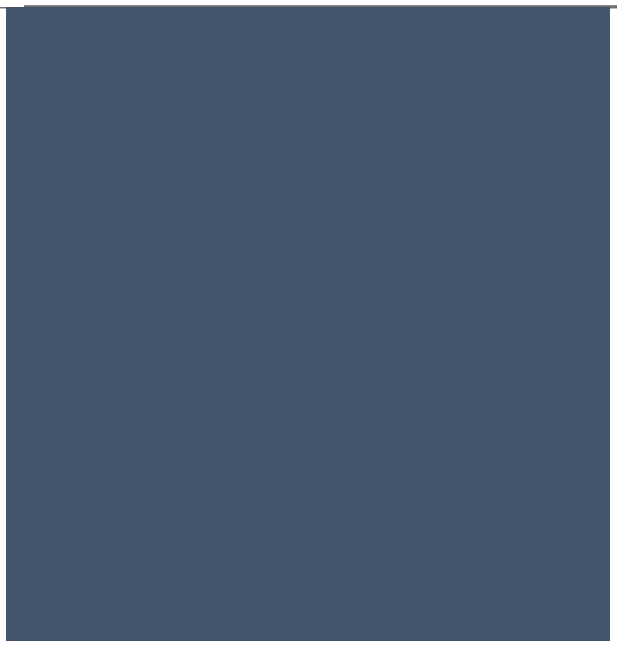

SK-ISO-27.00 Statement of Applicability

Table of Contents

Document Demographics

Organization	**SkyKick**
Document Classification	Public
Owner	Compliance Officer
Document Title	SkyKick-ISO27-00 Statement of Applicability
Document Location	Policies & Procedures SharePoint Site https://cloudvisorsllc.sharepoint.com/policies
Author(s)	Brad Younge & Gerard Doeswijk
Document No.	SK-ISO-27.00

Revision History

Version No.	Date	Author(s)	Summary of Changes
0.1	08/26/2021	Gerard Doeswijk	Initial draft for review
1.0	11/29/2021	Brad Younge & Gerard Doeswijk	Initial version approved for publication
1.1	01/26/2022	Dave Gill	Minor revision
1.2	03/22/2022	Dave Gill & Gerard Doeswijk	Major revision and comments for InfoSec team
1.3	03/29/2022	Dave Gill	Minor revision based on feedback InfoSec team
1.4	03/30/2022	Dave Gill & AIDA Crone	Review
1.5	04/07/2022	Dave Gill & Gerard Doeswijk	Reviewing comments and text revisions
1.6	04/29/2022	Gerard Doeswijk	Final review of comments and revisions by engineering for signoff by DAA.
2.0	05/19/2022	Brad Younge	Sign-off for publication
2.1	06/06/2022	Gerard Doeswijk	Revision to address external audit findings
3.0	06/08/2022	Brad Younge	Sign-off for publication
3.1	03/29/2023	Gerard Doeswijk	Annual review incorporating ISO27701 and new number format
4.0	03/29/2023	Brad Younge	Sign-off for publication
4.1	08/30/2023	Gerard Doeswijk	Updates to Annex B control descriptions for ISO27701
5.0		Brad Younge	Sign-off for publication

August 31, 2023 | 6:16 AM PDT

1 Purpose, scope, and users

The purpose of this document is to define which controls (safeguards) are appropriate to be implemented in SkyKick, the group of companies, the objectives of these controls and how they are implemented, as well as to approve residual risks and formally approve the implementation of said controls.

This document includes all applicable controls listed in Annex A of the ISO 27001 standard and Annex B (Processor) of the ISO27701 standard. ISO 27701 Annex A (Controller) is not in scope.

Controls are applicable to the entirety of the Information Security & Privacy Management System scope and all personal data processing activities.

This document is provided to all interested parties that require a copy of the SkyKick ISO certificates and is published online in the SkyKick Trust Center.

2 Reference documents

- ISO/IEC 27001 standard, clause 6.1.3 d
- ISO/IEC 27701 standard
- SkyKick Information Security & Privacy Risk Management Policy

3 Applicability of Controls

The information contained in this document describes the Information Security, Risk & Privacy Program Statement of Applicability for SkyKick as of the revision date specified. The information contained in this document is subject to change at any time and does not represent a commitment, contractual or otherwise, on the part of SkyKick.

