicability. Public cloud PII processor extended control set for PII protection.

ISMS
Last updated: 3/23/202 version 7
Company Confidential. If printed, this is not the authoritative version.

			ISO 27018:2019 Appendix A		
Section	Section Title	Section Objective	Included	Implemented	Justification for
A.10.3	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.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11	**Information Security**				
A.11.1	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.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.2	Restriction of the creation of hardcopy material	The creation of hardcopy material displaying PII should be restricted.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.3	Control and logging of data restoration	There should be a procedure for, and a log of, data restoration efforts.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.4	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 be accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.5	Use of unencrypted portable storage media and devices	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.	Yes	Yes	Public cloud PII processor extended control set for PII protection

Databricks ISO 27018 Appendix A Statement of Applicability. Public cloud PII processor extended control set for PII protection.

ISMS
Last updated: 3/23/202 version 7
Company Confidential. If printed, this is not the authoritative version.

			ISO 27018:2019 Appendix A		
Section	Section Title	Section Objective	Included	Implemented	Justification for
A.11.6	Encryption of PII transmitted over public data-transmission networks	PII that is transmitted over public data-transmission networks should be encrypted prior to transmission.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.7	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.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.8	Unique use 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.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.9	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.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.10	User ID management	De-activated or expired user IDs should not be granted to other individuals.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.11	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.	Yes	Yes	Public cloud PII processor extended control set for PII protection

Databricks ISO 27018 Appendix A Statement of Applicability. Public cloud PII processor extended control set for PII protection.

ISMS
Last updated: 3/23/202 version 7
Company Confidential. If printed, this is not the authoritative version.

			ISO 27018:2019 Appendix A		
Section	Section Title	Section Objective	Included	Implemented	Justification for
A.11.12	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.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.13	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.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.12	**Privacy Compliance**				
A.12.1	Geographical location of PII	The public cloud PII processor should specify and document the countries in which PII might possibly be stored.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.12.2	Intended destination of PII	PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.	Yes	Yes	Public cloud PII processor extended control set for PII protection

Databricks ISO 27017 Appendix B Statement of Applicability. Cloud service providers and customers extended control set for provision and user of cloud services.

ISMS
Last updated: 3/23/2023 version 7
Company Confidential. If printed, this is not the authoritative version.

			ISO 27017 : 2015 Appendix B		
Section	Section Title	Section Objective	Included	Implemented	Justification for inclusion or exclusion
CLD.6.3	**Relationship between cloud service customer and cloud service provider**	**To ensure that the information security is implemented and operated in accordance with the organizational security policies and standards.**			
CLD.6.3.1	Shared roles and responsibilities within a cloud computing environment	Responsibilities for shared information security roles in the use of the cloud service should be allocated to identified	Yes	Yes	Cloud service providers and customers extended control set for provision and user of cloud services
CLD.8.1	**Responsibility for assets**	**To ensure that the information security is implemented and operated in accordance with the organizational security policies and standards.**			
CLD.8.1.5	Removal of cloud service customer assets	Assets of the cloud service customer that are on the cloud service provider's premises should be removed, and returned if necessary, in a timely manner upon termination of the cloud service agreement.	Yes	Yes	Cloud service providers and customers extended control set for provision and user of cloud services
CLD.9.5	**Access control of cloud service customer data in shared virtual environment**	**To ensure that the information security is implemented and operated in accordance with the organizational security policies and standards.**			
CLD.9.5.1	Segregation in virtual computing environments	A cloud service customer's virtual environment running on a cloud service should be protected from other cloud service customers and unauthorized persons.	Yes	Yes	Cloud service providers and customers extended control set for provision and user of cloud services
CLD.9.5.2	Virtual machine hardening	Virtual machines in a cloud computing environment should be hardened to meet business needs.	Yes	Yes	Cloud service providers and customers extended control set for provision and user of cloud services
CLD.12.1	**Operational procedures and responsibilities**	**To ensure that the information security is implemented and operated in accordance with the organizational security policies and standards.**			
CLD.12.1.5	Administrator's operational security	Procedures for administrative operations of a cloud computing environment should be defined, documented and monitored.	Yes	Yes	Cloud service providers and customers extended control set for provision and user of cloud services

Databricks ISO 27017 Appendix B Statement of Applicability. Cloud service providers and customers extended control set for provision and user of cloud services.

