WHEN TRUST MATTERS

P1, IA Report

SkyKick LLC

Management System Certification

ISO/IEC 27001:2013, ISO/IEC 27701:2019

Audit Start - End date	2023/06/29 - 2023/08/31
Project Number	PRJN-267215-2021-MSC-NLD
DNV Team Leader	Roderick Krijgsman
Audit Team	Elena Bobkova, Marc Schipper
Prepared By	Roderick Krijgsman
Reported date	2023/09/01

Table of contents

Other Annexes

Introduction

This report summarizes the results and conclusions from the performed audit. The audit is performed as a formal part of the certification process with the aim to obtain or maintain certification of the management system. The key objective of a management system audit is to determine the conformity of the management system with the standard. Additionally to evaluate the effectiveness of the management system to ensure your organization is capable to achieve specified objectives and meet applicable statutory, regulatory and contractual requirements.

DNV

DNV is a global quality assurance and risk management company. Driven by our purpose of safeguarding life, property and the environment, we enable our customers to advance the safety and sustainability of their business. With origins stretching back to 1864 and operations in more than 100 countries, our experts are dedicated to helping customers make the world safer, smarter and greener.

As a world-leading certification body, DNV helps businesses assure the performance of their organizations, products, people, facilities and supply chains through certification, verification, assessment, and training services. Partnering with our customers, we build sustainable business performance and create stakeholder trust.

General information

Scope of certification

C595776(Draft) - ISO/IEC 27701:2019:
Privacy Information Management System for providing sales, software development, maintenance and support activities of cloud software including project management and integration services in the role of “processor”. This is in accordance with the Statement of Applicability version 5, dated 31 August 2023.

10000482117-MSC-UKAS-NLD(Issued/Current) - ISO/IEC 27001:2013:
Providing sales, software development, maintenance and support activities of cloud software including project management and integration services. This is inaccordance with the Statement of Applicability SK-ISO-27.00 version 4.0, dated March 29, 2023.

Scheme and Accredited Legal Entity

ISO/IEC 27701:2019:UKAS
DNV Business Assurance UK Limited
4th Floor, Vivo Building, 30 Stamford Street, London, SE1 9LQ, United Kingdom

ISO/IEC 27001:2013:UKAS
DNV Business Assurance UK Limited
4th Floor, Vivo Building, 30 Stamford Street, London, SE1 9LQ, United Kingdom

Statement of confidentiality

The contents of this report, including any notes and checklists completed during the audit will be treated in strictest confidence, and will not be disclosed to any third party without your written consent, except as required by the appropriate accreditation authorities.

Disclaimer

A management system audit is based on verification of a sample of available information. Consequently there is an element of uncertainty reflected in the audit findings. An absence of nonconformities does not mean that they do not exist in audited and/or other areas. Prior to awarding or renewing certification this report is also subject to an independent DNV internal review which may affect the report content and conclusions. An independent DNV internal review is also executed in case of major nonconformities raised during a periodic audit which may affect the conclusion and follow-up process indicated in this report.

Other results

Key points observed during the audit not included in the Focus Areas.

Positive indications

- The approach to implement Information Classification together with Data loss Prevention is exemplary. Setting up IC non-sensitive vs sensitive, classified per departmental classification. Implementation per BU.
- Staff can only used a privileged account when requested and granted via Azure AD PIM. The acquired privilege sessions are time limited and only by exception can the session duration altered.
- The local Systems manager has a pro-active approach concerning the hierarchical responsibilities of direct reports to a leaver.
- Organization has created a Privacy Management System that has a high maturity and has made it possible that the organisation is aware of changing legislation and compliance through a close relationship with legal counsel and proactive approach
- The organisation makes use of risk analysis based upon objective CMMI levels that will provide feedback on how to improve the risk treatment. The current model has been working for the organisation and it has made the risk model their own so that that they can quantitatively improve their risk treatment.

Main areas for improvement

Nonconformity (5.4.1 ISO 27701)

- Currently the risk analysis does not make clear which controls of Annex B of ISO 27701 are linked to which risk domains in the risk analysis or risk treatment.

Observations

- Currently, is not visible in the internal audit program “SK Internal Audit Workbook (Tab ISO27001 ISO 27701” that the Annex B elements were included during the rolling audit process and audits. However, it has been established that elements from Annex B ISO 27701 have been tested through the Data Pro Certification.