3.1 ISO27001:2013 Annex A

The following controls from ISO 27001 Annex A are applicable and have been validated against ISO27701:

				Justification for Implementation			
ID	**Controls according to ISO/IEC27001**	**Control Objectives**	**Applicable**	**Risk-based**	**Best Practice**	**Contractual**	**Implementation Status**
A.05.00.00	**Information security policies**						
A.05.01.00	***Management direction for information security***	*To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.*					
A.05.01.01	Policies for information security		Y	•	•	•	CMMI-3
A.05.01.02	Review of the policies for information security		Y	•	•	•	CMMI-3
A.06.00.00	**Organization of information security**						
A.06.01.00	***Internal organization***	*To establish a management framework to initiate and control the implementation and operation of information security within the organization.*					
A.06.01.01	Information security roles and responsibilities		Y	•	•	•	CMMI-3
A.06.01.02	Segregation of duties		Y	•	•	•	CMMI-2
A.06.01.03	Contact with authorities		Y	•	•	•	CMMI-2
A.06.01.04	Contact with special interest groups		Y	•	•	•	CMMI-2
A.06.01.05	Information security in project management		Y	•	•	•	CMMI-2
A.06.02.00	***Mobile devices and teleworking***	*To ensure the security of teleworking and use of mobile devices.*					
A.06.02.01	Mobile device policy		Y	•	•	•	CMMI-2
A.06.02.02	Teleworking		Y	•	•	•	CMMI-2
A.07.00.00	**Human resource security**						
A.07.01.00	***Prior to employment***	*To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.*					
A.07.01.01	Screening		Y	•	•	•	CMMI-2
A.07.01.02	Terms and conditions of employment		Y	•	•	•	CMMI-2
A.07.02.00	***During employment***	*To ensure that employees and contractors are aware of and fulfil their information security responsibilities.*					
A.07.02.01	Management responsibilities		Y	•	•	•	CMMI-2

A.07.02.02	Information security awareness, education, and training		Y	●	●	●	CMMI-2
A.07.02.03	Disciplinary process		Y	●	●	●	CMMI-2
A.07.03.00	***Termination and change of employment***	*To protect the organization's interests as part of the process of changing or terminating employment.*					
A.07.03.01	Termination or change of employment responsibilities		Y	●	●	●	CMMI-2
A.08.00.00	**Asset management**						
A.08.01.00	***Responsibility for assets***	*To identify organizational assets and define appropriate protection responsibilities.*					
A.08.01.01	Inventory of assets		Y	●	●	●	CMMI-2
A.08.01.02	Ownership of assets		Y	●	●	●	CMMI-2
A.08.01.03	Acceptable use of assets		Y	●	●	●	CMMI-2
A.08.01.04	Return of assets		Y	●	●	●	CMMI-2
A.08.02.00	***Information classification***	*To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.*					
A.08.02.01	Classification of information		Y	●	●	●	CMMI-2
A.08.02.02	Labelling of information		Y	●	●	●	CMMI-2
A.08.02.03	Handling of assets		Y	●	●	●	CMMI-2
A.08.03.00	***Media handling***	*To prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.*					
A.08.03.01	Management of removable media		Y	●	●	●	CMMI-2
A.08.03.02	Disposal of media		Y	●	●	●	CMMI-2
A.08.03.03	Physical media transfer		Y	●	●	●	CMMI-2
A.09.00.00	**Access control**						
A.09.01.00	***Business requirements of access control***	*To limit access to information and information processing facilities.*					
A.09.01.01	Access control policy		Y	●	●	●	CMMI-2
A.09.01.02	Access to networks and network services		Y	●	●	●	CMMI-2
A.09.02.00	***User access management***	*To ensure authorized user access and to prevent unauthorized access to systems and services.*					
A.09.02.01	User registration and de-registration		Y	●	●	●	CMMI-2
A.09.02.02	User access provisioning		Y	●	●	●	CMMI-2
A.09.02.03	Management of privileged access rights		Y	●	●	●	CMMI-2
A.09.02.04	Management of secret authentication information of users		Y	●	●	●	CMMI-2
A.09.02.05	Review of user access rights		Y	●	●	●	CMMI-2
A.09.02.06	Removal or adjustment of access rights		Y	●	●	●	CMMI-2
A.09.03.00	***User responsibilities***	*To make users accountable for safeguarding their authentication information.*					

