

simac



Statement of Applicability

Simac Triangle

ISO 27701:2019

29-08-2024

Version 1.0

Introduction

This document includes the Statement of Applicability for the purpose of certification for the ISO 27701:2019 standard. The objective of this document is to identify the appropriate controls that should be implemented to monitor and manage the threats against Simac and its business processes. The controls have been identified on the basis of the ISO 27701:2019 standard included controls of the standard. The applicability is shown for each control. If a control does not apply, an explanation will be given for this.

Management statement

The Management Board of Simac hereby declares the controls stated in this declaration of applicability to be ratified in relation to the risk analyzes performed and accepts the residual risk of controls not taken.

Statement of Applicability - ISO 27701:2019

Legend - Reason for application	
Best practice	Objectives and controls that are directly or indirectly related to mandatory objectives and controls in the ISO 27701:2019 standard or that are accepted as best practices.
Risk analysis	Objectives and controls directly related to an identified risk.
Laws and regulations	Objectives and controls directly related to laws and regulations.
Contract	Objectives and controls directly related to contractual obligations.

Controls			In scope	Implemented	Reason (not) in scope
A.7	Additional ISO/IEC 27002 guidance for PII controllers				
A.7.1	General	The guidance in Clause 6 and the additions in this clause create the PIMS-specific guidance for PII controllers. The implementation guidance documented in this clause relate to the controls listed in Annex A.	Yes	Yes	Best practice
A.7.2	Conditions for collection and processing				
A.7.2.1	Identify and document purpose	The organization should identify and document the specific purposes for which the PII will be processed.	Yes	Yes	Laws and regulations
A.7.2.2	Identify lawful basis	The organization should determine, document and comply with the relevant lawful basis for the processing of PII for the identified purposes.	Yes	Yes	Laws and regulations
A.7.2.3	Determine when and how consent is to be obtained	The organization should determine and document a process by which it can demonstrate if, when and how consent for the processing of PII was obtained from PII principals.	Yes	Yes	Laws and regulations
A.7.2.4	Obtain and record consent	The organization should obtain and record consent from PII principals according to the documented processes.	Yes	Yes	Laws and regulations
A.7.2.5	Privacy impact assessment	The organization should assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of PII or changes to existing processing of PII is planned.	Yes	Yes	Risk analysis, Laws and regulations

A.7.2.6	Contracts with PII processors	The organization should have a written contract with any PII processor that it uses, and should ensure that their contracts with PII processors address the implementation of the appropriate controls in Annex B.	Yes	Yes	Laws and regulations, Contract
A.7.2.7	Joint PII controller	The organization should determine respective roles and responsibilities for the processing of PII (including PII protection and security requirements) with any joint PII controller.	Yes	Yes	Laws and regulations
A.7.2.8	Records related to processing PII	The organization should determine and securely maintain the necessary records in support of its obligations for the processing of PII.	Yes	Yes	Laws and regulations
A.7.3	Obligations to PII principals				
A.7.3.1	Determining and fulfilling obligations to PII principals	The organization should determine and document their legal, regulatory and business obligations to PII principals related to the processing of their PII and provide the means to meet these obligations.	Yes	Yes	Laws and regulations
A.7.3.10	Automated decision making	The organization should identify and address obligations, including legal obligations, to the PII principals resulting from decisions made by the organization which are related to the PII principal based solely on automated processing of PII.	Yes	Yes	Laws and regulations
A.7.3.2	Determining information for PII principals	The organization should determine and document the information to be provided to PII principals regarding the processing of their PII and the timing of such a provision.	Yes	Yes	Laws and regulations
A.7.3.3	Providing information to PII principals	The organization should provide PII principals with clear and easily accessible information identifying the PII controller and describing the processing of their PII.	Yes	Yes	Laws and regulations
A.7.3.4	Providing mechanism to modify or withdraw consent	The organization should provide a mechanism for PII principals to modify or withdraw their consent.	Yes	Yes	Laws and regulations
A.7.3.5	Providing mechanism to object to PII processing	The organization should provide a mechanism for PII principals to object to the processing of their PII.	Yes	Yes	Laws and regulations
A.7.3.6	Access, correction and/or erasure	The organization should implement policies, procedures and/or mechanisms to meet their obligations to PII principals to access, correct and/or erase their PII.	Yes	Yes	Laws and regulations
A.7.3.7	PII controllers' obligations to inform third parties	The organization should inform third parties with whom PII has been shared of any modification, withdrawal or objections pertaining to the shared PII, and implement appropriate policies, procedures and/or mechanisms to do so.	Yes	Yes	Laws and regulations
A.7.3.8	Providing copy of PII processed	The organization should be able to provide a copy of the PII that is processed when requested by the PII principal.	Yes	Yes	Laws and regulations
A.7.3.9	Handling requests	The organization should define and document policies and procedures for handling and responding to legitimate requests from PII principals.	Yes	Yes	Laws and regulations
A.7.4	Privacy by design and privacy by default				
A.7.4.1	Limit collection	The organization should limit the collection of PII to the minimum that is relevant, proportional and necessary for the identified purposes.	Yes	Yes	Laws and regulations
A.7.4.2	Limit processing	The organization should limit the processing of PII to that which is adequate, relevant and necessary for the identified purposes.	Yes	Yes	Laws and regulations

