CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	ConfigCat has a comprehensive set of information security policies based on industry standards and best practices. ConfigCat has mapped its policies and standards to ISO27001 controls.		A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	Audit and Assurance Policy and Procedures	Audit & Assurance
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Yes	CSP-owned	The policies and standards are reviewed by relevant stakeholders and approved by the management at least annually.					
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes	CSP-owned	ConfigCat leverages an independent third-party auditor to conduct a ISO 27001 annual audit. This includes the testing of the effectiveness of ConfigCat's security policies and controls.		A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Independent Assessments	
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes	CSP-owned	ConfigCat's internal independent audit and assurance program uses a Risk Management Plan to conduct assessments at least annually.		A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	Risk Based Planning Assessment	
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Yes	CSP-owned	ConfigCat's information Security Policies and Procedures are in adherence with ISO27001 standards.		A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	Requirements Compliance	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence?	Yes	CSP-owned	Internal audits are planned and performed according to the documented audit management process to review ConfigCat's performance against standards-based criteria and to identify general improvement opportunities.		A&A-05	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	Audit Management Process	
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	ConfigCat's Risk Assessment Plan is based on ISO 27001 best practices and offers a repeatable process that includes all assets that contain, process, or impact customer data.		A&A-06	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.	Remediation	
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	Yes	CSP-owned	During management reviews, audit findings are reported to relevant stakeholders.					
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities?	Yes	CSP-owned	ConfigCat has a comprehensive set of information security policies based on industry standards and best practices. ConfigCat has mapped its policies and standards to ISO27001. From development point of view, ConfigCat follows the SDL security		AIS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually.	Application and Interface Security Policy and	

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	ConfigCat maintains and periodically updates when there is a significant change to systems or environment, or at the least annually.		AIS-01		Security Policy and Procedures	Application & Interface Security
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes	CSP-owned	ConfigCat follows ISO 27001 framework and adheres to the industry standards in defining the baseline requirements to secure all its applications. All our standards and policies are reviewed by top management annually.		AIS-02	Establish, document and maintain baseline requirements for securing different applications.	Application Security Baseline Requirements	
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes	CSP-owned	Technical metrics and operational metrics are defined and implemented as per the our business objectives, security requirements and compliance obligations.		AIS-03	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	Application Security Metrics	
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes	CSP-owned	ConfigCat's Software Development Lifcycle (SDLC) mandates adherence to secure coding guidelines, and screening of code changes for potential security issues with our code analyzer tools, vulnerability scanners,		AIS-04	Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	Secure Application Design and Development	
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Yes	CSP-owned	A formal Change Management Policy has been defined in order to ensure that all application changes have been authorized prior to implementation into the production environments. ConfigCat follows the git-flow development lifecycle in which developers create Pull Request with		AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.	Automated Application	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
AIS-05.2	Is testing automated when applicable and possible?	Yes	CSP-owned	Automated secure code analysis is performed using SonarQube as a static analysis scanning tool. Also, ConfigCat has a bug bounty program (https://configcat.com/bounty/) in which independent developers and security researchers discover and		AIS-05		Security Testing	
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes	CSP-owned	All code is reviewed as part of the organizational SDLC processes in order to identify possible security vulnerabilities. In general, development follows security best-practices, features are considered with security in		AIS-06	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Automated Secure Application Deployment	
AIS-06.2	Is the deployment and integration of application code automated where possible?	Yes	CSP-owned	ConfigCat utilizes automated code deployment and integration method where feasible.					
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes	Shared CSP and 3rd-party	ConfigCat uses Snyk.io for automatic vulnerability reports. ConfigCat has a Third Party Dependecies Management in place		AIS-07	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.	Application Vulnerability Remediation	
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	Yes	CSP-owned	In case of Pull requests, there is a SonarCloud check in place. See AIS-07.1 for further reference.					
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	ConfigCat has a well-established Business Continuity Plan in place. The business continuity plan is a comprehensive runbook that walks all ConfigCat Team-members through exactly what their individual responsibilities are, in the event of a disruption to ConfigCat operations		BCR-01	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually.	Business Continuity Management Policy and	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	ConfigCat's Business Continuity Plan is reviewed at least annually or upon significant organizational changes.		BCR-01		Management Policy and Procedures	
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes	CSP-owned	ConfigCat's Business Continuity Plan provides guidance on how to plan and execute operations to address potential business interruptions caused by emergency events.		BCR-02	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.	Risk Assessment and Impact Analysis	
BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	Yes	CSP-owned	ConfigCat's Business Continuity Plan includes strategies to reduce the impact of and recover from business disruptions.		BCR-03	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.	Business Continuity Strategy	
BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	Yes	CSP-owned	ConfigCat continually assesses ways to improve the recovery capabilities across the full platform to ensure that should a disaster arise, normal operation can be restored as quickly, and with as little disruption, as possible.		BCR-04	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.	Business Continuity Planning	
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	Yes	CSP-owned	ConfigCat has a well-established Business Continuity Plan, Backup Plan and Disaster Recovery Plan in place.			Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review periodically.		