A.09.03.01	Use of secret authentication information		Y	●	●	●	CMMI-3
A.09.04.00	***System and application access control***	*To prevent unauthorized access to systems and applications.*					
A.09.04.01	Information access restriction		Y	●	●	●	CMMI-2
A.09.04.02	Secure log-on procedures		Y	●	●	●	CMMI-2
A.09.04.03	Password management system		Y	●	●	●	CMMI-3
A.09.04.04	Use of privileged utility programs		Y	●	●	●	CMMI-3
A.09.04.05	Access control to program source code		Y	●	●	●	CMMI-3
A.10.00.00	**Cryptography**						
A.10.01.00	***Cryptographic controls***	*To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.*					
A.10.01.01	Policy on the use of cryptographic controls		Y	●	●	●	CMMI-2
A.10.01.02	Key management		Y	●	●	●	CMMI-2
A.11.00.00	**Physical and environmental security**						
A.11.01.00	***Secure areas***	*To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.*					
A.11.01.01	Physical security perimeter		Y	●	●	●	CMMI-2
A.11.01.02	Physical entry controls		Y	●	●	●	CMMI-2
A.11.01.03	Securing offices, rooms and facilities		Y	●	●	●	CMMI-2
A.11.01.04	Protecting against external and environmental threats		Y	●	●	●	CMMI-2
A.11.01.05	Working in secure areas		Y	●	●	●	CMMI-2
A.11.01.06	Delivery and loading areas		Y	●	●	●	CMMI-2
A.11.02.00	***Equipment***	*To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.*					
A.11.02.01	Equipment siting and protection		Y	●	●	●	CMMI-2
A.11.02.02	Supporting utilities		Y	●	●	●	CMMI-2
A.11.02.03	Cabling security		Y	●	●	●	CMMI-2
A.11.02.04	Equipment maintenance		Y	●	●	●	CMMI-2
A.11.02.05	Removal of assets		Y	●	●	●	CMMI-2
A.11.02.06	Security of equipment and assets off-premises		Y	●	●	●	CMMI-2
A.11.02.07	Secure disposal or reuse of equipment		Y	●	●	●	CMMI-2
A.11.02.08	Unattended user equipment		Y	●	●	●	CMMI-2
A.11.02.09	Clear desk and clear screen policy		Y	●	●	●	CMMI-2
A.12.00.00	**Operations security**						
A.12.01.00	***Operational procedures and responsibilities***	*To ensure correct and secure operations of information processing facilities.*					

A.12.01.01	Documented operating procedures		Y	●	●	●	CMMI-2
A.12.01.02	Change management		Y	●	●	●	CMMI-2
A.12.01.03	Capacity management		Y	●	●	●	CMMI-2
A.12.01.04	Separation of development, testing and operational environments		Y	●	●	●	CMMI-2
A.12.02.00	***Protection from malware***	*To ensure that information and information processing facilities are protected against malware.*					
A.12.02.01	Controls against malware		Y	●	●	●	CMMI-2
A.12.03.00	***Backup***	*To protect against loss of data.*					
A.12.03.01	Information backup		Y	●	●	●	CMMI-2
A.12.04.00	***Logging and monitoring***	*To record events and generate evidence.*					
A.12.04.01	Event logging		Y	●	●	●	CMMI-2
A.12.04.02	Protection of log information		Y	●	●	●	CMMI-2
A.12.04.03	Administrator and operator logs		Y	●	●	●	CMMI-2
A.12.04.04	Clock synchronization		Y	●	●	●	CMMI-2
A.12.05.00	***Control of operational software***	*To ensure the integrity of operational systems.*					
A.12.05.01	Installation of software on operational systems		Y	●	●	●	CMMI-2
A.12.06.00	***Technical vulnerability management***	*To prevent exploitation of technical vulnerabilities.*					
A.12.06.01	Management of technical vulnerabilities		Y	●	●	●	CMMI-2
A.12.06.02	Restrictions on software installation		Y	●	●	●	CMMI-2
A.12.07.00	***Information systems audit considerations***	*To minimize the impact of audit activities on operational systems.*					
A.12.07.01	Information systems audit controls		Y	●	●	●	CMMI-2
A.13.00.00	**Communications security**						
A.13.01.00	***Network security management***	*To ensure the protection of information in networks and its supporting information processing facilities.*					
A.13.01.01	Network controls		Y	●	●	●	CMMI-2
A.13.01.02	Security of network services		Y	●	●	●	CMMI-2
A.13.01.03	Segregation in networks		Y	●	●	●	CMMI-2
A.13.02.00	***Information transfer***	*To maintain the security of information transferred within an organization and with any external entity.*					
A.13.02.01	Information transfer policies and procedures		Y	●	●	●	CMMI-2
A.13.02.02	Agreements on information transfer		Y	●	●	●	CMMI-2
A.13.02.03	Electronic messaging		Y	●	●	●	CMMI-2
A.13.02.04	Confidentiality or nondisclosure agreements		Y	●	●	●	CMMI-2
A.14.00.00	**System acquisition, development, and maintenance**						

