AUDIT REPORT

Project number: HU20271/22

Client name:	ConfigCat Kft.
Client address:	1136 Budapest, Tátra u. 5/A
Client's management representative:	Zoltán Dávid
Examined site(s) during the audit:	1136 Budapest, Tátra u. 5/A
Examined temporary locations during the audit[1]:	-
Audit date:	16 05 2024 - 17 05 2024
Lead auditor:	László Németh
Co-auditor(s):	-
Expert(s):	-
Other accompanying persons (eg.: observers, interpreters):	-
Audit type:	Certification audit
Audit method:	on site audit / [✓ remote audit] / blended audit
Standard(s):	**ISO/IEC 27001:2013 (MSZ ISO/IEC 27001:2014)** Information Security Management System

1 The objective of the audit is:

- to define if Client's management system complies with audit criteria
- to evaluate if client is able to ensure compliance with applicable statutory, regulatory and contractual requirements
- to evaluate management system's effectiveness
- to define any area for potential improvement (if applicable)

2 Client scope

Scope of certification:	design, production, deployment and provision of the ConfigCat feature management system
Changes in the scope of certification:	There was no change in the scope of certification. The Statement of Applicability has changed (08 05 2023)

[1] A temporary site is established by the organization to perform a specific work or provide a service for a limited period of time and not intended to function as a permanent site (eg construction site, service site).

Project number: HU20271/22

3 Result of the audit

	Yes	Partly	No
The organization has properly adopted and operated its management system in accordance with standard requirements.	☑	□	□
The organization presented its ability to provide compliance of a product/service with agreed requirements in accordance with the organisation’s policy and objectives.	☑	□	□
Scope of the management system is properly determined.	☑	□	□
Objective of the audit was achieved during the organization's management system's revision.	☑	□	□

4 Summary of the audit

Introduction of the organization / Changes in certified scope (audit criteria, headcount, activity, personal changes):	Scope: design, production, deployment and provision of the ConfigCat feature management system The company has been operating for 6 years, providing service is in SaaS form. Significant growth, business expansion 3x (also in the number of customers). 350 clients, companies and government entities, mainly foreigners. The 6 founding members are still owners today, the number of the staff has increased to a total of 11 people. All employees continue to work from home. They only use cloud-based technology, but they also use their own devices, this was taken into account when changing the Applicability Statement. Headquarters: 1136 Budapest Tátra utca 5/A – provides only headquarters service.
Evaluation of corrective actions for previous year's nonconformities:	-
Unexamined activities and standard requirements during this audit:	Controls of the ISO/IEC 27001:2013 standard chapters 4.2, 5.1, 5.3, 7.2, 7.5 and Annex A A5, A6, A7, A8, A9, A10, A11 of
Use of CERTOP certification logo:	The Certificate can be downloaded from the homepage: https://configcat.com/iso/
Strengths of the system:	Strategic thinking, SWOT, management commitment Management of documented information (GITHUB/WIKI, issue tracking) They plan to include a fourth level (stage), the environment (is very similar to the live one). This can also be used for penetration test. Annual security training, awareness Internal communication, SLACK, trello Management of internal audits and non-conformities Monitoring – public feedback to customers Vulnerability testing
Possibilities for development:	It is recommended to include Climate Change in the evaluation of the organization's environment – in line with the addition to ISO standards (February 2024). It is recommended to clarify the expectations related to climate change among the requirements of the interested parties - – in line with the addition to ISO standards (February 2024). Make the Policy Statement available to interested parties via the website

	or upon request - similarly to an audit report Definition of sub-goals for the information security goals based on the Policy Statement, regarding of the actual period and circumstances (e.g. risks, development recommendations, external effects revealed in SWOT, etc.). Updating the data processor & supplier list with service providers managing the organization's own information. In the legal environment, the IS relevant EU directives (AI, NIS2) must be taken into account.

5 Recorded Nonconformities[2]

Number	Description of nonconformities	Standard requirement	Category[3]
-	-	-	-

6 Operation of the system/Findings of the audit[4]

Understanding the organization and its context	Yes	Partly	No
Corresponds to the requirements of the standard.	☑	□	□
Comments to the standard requirement: based on he SWOT analysis			

Understanding the needs and expectations of interested parties	Yes	Partly	No
Corresponds to the requirements of the standard.	□	□	□
Comments to the standard requirement:			

Determining the scope of the information security management system	Yes	Partly	No
Corresponds to the requirements of the standard.	☑	□	□
Comments to the standard requirement: The Statement of Applicability has changed 08 05 2023			

Information security management system	Yes	Partly	No
Corresponds to the requirements of the standard.	☑	□	□
Comments to the standard requirement:			

Leadership and commitment	Yes	Partly	No
Corresponds to the requirements of the standard.	□	□	□
Comments to the standard requirement: Deployed, documented, operational and			

[2] Each nonconformities have to be recorded in a new row.
[3] Major nonconformity – submission of proving documents of the introduced corrective action is mandatory
Minor nonconformities – the supporting documents for the corrective action must be presented at the next audit.