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes	CSP-owned	The Business Continuity Plan is shared and available to all ConfigCat employees.		BCR-05		Documentation	Business Continuity Management and Operational Resilience
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Yes	CSP-owned	ConfigCat's Business Continuity Plan is reviewed at least annually or upon significant organizational changes.					
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	Yes	CSP-owned	Verification of ConfigCat's Disaster Recovery Plan is conducted at least annually, database restore test is completed at least annually.		BCR-06	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	Business Continuity Exercises	
BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	Yes	CSP-owned			BCR-07	Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.	Communication	
BCR-08.1	Is cloud data periodically backed up?	Yes	CSP-owned	ConfigCat's Backup Plan defines the retention and protection requirements of backups created of specified ConfigCat assets.			Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.		

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	Yes	CSP-owned	ConfigCat's backup data is protected with similar controls as production data, and is encrypted.		BCR-08		Backup	
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	CSP-owned						
BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	Yes	CSP-owned	ConfigCat's Business Continuity and Disaster Recovery procedures provide guidance on how to plan and execute operations to address potential business interruptions caused by emergency events.		BCR-09	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.	Disaster Response Plan	
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes	CSP-owned	ConfigCat's Disaster Recovery Plan is reviewed at least annually or upon significant organizational changes.					
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes	CSP-owned	Verification of ConfigCat's Disaster Recovery Plan is conducted at least annually, database restore test is completed at least annually.		BCR-10	Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities.	Response Plan Exercise	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	No	CSP-owned	Local emergency authorities are not included in ConfigCat's BCP/DR exercises.		BCR-10		Response Plan Exercise	
BCR-11.1	Is business-critical equipment supplemented with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards?	NA	3rd-party outsourced	ConfigCat services reside within Linode, DigitalOcean and Microsoft Azure hence ConfigCat does not own or maintain any physical infrastructure that would be considered business-critical equipement.		BCR-11	Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.	Equipment Redundancy	
CCC-01.1	Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)?	Yes	CSP-owned	ConfigCat maintains a Risk Management Policy that outlines the scope and goals of our Risk Management Plan. The risk assessment must be executed annually or in case of any significant event or change that causes the Core Team to decide that the process needs to be repeated.		CCC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.	Change Management Policy and Procedures	
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed and approved at least annually.					