A.14.01.00	***Security requirements of information systems***	*To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.*					
A.14.01.01	Information security requirements analysis and specification		Y	●	●	●	CMMI-2
A.14.01.02	Securing application services on public networks		Y	●	●	●	CMMI-2
A.14.01.03	Protecting application services transactions		Y	●	●	●	CMMI-2
A.14.02.00	***Security in development and support processes***	*To ensure that information security is designed and implemented within the development lifecycle of information systems.*					
A.14.02.01	Secure development policy		Y	●	●	●	CMMI-2
A.14.02.02	System change control procedures		Y	●	●	●	CMMI-2
A.14.02.03	Technical review of applications after operating platform changes		Y	●	●	●	CMMI-2
A.14.02.04	Restrictions on changes to software packages		Y	●	●	●	CMMI-2
A.14.02.05	Secure system engineering principles		Y	●	●	●	CMMI-2
A.14.02.06	Secure development environment		Y	●	●	●	CMMI-2
A.14.02.07	Outsourced development		Y	●	●	●	CMMI-2
A.14.02.08	System security testing		Y	●	●	●	CMMI-2
A.14.02.09	System acceptance testing		Y	●	●	●	CMMI-2
A.14.03.00	***Test data***	*To ensure the protection of data used for testing.*					
A.14.03.01	Protection of test data		Y	●	●	●	CMMI-2
A.15.00.00	**Supplier relationships**						
A.15.01.00	***Information security in supplier relationships***	*To ensure protection of the organization's assets that is accessible by suppliers*					
A.15.01.01	Information security policy for supplier relationships		Y	●	●	●	CMMI-2
A.15.01.02	Addressing security within supplier agreements		Y	●	●	●	CMMI-2
A.15.01.03	Information and communication technology supply chain		Y	●	●	●	CMMI-2
A.15.02.00	***Supplier service delivery management***	*To maintain an agreed level of information security and service delivery in line with supplier agreements.*					
A.15.02.01	Monitoring and review of supplier services		Y	●	●	●	CMMI-2
A.15.02.02	Managing changes to supplier services		Y	●	●	●	CMMI-2
A.16.00.00	**Information security incident management**						
A.16.01.00	***Management of information security incidents and improvements***	*To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.*					
A.16.01.01	Responsibilities and procedures		Y	●	●	●	CMMI-2
A.16.01.02	Reporting information security events		Y	●	●	●	CMMI-2
A.16.01.03	Reporting information security weaknesses		Y	●	●	●	CMMI-2
A.16.01.04	Assessment of and decision on information security events		Y	●	●	●	CMMI-2