Opportunity for Improvement

- The desktop PC stored in the server room are not labelled. Status is unknown, likely to be decomissioned or disposed via certified data destruction.

Audit findings and compliance status

Number of nonconformities identified during this audit	**1**
Number of category 1 (major) nonconformities:	0
Number of category 2 (minor) nonconformities:	1
Number of observations identified during this audit	**1**
Number of opportunities for improvement identified during this audit	**1**
The status of corrective actions for nonconformities from previous audit was reviewed. **Number of nonconformities still not closed from previous audits**	**0**

Notes

1. For details of nonconformities, observations and opportunities for improvement,see List of findings
2. See definitions of findings in Annex B

Conclusions

- The audit was carried out without use of remote auditing techniques.
- The key audit objectives were achieved and the audit plan was followed without major changes.
- The general conclusions and key findings were presented, discussed and agreed at the closing meeting.
- There are no major changes affecting the management system since last audit.
- Nonconformities were not identified during the audit. The management system is considered effective and in compliance with the standard, based on the audit sample taken.
- The organization will be recommended for certification by the team leader when all nonconformities have been reviewed and accepted.
- The certificate remains valid as no nonconformities were identified during the audit.
- Necessary immediate corrections and corrective actions for the nonconformities are required to be implemented by the organization, see conditions in Handling of findings (annex).
- According to the conditions under Handling of findings the organization must give satisfactory response to the non-conformities within the given due date set by the Team Leader: 2023/09/08
- Although not an obligation, the Team Leader recommends that the observations are considered and responded to.
- Due to the positive result of the audit there is no need for a follow-up audit.
- The appropriateness of the certification scope (and boundaries) was evaluated by considering factors such as the organizational structure, site(s), processes and products/services. The conclusion is that the certification scope (and boundaries) is considered appropriate.
- The audit identified the following issues that impact the periodic audit programme for the current certification cycle: Integration of ISO 27701 into the PAP and the entity in USA.

- Based on consideration of the status of relevant factors such as number of personnel, geographical locations, processes and products, and complexity level of the organization, the conclusion is that there is no need to review the audit time.
- Based on evaluation of the commonality of processes performed and the management system used on each of the sites, including the central office authority and ability to exercise control when needed in any site, the conclusion is that the organization is eligible for a site sampling approach.

Next audit

Audit start date 2023/11/17

Annex A - Auditor statements

Verified elements of the standard	Objective evidence and result
Effectiveness of processes for management review	The minutes from the management review 3 March 2023 and associated documentation were assessed. The process is considered to be effective and no nonconformities towards the requirements of the standard were identified. The management review for ISO 27701 is integrated with the ISO 27001 managment review. The management review is available as documented information in ISMS Skykick, Management Review Meeting and notes in OneNote. The management review is conducted during the sprint and rolling reviews have been performed on the status of implementation. The Management review from now on is scheduled to be done annually but every ISMS-steering committee member is allowed to ask for a new Management review. Notes have been stored in OneNote with links to the discussed policies and monitoring dashboards.

Effectiveness of processes for internal audits	The programme for internal audits for the period 2023, and records from performed audits were assessed. The process is considered effective and no nonconformities towards the requirements of the standard were identified. The Internal audits are combined for ISO 27001, ISO 27701. The following records were assessed as basis for the conclusion: "SK Internal Audit Workbook (Tabblad ISO27001 ISO 27701)" and "230223 Internal audit report – ON-Site audit LLC d.d. 23-02-2023". The internal audit findings are available as documented information SK BV Audit log - findings and corrective actions.xlsx Audit findings have been identified and are registered also in the improvement register (The improvement - implementation status - corrective actions and improvement initiatives). The Rolling audit approach for continuous internal audits is described and manager in the internal audit planning (Audit planning 2023.MPP). During every ISMS Steering Meeting the scope for the next internal audit is discussed and approved and being performed by an external party together with DPO or SO.