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Yes	CSP-owned	ConfigCat has a formal Change Management Process in place that collects procedures of all changes made to the ConfigCat services or infrastructure elements. The scope of the Change Management		CCC-02	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.	Quality Testing	Change Control and Configuration Management
CCC-03.1	Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?	Yes	CSP-owned	Risks associated with new or modified assets are reviewed by relevant engineering, operations and security teams according to compliance standards.		CCC-03	Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced).	Change Management Technology	
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes	CSP-owned	Any changes to ConfigCat's systems, applications, etc. must be approved by the owner of the given systems, applications, etc. Unauthorized changes are prohibited.		CCC-04	Restrict the unauthorized addition, removal, update, and management of organization assets.	Unauthorized Change Protection	
CCC-05.1	Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs?	NA	CSP-owned	ConfigCat is a SaaS provider, customers do not own any of our environments.		CCC-05	Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.	Change Agreements	
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes	CSP-owned	ConfigCat has a formal Change Management Process in place that collects procedures of all changes made to the ConfigCat services or infrastructure elements. The scope of the change management		CCC-06	Establish change management baselines for all relevant authorized changes on organization assets.	Change Management Baseline	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Yes	CSP-owned	Multiple monitoring tools are in place to proactively detect baseline deviations.		CCC-07	Implement detection measures with proactive notification in case of changes deviating from the established baseline.	Detection of Baseline Deviation	
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes	CSP-owned	Every time a new entity is added to ConfigCat that is not covered by Change Management Process, its change management procedures must be discussed with the Core Team and added to the process.		CCC-08	'Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.'	Exception Management	
CCC-08.2	'Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?'	Yes	CSP-owned						
CCC-09.1	Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?	Yes	CSP-owned	Roll back plans are included as part of the Change Management Process.		CCC-09	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.	Change Restoration	
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	We have cryptography, encryption, and key management policies in place. Plus we have ConfigCat's Secret Management Policy that describes the requirements for handling existing and new secrets. All employees are		CEK-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually.	Encryption and Key Management Policy and Procedures	
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	ConfigCat's cryptography, encryption, and key management policies and Secret Management Policy is reviewed on annually.					

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes	CSP-owned	Yes, we have a dedicated team who is responsible for cryptography, encryption, and key management.		CEK-02	Define and implement cryptographic, encryption and key management roles and responsibilities.	CEK Roles and Responsibilities	
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	NA	CSP-owned	For data transit and replication between nodes using TLS 1.2/1.3 and data at-rest using standard AES (CBC) algorithm with built-in MySQL plugin.		CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.	Data Encryption	
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Yes	CSP-owned	ConfigCat uses various strong encryption mechanisms across our environments and product.		CEK-04	Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.	Encryption Algorithm	
CEK-05.1	Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	Yes	CSP-owned	A formal Change Management Policy has been defined in order to ensure that cryptogprahy, encryption, and key management technology changes have been authorized and communicated.		CEK-05	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.	Encryption Change Management	
CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	Yes	CSP-owned	All ConfigCat production systems are managed through our change management processes.		CEK-06	Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.	Encryption Change Cost Benefit Analysis	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	Yes	CSP-owned	Related risks are part of ConfigCat's Risk Management Plan		CEK-07	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	Encryption Risk Management	
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	No	CSP-owned			CEK-08	CSPs must provide the capability for CSCs to manage their own data encryption keys.	CSC Key Management Capability	
CEK-09.1	Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event?	Yes	CSP-owned	All policies and processes are reviewed at minimum annually and more frequently due to any changes or a security event. The policies and procedures are then reviewed and attested to by third-party auditor(s) as part of our annual ISO audit.		CEK-09	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s).	Encryption and Key Management Audit	
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Yes	CSP-owned	ConfigCat reviews and audits at least annually and on an as-needed basis its encryption and key management systems, policies, and processes.					
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Yes	CSP-owned	ConfigCat services are required to adhere to both the key management standard and the cryptographic standard. These standards mandate the use of standard algorithms in the context of ConfigCat's key management and cryptographic practices		CEK-10	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	Key Generation	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes	CSP-owned	Private keys are managed, and cryptography is kept secret.		CEK-11	Manage cryptographic secret and private keys that are provisioned for a unique purpose.	Key Purpose	Cryptography, Encryption & Key Management
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Yes	CSP-owned	This process is governed by ConfigCat's SSL Renewal Policy and Secret Management Policy.		CEK-12	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.	Key Rotation	
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?	Yes	CSP-owned	This process is governed by ConfigCat's SSL Renewal Policy and Secret Management Policy.		CEK-13	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.	Key Revocation	
CEK-14.1	Are processes, procedures and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions?	Yes	CSP-owned	This process is governed by ConfigCat's SSL Renewal Policy and Secret Management Policy.		CEK-14	Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements.	Key Destruction	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
CEK-15.1	Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	CSP-owned			CEK-15	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.	Key Activation	
CEK-16.1	Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	CSP-owned			CEK-16	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.	Key Suspension	
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	CSP-owned			CEK-17	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.	Key Deactivation	
CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	CSP-owned			CEK-18	Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.	Key Archival	