[4] The objective evidences reviewed at the audit to support compliance or non-compliance ares detailed in the Audit Note.

continuously improved. Regulations in GitHub/WIKI, ISPs and policies

Policy	Yes	Partly	No
Corresponds to the requirements of the standard.	☑	□	□

Comments to the standard requirement: Policy Statement - unchanged, part of the Information Security Policy. Possibility for improvement: make the Policy Statement available to stakeholders via the website, even on request - similar to an audit report

Organizational roles, responsibilities and authorities	Yes	Partly	No
Corresponds to the requirements of the standard.	□	□	□

Comments to the standard requirement:

Actions to address risks and opportunities	Yes	Partly	No
Corresponds to the requirements of the standard.	☑	□	□

Comments to the standard requirement: Regulated by Risk Management Plan

Information security risk assessment	Yes	Partly	No
Corresponds to the requirements of the standard.	☑	□	□

Comments to the standard requirement: Documented in Risk management.xlsx, evaluation: Likelihood*Impact=Risk weight. below 6 low, 7-11 medium, above 11 high.

Information security risk treatment	Yes	Partly	No
Corresponds to the requirements of the standard.	☑	□	□

Comments to the standard requirement: The Risk treatment plan is a part of the Risk management.xlsx.

Information security objectives and planning to achieve them	Yes	Partly	No
Corresponds to the requirements of the standard.	☑	□	□

Comments to the standard requirement: 3 goals defined on the basis of the Ploicy Statement. Evaluated at the Management Review (29.03.2023).

Possibility for improvement: sub-objectives defined for information security objectives based on Policy Statement, based on the period and circumstances (e.g. risks, development proposals, externalities identified in SWOT, etc.).

Resources / Competence / Awareness / Communication	Yes	Partly	No
Corresponds to the requirements of the standard.	☑	□	□

Comments to the standard requirement: Annual awareness training and log of participation. Exam (acceptable in case of 100%), Communication: Slack channels, every two month Security Week.

Documented information	Yes	Partly	No
Corresponds to the requirements of the standard.	□	□	□

Comments to the standard requirement:

Operational planning and control	Yes	Partly	No
Corresponds to the requirements of the standard.	☑	□	□

Comments to the standard requirement: Regulations in GITHUB/WIKI. Information security policy 2023.09.14. + Policies. Change management by the Change Management (2023.10.04.) regulation.

Information security risk assessment and treatment	Yes	Partly	No
Corresponds to the requirements of the standard.	☑	□	□

Comments to the standard requirement: Documented in the Risk management.xlsx. 45 risks, 3 medium level risks. Risk treatment plan is a part of the Risk management.xlsx – action documented in Trello tickets.

Monitoring, measurement, analysis and evaluation	Yes	Partly	No
Corresponds to the requirements of the standard.	☑	□	□

Comments to the standard requirement: Regulated by the Logging and monitoring policy. for example. site24 monitor. Data about the Availabity are public: status.configcat.com

Internal audit	Yes	Partly	No
Corresponds to the requirements of the standard.	☑	□	□

Comments to the standard requirement: Internal audit master plan: the audits planned to 2024 are in progress. Audit done: for A.14.2 control at 2024.05.06. 4 nonconformities, actions in progress.

Management review	Yes	Partly	No
Corresponds to the requirements of the standard.	☑	□	□

Comments to the standard requirement: Last one was at 2023.03.29. Scheduled for this year at 2024.08.09. Minute according to the Agenda.

Nonconformities and corrective actions	Yes	Partly	No
Corresponds to the requirements of the standard.	☑	□	□

Comments to the standard requirement: Nonconformity management.xlsx - 4 nonconformities based on internal audit. Last year's internal audit nonconformity: the Follow-up handled and traced by Trello.

Continuous improvement	Yes	Partly	No
Corresponds to the requirements of the standard.	☑	□	□

Comments to the standard requirement: Strategic planning and SWOT + Management review. Development focuses are determined (for example. Allocating financials for the use of AI.)

Annex „A" – Control objectives and controls	Observed?	Appropriate?		
A5 Information security policies	□ Yes	Yes	Partly	No
A5.1 Management direction for information security.	□	□	□	□

Comments to the standard requirement:

A6 Organization of information security	□ Yes	Yes	Partly	No
A6.1 Internal organization.	□	□	□	□
A6.2 Mobile devices and teleworking.	□	□	□	□

Comments to the standard requirement:

A7 Human resource security	□ Yes	Yes	Partly	No
A7.1 Prior to employment.	□	□	□	□
A7.2 During employment.	□	□	□	□
A7.3 Termination and change of employment.	□	□	□	□

Comments to the standard requirement:

A8 Asset management	□ Yes	Yes	Partly	No
A8.1 Responsibility for assets.	□	□	□	□
A8.2 Information classification.	□	□	□	□
A8.3 Media handling.	□	□	□	□

Comments to the standard requirement:

A9 Access control	□ Yes	Yes	Partly	No
A9.1 Business requirements of access control.	□	□	□	□
A9.2 User access management.	□	□	□	□
A9.3 User responsibilities.	□	□	□	□
A9.4 System and application access control.	□	□	□	□

Comments to the standard requirement:

A10 Cryptography	□ Yes	Yes	Partly	No
A10.1 Cryptographic controls.	□	□	□	□

Comments to the standard requirement:

A11 Physical and environmental security	□ Yes	Yes	Partly	No
A11.1 Secure areas.	□	□	□	□
A11.2 Equipment.	□	□	□	□

Comments to the standard requirement:

A12 Operations security	☑ Yes	Yes	Partly	No

A12.1 Operational procedures and responsibilities.	☑	☑	□	□
A12.2 Protection from malware.	☑	☑	□	□
A12.3 Backup.	☑	☑	□	□
A12.4 Logging and monitoring.	☑	☑	□	□
A12.5 Control of operational software.	☑	☑	□	□
A12.6 Technical vulnerability management.	☑	☑	□	□
A12.7 Information systems audit considerations.	☑	☑	□	□

Comments to the standard requirement: Operation regulated by for example the Change management, Virtual Private Servers, Backup Plan, Logging and Monitoring Policy és done, for example Sentry.io, Intruder.io – monthly checks.

A13 Communications security	☑ Yes	Yes	Partly	No
A13.1 Network security management.	☑	☑	□	□
A13.2 Information transfer.	☑	☑	□	□

Comments to the standard requirement: They have no networks, so there is no separation (13.1.3. not applicable requirement). The security of network services is taking the security of service providers into account when choosing, for example own services via HTTPS and a SSH. Non disclosure agreements.

A14 System acquisition, development and maintenance	☑ Yes	Yes	Partly	No
A14.1 Security requirements of information systems.	☑	☑	□	□
A14.2 Security in development and support processes.	☑	☑	□	□
A14.3 Test data.	☑	☑	□	□

Comments to the standard requirement: Change management policy, Sonarcloud testing, code review (with Pull request), source code in GitHub, testing: automatic and manual (QA) tests, smoke test when going operational. There is no outsourced development now.

A15 Supplier relationships	☑ Yes	Yes	Partly	No
A15.1 Information security in supplier relationships.	☑	☑	□	□
A15.2 Supplier service delivery management.	☑	☑	□	□

Comments to the standard requirement: Supplier/Data Processor Policy, Data processor&suppliers list.xlsx. Possibility for improvement: update it with the service providers handling the own company’s information.

A16 Information security incident management	☑ Yes	Yes	Partly	No
A16.1 Management of information security incidents and improvements.	☑	☑	□	□

Comments to the standard requirement: Incident Communication Plan. Bug Bounty Hunter program, Trello ticket abuot the valid problems. only few real weaknesses

A17 Information security aspects of business continuity management	☑ Yes	Yes	Partly	No
A17.1 Information security continuity.	☑	☑	□	□
A17.2 Redundancies.	☑	☑	□	□

Comments to the standard requirement: BCP - Business Continuity Plan, DRP - Disaster Recovery Plan: It covers the goals and actions. Tested on 2024.05.02.

A18 Compliance	☑ Yes	Yes	Partly	No
A18.1 Compliance with legal and contractual requirements.	☑	☑	□	□
A18.2 Information security reviews.	☑	☑	□	□

Comments to the standard requirement: Compliance regulation. Possibility for improvement: Taking into account the information security relevant EU directives (AI, NIS2) too.

7 Comments

Identified, unresolved issues during the audit (if applicable):	-
Deviation from the audit plan and its reasons (if applicable):	-

Assessment of remote audit (if applicable)

	Yes	Partly	No
Remote audit method was appropriate.	☑	□	□
Confidentiality, information security and data protection were ensured during the audit.	☑	□	□
Reviewing of the planned processes, activities, sites, and the availability of the planned employees were ensured. The remote assessment did not affect the effectiveness of the audit.	☑	□	□
Required audit time was fulfilled.	☑	□	□
In case of remote audit agreed Information and Communication Technology: (ICT): Google meet			

Any identified risks, other comments regarding the nature of the remote audit: -

The suggestion of the audit team concerning the issue / maintenance of the Certificate is included in the Certificate of perrformance that was filled out during the closing meeting of the audit.

We kindly ask to **report any changes concerning the certified management system**, in accordance with the General Terms and Conditions at our website (https://hu.certop.com).

The audit was based on a sampling procedure.

The Audit report contains confidential information.

8 Planned date of the following year's audit

Execution of the annual surveillance procedures in time is the condition of the certificate to stay in force.

Due surveillance audits have to be implemented within 12 to 24 months after the recertification audit's/initial audit's certification decision, recertification audit and the related certification decision has to be conducted before the expiry of a validity date!

Project number: HU20271/22

The following audit’s planned date: 30 05 2025

Date: 17 05 2024

László Németh
Lead auditor