Effectiveness of processes for handling of nonconformities (including incidents and customer and/or stakeholder complaints)	There were no complaints registered since the last audit. The internal audit findings are available as documented information SK BV Audit log - findings and corrective actions.xlsx Audit findings have been identified and are registered also in the improvement register (The improvement - implementation status – corrective actions and improvement initiatives). Data breaches and security incident procedures are defined. There haven't been any privacy incidents or registered data breaches (in scope of the audit). When they would happen these will be registered and a root cause analysis will be performed. Then this will be discussed during ISMS steering committee and corrective actions will be registered in the Teams overview with an owner and deadline.

Effectiveness of process for determining and addressing risks and opportunities relevant for the management system	hThe process is considered to be effective and in compliance with the requirements of the standard, with the exceptions noted in the List of findings. The conclusion is based on interviews with relevant managers and verification of the following activities and records: "SCF RMM – SK Risk management Workbook d.d. 21-08-2023" and "CAIQv4.0.2_STAR_Skykick 2023,v1.0". The risk treatment criteria are defined and risks are estimated based upon inherent risks and residual risks after treatment. The risk treatment is then quantitatively measured in CMMI levels so that the organisation can set KPI's to achieve in certain time periods. The risk treatment plans are being registered in the SharePoint/ Teams register with an owner and deadline. The DPO and SO together make sure the tasks are being closed on time.

Effectiveness of the processes to establish objectives, planning of actions and evaluation of progress and results	The process is considered to be effective and no nonconformities towards the requirements of the standard were identified. The conclusion is based on interviews with relevant managers and verification of the following records: The objectives have been defined and reviewed by the management review. Policy objectives are defined within SK-ISO27-02 Information Secuity Policy Integrated, chapter 5.1 and SK-InfoSec & Compliance Stakeholder Analysis.xlsx. Here is also KPi's mentioned for privacy and this is also being tracked through the management review and relevant dashboard.

Effectiveness of the management system to ensure the organization is capable to meet applicable legal and contractual requirements	The processes established to ensure fulfilment of requirements is considered effective and no nonconformities towards the requirements of the standard were identified. The conclusion is based on interviews with relevant personnel, and verification of the following activities and records: Legal & Terms folder and subfolder in the Sharepoint. Denton (law firm) 2023 support for the legal requirements. Applicable laws and regulations: Title, Territory, Law type (relevant for the context (privacy or commercial or privacy), Scope The organization has identified its legal position. Key relevant legislation are copyright law and GDPR. The organization has a legal firms supporting their compliance towards legal aspects and ensuring contracts are covering the required legal aspects.
Effective control of the use of certification marks and reference to certification	The use of certification marks and other references to the certification were assessed. There are certification marks in the signatures of emails and on the corporate website. Current use is in line with the given guideline.

Additional for multi-site certification based on a site sampling approach: Effectiveness of the central unit’s ability and authority to collect and analyse key data from all sites and to initiate change if required	The following key elements were assessed to conclude on the central unit's authority and ability to exercise effective control: Management system changes, management review, complaints, evaluation of corrective actions, internal audit planning and evaluation of the results, changes to risks/aspects and associated impacts for the management system (ISMS and PIMS) and different legal requirements. The Periodic Audit Plan has been updated including any changes to multi☐site sampling based on the above as well as relevant additional items identified in: IAF MD1:2018 6.1.2.4. The following records were reviewed: SK-CP-02.01 Global Employee Privacy Policy Rev 2.0 3/31//2023 Privacy Policy for employees BV and LLC Data protection officer email and other contacts; SK-CP-00.00 Corporate Policies and Procedures: Data protection officer responsibilities in 3.2.3; SK-ISO-27.01 Information Security &Privacy Management System Scope; 3.0 March 29, 2023 (annual review); SK-ISO-27.02 Information Security & Privacy Policy Integrated 3.0 March 29, 2023 (annual review); Data privacy process diagram rev. V4, June 2021; Vendor review process 4/24/2023 Business system criticality 3 tiers from 1 to 3. Satisfactory control was demonstrated and no nonconformities were identified.

Effectiveness of the process for information security risk assessment and risk treatment	The report from the risk assessment dated 21 august 2023 and the Statement of applicability version 5,0, 31 august 2023 were reviewed and demonstrated a process that comply s with requirements of the standard. The organization has defined certain Risk domains and calculated the inherent risks. The risk treatment criteria are defined and risks are estimated based upon inherent risks and residual risks after treatment. The risks are estimated on an inherent impact* inherent Likelihood. The risk appetite is defined within the tool. The Statement of Applicability (SOA) is available as documented information. The SOA has been updated including the reason for inclusion. All controls have been found applicable, which is fitting to the organizational activities. Within the document there is an explicit link towards the requirements of the ISO 27001 and ISO 27701 standard. The organization has adopted a risk based approach. CMMI levels have been identified to indicate the implementation status.