A.7.4.3	Accuracy and quality	The organization should ensure and document that PII is as accurate, complete and up-to-date as is necessary for the purposes for which it is processed, throughout the life-cycle of the PII.	Yes	Yes	Laws and regulations
A.7.4.4	PII minimization objectives	The organization should define and document data minimization objectives and what mechanisms (such as de-identification) are used to meet those objectives.	Yes	Yes	Laws and regulations
A.7.4.5	PII de-identification and deletion at the end of processing	The organization should either delete PII or render it in a form which does not permit identification or re-identification of PII principals, as soon as the original PII is no longer necessary for the identified purpose(s).	Yes	Yes	Laws and regulations
A.7.4.6	Temporary files	The organization should 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	Contract
A.7.4.7	Retention	The organization should not retain PII for longer than is necessary for the purposes for which the PII is processed.	Yes	Yes	Laws and regulations
A.7.4.8	Disposal	The organization should have documented policies, procedures and/or mechanisms for the disposal of PII.	Yes	Yes	Laws and regulations
A.7.4.9	PII transmission controls	The organization should subject PII transmitted (e. g. sent to another organization) over a datatransmission network to appropriate controls designed to ensure that the data reaches its intended destination.	Yes	Yes	Best practice
A.7.5	PII sharing, transfer, and disclosure				
A.7.5.1	Identify basis for PII transfer between jurisdictions	The organization should identify and document the relevant basis for transfers of PII between jurisdictions.	Yes	Yes	Laws and regulations
A.7.5.2	Countries and international organizations to which PII can be transferred	The organization should specify and document the countries and international organizations to which PII can possibly be transferred.	Yes	Yes	Laws and regulations, Contract
A.7.5.3	Records of transfer of PII	The organization should record transfers of PII to or from third parties and ensure cooperation with those parties to support future requests related to obligations to the PII principals.	Yes	Yes	Laws and regulations
A.7.5.4	Records of PII disclosure to third parties	The organization should record disclosures of PII to third parties, including what PII has been disclosed, to whom and at what time.	Yes	Yes	Laws and regulations
B.8	Additional ISO/IEC 27002 guidance for PII processors				
B.8.1	General	The guidance in Clause 6 and the additions of this clause create the PIMS-specific guidance for PII processors. The implementation guidance documented in this clause relate to the controls listed in Annex B.	Yes	Yes	Best practice
B.8.2	Conditions for collection and processing				
B.8.2.1	Customer agreement	The organization should 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	Contract

B.8.2.2	Organization's purposes	The organization should 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	Contract
B.8.2.3	Marketing and advertising use	The organization should 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 should not make providing such consent a condition for receiving the service.	Yes	Yes	Contract
B.8.2.4	Infringing instruction	The organization should inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation.	Yes	Yes	Laws and regulations
B.8.2.5	Customer obligations	The organization should provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations.	Yes	Yes	Contract
B.8.2.6	Records related to processing PII	The organization should 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	Laws and regulations, Contract
B.8.3	Obligations to PII principals				
B.8.3.1	Obligations to PII principals	The organization should provide the customer with the means to comply with its obligations related to PII principals.	Yes	Yes	Laws and regulations, Contract
B.8.4	Privacy by design and privacy by default				
B.8.4.1	Temporary files	The organization should 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	Contract
B.8.4.2	Return, transfer or disposal of PII	The organization should provide the ability to return, transfer and/or disposal of PII in a secure manner. It should also make its policy available to the customer.	Yes	Yes	Laws and regulations, Contract
B.8.4.3	PII transmission controls	The organization should subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.	Yes	Yes	Contract
B.8.5	PII sharing, transfer, and disclosure				
B.8.5.1	Basis for PII transfer between jurisdictions	The organization should 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	Laws and regulations
B.8.5.2	Countries and international organizations to which PII can be transferred	The organization should specify and document the countries and international organizations to which PII can possibly be transferred.	Yes	Yes	Laws and regulations, Contract
B.8.5.3	Records of PII disclosure to third parties	The organization should record disclosures of PII to third parties, including what PII has been disclosed, to whom and when.	Yes	Yes	Laws and regulations, Contract

B.8.5.4	Notification of PII disclosure requests	The organization should notify the customer of any legally binding requests for disclosure of PII.	Yes	Yes	Laws and regulations, Contract
B.8.5.5	Legally binding PII disclosures	The organization should 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	Laws and regulations
B.8.5.6	Disclosure of subcontractors used to process PII	The organization should disclose any use of subcontractors to process PII to the customer before use.	Yes	Yes	Laws and regulations, Contract
B.8.5.7	Engagement of a subcontractor to process PII	The organization should only engage a subcontractor to process PII according to the customer contract.	Yes	Yes	Laws and regulations, Contract
B.8.5.8	Change of subcontractor to process PII	The organization should, 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	Laws and regulations, Contract