ISMS
Last updated: 3/23/2023 version 7
Company Confidential. If printed, this is not the authoritative version.

			ISO 27017 : 2015 Appendix B		
Section	Section Title	Section Objective	Included	Implemented	Justification for inclusion or exclusion
CLD.12.4	**Logging and monitoring**	**To ensure that the information security is implemented and operated in accordance with the organizational security policies and standards.**			
CLD.12.1.5	Monitoring of Cloud Services	The cloud service customer should have the capability to monitor specified aspects of the operation of the cloud services that the cloud service customer uses.	Yes	Yes	Cloud service providers and customers extended control set for provision and user of cloud services
CLD.13.1	**Network security management**	**To ensure that the information security is implemented and operated in accordance with the organizational security policies and standards.**			
CLD.13.1.4	Alignment of security management for virtual and physical networks	Upon configuration of virtual networks, consistency of configurations between virtual and physical networks should be verified based on the cloud service provider's network security policy.	Yes	Yes	Cloud service providers and customers extended control set for provision and user of cloud services

Databricks ISO 27701 Appendix C Statement of Applicability. PIMS-specific reference control objectives and controls (PII Processors)

PIMS
Last updated: 3/23/2023 version 1
Company Confidential. If printed, this is not the authoritative version.

			ISO 27701:2019 Appendix C		
Section	Section Title	Section Objective	Included	Implemented	Justification for inclusion or exclusion
B.8.2	**Conditions for collection and processing**				
B.8.2.1	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).	yes	yes	PIMS-specific reference control objectives and controls (PII Processors)
B.8.2.2	Organization's purpose	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.	yes	yes	PIMS-specific reference control objectives and controls (PII Processors)
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.	yes	yes	PIMS-specific reference control objectives and controls (PII Processors)
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.	yes	yes	PIMS-specific reference control objectives and controls (PII Processors)
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.	yes	yes	PIMS-specific reference control objectives and controls (PII Processors)
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.	yes	yes	PIMS-specific reference control objectives and controls (PII Processors)
B.8.3	**Obligations to PII principals**				
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.	yes	yes	PIMS-specific reference control objectives and controls (PII Processors)
B.8.4	**Privacy by design and by default**				
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.	yes	yes	PIMS-specific reference control objectives and controls (PII Processors)
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.	yes	yes	PIMS-specific reference control objectives and controls (PII Processors)
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.	yes	yes	PIMS-specific reference control objectives and controls (PII Processors)
B.8.5	**PII sharing, transfer and disclosure**				
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.	yes	yes	PIMS-specific reference control objectives and controls (PII Processors)
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.	yes	yes	PIMS-specific reference control objectives and controls (PII Processors)

Databricks ISO 27701 Appendix C Statement of Applicability. PIMS-specific reference control objectives and controls (PII Processors)

PIMS
Last updated: 3/23/2023 version 1
Company Confidential. If printed, this is not the authoritative version.

			ISO 27701:2019 Appendix C		
Section	Section Title	Section Objective	Included	Implemented	Justification for inclusion or exclusion
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.	yes	yes	PIMS-specific reference control objectives and controls (PII Processors)
B.8.5.4	Notification of PII disclosure requests	The organization shall notify the customer of any legally binding requests for disclosure of PII.	yes	yes	PIMS-specific reference control objectives and controls (PII Processors)
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.	yes	yes	PIMS-specific reference control objectives and controls (PII Processors)
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.	yes	yes	PIMS-specific reference control objectives and controls (PII Processors)
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.	yes	yes	PIMS-specific reference control objectives and controls (PII Processors)
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.	yes	yes	PIMS-specific reference control objectives and controls (PII Processors)