Annex B - Handling of findings

Definition of findings

Major nonconformity (Category 1)
A nonconformity that affects the capability of the management system to achieve the intended results.

Nonconformities could be classified as major in the following circumstances:

- if there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements
- a number of minor nonconformities associated with the same requirement or issue that demonstrates a systemic failure and thus constitute a major nonconformity

Minor nonconformity (Category 2)
A nonconformity that does not affect the capability of the management system to achieve the intended results

Observation
An observation is not a non-conformance, but something that could lead to a non-conformance, if allowed to continue uncorrected; or an existing condition without adequate supporting evidence to verify that it constitutes a non-conformance.

Opportunity for improvement
Opportunities for improvement relates to areas and/or processes of the organization which may meet the minimum requirement of the standard, but which could be improved.

Conditions for handling of nonconformities

The standard deadline to respond to nonconformities is maximum 90 days. Within this timeframe the following is expected to be performed by the organization:

- Immediate action(s) to eliminate the non-conforming situation (if relevant for the nonconformity).
- Root cause analysis to identify corrective actions to prevent recurrence of the nonconformity.
- Implement corrective actions and verify the effectiveness of action(s).

- Fill in the pertinent part of the “List of Findings” and submit to DNV’s team leader with relevant supporting documentation as evidence (when applicable).

Within the maximum timeframe and as a prerequisite before a certificate can be issued the following conditions apply:

- Major nonconformities: Evidence of root cause analysis and effectively implemented corrections and corrective actions shall be provided.
- Minor nonconformities: Preferred and normal status is the same as for major nonconformities. However, DNV's team leader may also accept a plan for implementing identified corrective actions. The implementation of planned actions will at latest be verified during next audit.

There is no obligation to investigate or respond formally to an observations or opportunity for improvement. However, to support an effective certification process DNV recommends that observations are also considered and responded to by the organization.

DNV will normally perform an on-site follow-up when major nonconformities are issued. For minor nonconformities follow-up is normally performed as a desk review based on received documentation.

Insufficient response to nonconformities or lack of corrective actions may result in suspension or withdrawal of a certificate.

Response deadline for re-certification

Where the certificate expires within the 90 day period a shorter deadline will be set to ensure proper follow-up and renewal of the certificate within the expiry date. This is to provide for the continual validity of certification. If the expiry date is exceeded without the process being finalised, the current certificate is not allowed to be extended and will in effect be suspended until renewal of the certificate.

ViewPoint

ViewPoint is our customer community comprised of more than 10,000 customers from around the world. They voluntarily express their opinions and share insight on topical subjects related to certification and sustainable business performance in their industry.

Participation is free and all ViewPoint members have full access to the data and full reports from every survey. They also benefit from networking opportunities, access to eLearning modules, and invitations to webinars, online forums and much more.

Would you like to become a member?
Join us here: https://www.dnv.com/assurance/viewpoint/viewpoint-application.html

Did you know?

Looking for news and developments in the certification and assurance market? You can find more on our website and learn about the initiatives and services exclusively available to you as a DNV customer.

Download A broader view from: https://www.dnv.com/broaderview

DNV

ABOUT DNV

We are the independent expert in risk management and assurance. Driven by our purpose, to safeguard life, property and the environment, we empower our customers and their stakeholders with facts and reliable insights so that critical decisions can be made with confidence. As a trusted voice for many of the world's most successful organizations, we use our knowledge to advance safety and performance, set industry benchmarks, and inspire and invent solutions to tackle global transformations.

DNV is one of the world's leading certification, assurance and risk management providers. Whether certifying a company's management system or products, providing training, or assessing supply chains, and digital assets, we enable customers and stakeholders to make critical decisions with confidence. We are committed to support our customers to transition and realize their long-term strategic goals sustainably, collectively contributing to the UN Sustainable Development Goals.

www.dnv.com

WHEN TRUST MATTERS