AUDIT REPORT

Project number: HU21841/25

Client name:	ConfigCat Kft.
Client address:	1136 Budapest, Tátra u. 5/A
Client's management representative:	Dávid Zoltán
Examined site(s) during the audit:	
1136 Budapest, Tátra u. 5/A	
Examined temporary locations during the audit[1]:	
Audit date:	2025. 05. 26.; 2025. 05. 27.
Lead auditor:	Németh László
Co-auditor(s):	-
Expert(s):	-
Other accompanying persons (eg.: observers, interpreters):	
Audit type:	recertification audit
Audit method:	on site audit / remote audit / blended audit
Standard(s):	**ISO/IEC 27001:2022 (MSZ ISO/IEC 27001:2023)** 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:	no changes
Statement of Applicability (date, version):	SoA 2025.05.23.

[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).

Not applicable controls and their justification:	A7.1 Physical security perimeter - Company does not have a physical office. Server hosting providers compliant with requirement. A7.2 Physical entry controls - Company does not have a physical office. Server hosting providers compliant with requirement. A7.3 Securing offices, rooms, and facilities - Company does not have a physical office. Server hosting providers compliant with requirement. A7.4 Physical security monitoring - Company does not have a physical office. Server hosting providers compliant with requirement. A7.5 Protecting against physical and environmental threats - Company does not have a physical office. Server hosting providers compliant with requirement. A7.6 Working in secure areas - Company does not have a physical office. Server hosting providers compliant with requirement. A7.11 Supporting utilities - Company does not have a physical office. Server hosting providers compliant with requirement. A7.12 Cabling security - Company does not have a physical office. Server hosting providers compliant with requirement. A7.13 Equipment maintenance - Company does not manage physical assets. Server hosting providers compliant with requirement. A8.20 Network controls - Company does not have any networks it manages. Datacenters are certified to meet these requirements. A8.21 Security of network services - Company does not have a physical office and server hosting is done by certified datacenter that meets these requirements according to contractual agreement. Requirements on networks are included in business continuity plan. A8.22 Segregation in networks - Company does not have any networks it manages. Datacenters are certified to meet these requirements. The justifications are acceptable.

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.	☑	☐	☐

Project number: HU21841/25

4 Summary of the audit

Introduction of the organization / Changes in certified scope (audit criteria, headcount, activity, personal changes):	The company has been operating for 7 years, providing service is in SaaS form. The staff is 11 people. All employees continue to work from home. They only use cloud-based technology, but they also use their own devices. They started forming teams (i.e.: DevOps, Marketing). Dániel Toth became the new ISMS Officer. Headquarters: 1136 Budapest Tátra utca 5/A – provides only headquarters service.
Evaluation of corrective actions for previous year's nonconformities:	There were no nonconformity.
Unexamined activities and standard requirements during this audit:	Renewal audit, all requirements were audited.
Use of CERTOP certification logo:	The organization did not use the Certop logo. The Certificate can be downloaded from the homepage: https://configcat.com/iso/
Strengths of the system:	Strategic thinking, SWOT, management commitment Cloud based information management system (GDrive GITHUB, Trello) Security week in every two month. Monitoring – public feedback to customers. Environmental aspects, responsibility, plant a tree program (3000 tree), ESG evaluation. Documentation system (short policies but a lot of them).
Possibilities for development:	It is recommended to change on the homepage the generally used ISO 27001 logo to the Certop Certification logo. The SWOT analysis is a separate document but it is included (inserted, not linked) in the Misson. It is recommended not to hold the SWOT twice. It is recommended to check that all employees have their certificates stored. It is recommended to update the Compliance logs and standards with the law regulation regarding internation clients and financial clients (e.g. DORA). It is recommended to expand the scope of KPIs to include the number of modifications made based on access reviews.

5 Recorded Nonconformities[2]

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

[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.

Project number: HU21841/25

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

Evaluation of compliance:	Yes	Partly	No
Context of the organization The organization has determined and monitored external and internal issues that are relevant to its purpose and strategic direction, the requirement of interested parties that are relevant to the quality management system, the boundaries and applicability of MS, documented its processes and made it available for the interested parties.	☑	☐	☐

Comment on the standard requirement:

Evaluation based on SWOT analysis. The SWOT analysis is a separate document but it is included (inserted, not linked) in the Misson. It is recommended not to hold the SWOT twice. The Statement of Applicability has changed 25 05 2025. Lot's of policies define the ISM processes, the ISMS Process flow covers them.

	Yes	Partly	No
Leadership Leadership and commitment are ensured regarding the operation and development of quality management system. The quality policy complies with the strategic direction, the appropriate organizational roles, responsibilities and authorities are determined.	☑	☐	☐

Comment on the standard requirement:

The management commitment proven to the operation and improvement of the ISMS. Dániel Tóth appointed as new ISMS officer.

	Yes	Partly	No
Planning The management system is planned, the risks and opportunities related to the business activities are defined and evaluated, the information security risk assessment process is applied and documented, its goals are defined and the changes are managed in a planned manner.	☑	☐	☐

Comment on the standard requirement:

Risk assessment and treatment is Regulated by Risk Management Plan, Documented in Risk management.xlsx, evaluation: Likelihood*Impact=Risk weight. below 6 low, 7-11 medium, above 11 high. The Risk treatment plan is a part of the Risk management.xlsx and Trello tickets for the actions. Security goals defined on the basis of the Policy Statement. Evaluated at the Management Review (08.04.2025).