A.16.01.05	Response to information security incidents		Y	●	●	●	CMMI-2
A.16.01.06	Learning from information security incidents		Y	●	●	●	CMMI-2
A.16.01.07	Collection of evidence		Y	●	●	●	CMMI-2
A.17.00.00	**Information security aspects of business continuity management**						
A.17.01.00	***Information security continuity***	*Information security continuity should be embedded in the organization's business continuity management systems.*					
A.17.01.01	Planning information security continuity		Y	●	●	●	CMMI-2
A.17.01.02	Implementing information security continuity		Y	●	●	●	CMMI-2
A.17.01.03	Verify, review and evaluate information security continuity		Y	●	●	●	CMMI-2
A.17.02.00	***Redundancies***	*To ensure availability of information processing facilities. Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.*					
A.17.02.01	Availability of information processing facilities		Y	●	●	●	CMMI-2
A.18.00.00	**Compliance**						
A.18.01.00	***Compliance with legal and contractual requirements***	*To avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security and of any security requirements.*					
A.18.01.01	Identification of applicable legislation and contractual requirements		Y	●	●	●	CMMI-3
A.18.01.02	Intellectual property rights		Y	●	●	●	CMMI-2
A.18.01.03	Protection of records		Y	●	●	●	CMMI-2
A.18.01.04	Privacy and protection of personally identifiable information		Y	●	●	●	CMMI-3
A.18.01.05	Regulation of cryptographic controls		Y	●	●	●	CMMI-2
A.18.02.00	***Information security reviews***	*To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.*					
A.18.02.01	Independent review of information security		Y	●	●	●	CMMI-3
A.18.02.02	Compliance with security policies and standards		Y	●	●	●	CMMI-2
A.18.02.03	Technical compliance review		Y	●	●	●	CMMI-2[1]

[1] The implementation status of the ISMS and the PIMS is measured using CMMI V1.3, from CMMI-1 initial, to CMMI-2 managed, to CMMI-3 defined, to CMMI-4 measured, through to CMMI-5 optimizing.

3.2 ISO27701:2019 Annex B

				Justification for Implementation			
ID	**Controls according to ISO/IEC27701**	**Control Objectives**	**Applicable**	**Risk-based**	**Best Practice**	**Contractual**	**Implementation Status**
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		Y	●	●	●	CMMI-2
B.8.2.2	Organization's purposes		Y	●	●	●	CMMI-2
B.8.2.3	Marketing and advertising use		Y	●	●	●	CMMI-2
B.8.2.4	Infringing instruction		Y	●	●	●	CMMI-2
B.8.2.5	Customer Obligations		Y	●	●	●	CMMI-2
B.8.2.6	Records related to processing PII		Y	●	●	●	CMMI-2
B.8.3	***Obligations to PII principles***	*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 principles		Y	●	●	●	CMMI-2
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		Y	●	●	●	CMMI-2
B.8.4.2	Return, transfer or disposal of PII		Y	●	●	●	CMMI-2
B.8.4.3	PII transmission controls		Y	●	●	●	CMMI-2
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 transfer between jurisdictions		Y	●	●	●	CMMI-2
B.8.5.2	Countries and international organizations to which PII can be transferred		Y	●	●	●	CMMI-2
B.8.5.3	Records of PII disclosure to third parties		Y	●	●	●	CMMI-2
B.8.5.4	Notification of PII disclosure requests		Y	●	●	●	CMMI-2
B.8.5.5	Legally binding PII disclosures		Y	●	●	●	CMMI-2
B.8.5.6	Disclosure of subcontractors used to process PII		Y	●	●	●	CMMI-2
B.8.5.7	Engagement of a of subcontractor to process PII		Y	●	●	●	CMMI-2
B.8.5.8	Change of subcontractors to process PII		Y	●	●	●	CMMI-2

4 Acceptance of Residual Risks

Since not all risks could be reduced in the risk management process, all residual risks are hereby accepted by the Designated Approving Authority (DAA) which is recorded through his formal approval in the Management Review or Steering Committee meeting and related document library.

4.1 Signature

DocuSigned by:
Brad Younge
E153103A8A794F6...
Brad Younge, CTO
August 31, 2023 | 6:16 AM PDT

5 Validity and document management

This document is valid as of its initial publication. The owner of this document must check and, if necessary, update the document at least annually, or as deemed necessary such as after a risk assessment review, material updates to the risk register or improvement planner.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of nonconformities due to unclearly defined implementation method of individual controls
- number of nonconformities due to unclearly defined control objectives
- number of controls for which the achievement of objectives cannot be measured