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

Project number: HU21841/25

	Yes	Partly	No
Support The necessary resources needed for the establishment, implementation, maintenance and improvement of the managemnent system are available. The competence and awareness of the staff is proven. The organization has determined the need for internal and external communication relevant to the information security management system. Documented information required by the management system and the organization is available.	☑	☐	☐

Comment on the standard requirement:

It is recommended to check that all employees have their certificates stored. Annual awareness training (acceptable in case of 100%), Communication: Slack channels, every two month Security Week. It is recommended to update the Compliance logs and standards with the law regulation regarding internation clients and financial clients (e.g. DORA)

	Yes	Partly	No
Operation The organization has planned, implemented and controlled the processes needed to meet the requirements and achieve the goals of the management system. Documented information is available. Control of externally provided processes, pruducts and services is appropriate and well documented. (if applicable) Control of nonconforming outputs is documented and appropriate.	☑	☐	☐
The information security risk assessment has been performed and the organization has implemented the information security risk treatment plan. Documented information is available.	☑	☐	☐

Comment on the standard requirement:

ISMS processes are regulated in Policies (lot's of them applied), the ISMS Process flow covers them. Risk assessment documented in the Risk management.xlsx. Risk treatment plan is a part of the Risk management.xlsx – action documented in Trello tickets.

	Yes	Partly	No
Performance evaluation The organization regularly evaluate the effectiveness and performance of the management system. Monitoring, measurment and analyzing methods are determined; planning and implementing of internal audits and management review are effective, verified and documented.	☑	☐	☐

Comment on the standard requirement:

Regulated by the Logging and monitoring policy, for example. site24 monitor. Data about availability are public: status.configcat.com. It is recommended to expand the scope of KPIs to include the number of modifications made based on access reviews. Internal audits were conducted in May 2025, as a part of the upgrading to the ISO/IEC 27001:2022. Management review was performed in 08.04.2025, the evaluate the effectiveness of the ISMS.

	Yes	Partly	No
Improvement Improvement of the management system is verified, the organization determines and implements the selected opportunities for improvement, handling of nonconformities and corrective actions are efficent and properly documented.	☑	☐	☐

Comment on the standard requirement:

The base of the improvement are the Strategic planning and SWOT + Management review. The nonconformities found on internal audits were handled well.

Annex A – Information security controls

	Examined during current audit	Conformity assessment	
		Yes	No
A5.1-5.8 ISMS roles/responsibilities	☑	☐	☐

Comments on the controls:

Glossary, core team responsibilities, ISMS officer 's responsibilities. Threat intelligence: NKI and Cloudflare.

	Examined during current audit	Conformity assessment	
		Yes	No
A5.9-5.14 Assets	☑	☐	☐

Comments on the controls:

Inventory of assets policy, Access control policy controls.

	Examined during current audit	Conformity assessment	
		Yes	No
A5.15-5.18 Access control	☑	☐	☐

Comments on the controls:

Regulated by the Access Control Policy. Password rules in Cyber Hygiene policy. It is recommended to expand the scope of KPIs to include the number of modifications made based on access reviews.

	Examined during current audit	Conformity assessment	
		Yes	No
A5.19-5.23 Supplier relationships	☑	☐	☐

Comments on the controls:

Supplier/Data Processor Policy. Data processor&suppliers list.xlsx – the list contains service providers handling the own company's information. Rules for cloud services included in supplier policy.

Project number: HU21841/25

	Examined during current audit	Conformity assessment	
		Yes	No
A5.24-5.30 Incident management	☑	☐	☐

Comments on the controls:

Incident Communication Plan. There were no security incidents. Bug Bounty Hunter program, Trello ticket about the valid problems. only few real weaknesses. BCP - Business Continuity Plan, DRP - Disaster Recovery Plan: It covers the goals and actions. Annually tested.

	Examined during current audit	Conformity assessment	
		Yes	No
A5.31-5.37 Legal requirements, documentation	☑	☐	☐

Comments on the controls:

Compliance regulation. Possibility for improvement: Taking into account the information security relevant law regulation regarding internation clients and financial clients (e.g. DORA).

	Examined during current audit	Conformity assessment	
		Yes	No
A6.1-6.8 HR processes	☑	☐	☐

Comments on the controls:

Employee onboarding and offboarding procedure. The NDA is included in the employment contract. Remote working is common.

	Examined during current audit	Conformity assessment	
		Yes	No
A7.1-7.14 Phisical security, controls	☑	☐	☐

Comments on the controls:

A7.1 , A7.2, A7.3, A7.4, A7.5, A7.6, A7.11, A7.12, A7.13 controls aren't applicable, because the company does not manage physical assets. Server hosting providers compliant with requirement. Remote working is common.

	Examined during current audit	Conformity assessment	
		Yes	No
A8.1-8.19 IT	☑	☐	☐

Comments on the controls:

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. GitHub, 2 factor authentication. Monitoring: Grafana.

Project number: HU21841/25

	Examined during current audit	Conformity assessment	
		Yes	No
A8.20-8.24 Network security	☑	☐	☐

Comments on the controls:

A8.20, A8.2, A8.22 controls aren't applicable, because the company does not have any networks it manages. Datacenters are certified to meet these requirements.

	Examined during current audit	Conformity assessment	
		Yes	No
A8.25-8.34 Development	☑	☐	☐

Comments on the controls:

Change management policy, Sonarqube 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.

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.	☐	☐	☐
Information and communication technology (ICT) used during remote audit:			

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.

Project number: HU21841/25

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 deed!

The following audit's planned date: 2027. 05. 27.

Date: 2025. 05. 27.

Németh László sk.
Lead auditor