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
CEK-19.1	Are processes, procedures, and technical measures to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	CSP-owned			CEK-19	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.	Key Compromise	
CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSP-owned	This process is governed by ConfigCat's SSL Renewal Policy and Secret Management Policy.		CEK-20	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.	Key Recovery	
CEK-21.1	Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions?	NA	CSP-owned			CEK-21	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.	Key Inventory Management	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DCS-01.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does not own or maintain any physical infrastructure or data centers. More information can be found here: https://www.linode.com/legal-security/		DCS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually.	Off-Site Equipment Disposal Policy and Procedures	
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does not own or maintain any physical infrastructure or data centers. More information can be found here: https://www.linode.com/legal-security/					
DCS-01.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does not own or maintain any physical infrastructure or data centers. More information can be found here: https://www.linode.com/legal-security/					
DCS-02.1	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does not own or maintain any physical infrastructure or data centers. More information can be found here: https://www.linode.com/legal-security/ https://www.digitalocean.com/security			Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually.		

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does not own or maintain any physical infrastructure or data centers. More information can be found here: https://www.linode.com/legal-security/ https://www.digitalocean.com/security		DCS-02		Off-Site Transfer Authorization Policy and Procedures	
DCS-02.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does not own or maintain any physical infrastructure or data centers. More information can be found here: https://www.linode.com/legal-security/ https://www.digitalocean.com/security					
DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	NA	CSP-owned	ConfigCat is a remote-only company, we do not have a physical office.		DCS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually.	Secure Area Policy and Procedures	
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	NA	CSP-owned	ConfigCat is a remote-only company, we do not have a physical office.					

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does not own or maintain any physical		DCS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually.	Secure Media Transportation Policy and Procedures	Datacenter Security
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does not own or maintain any physical					
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does		DCS-05	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.	Assets Classification	
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does		DCS-06	Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.	Assets Cataloguing and Tracking	
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does not own or maintain any physical infrastructure or data centers. More information can be found here:		DCS-07	Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas.	Controlled Access Points	

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does not own or maintain any physical infrastructure or data centers. More information can be found here:		DCS-07		Controlled Access Points	
DCS-08.1	Is equipment identification used as a method for connection authentication?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by		DCS-08	Use equipment identification as a method for connection authentication.	Equipment Identification	
DCS-09.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does not own or maintain any physical infrastructure or data centers. More information can be found here:		DCS-09	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.	Secure Area Authorization	
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does not own or maintain any physical infrastructure or data centers. More information can be found here:					
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does not own or maintain any physical		DCS-10	Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.	Surveillance System	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does		DCS-11	Train datacenter personnel to respond to unauthorized ingress or egress attempts.	Unauthorized Access Response Training	
DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does not own or maintain any physical infrastructure or data centers. More information can be found here: https://www.linode.com/legal-security/		DCS-12	Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.	Cabling Security	
DCS-13.1	Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does not own or maintain any physical		DCS-13	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	Environmental Systems	
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does		DCS-14	Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.	Secure Utilities	
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean. ConfigCat utilizes the Linode and DigitalOcean architecture and hardware provided by their cloud service offerings and does		DCS-15	Keep business-critical equipment away from locations subject to high probability for environmental risk events.	Equipment Location	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	Yes	CSP-owned	ConfigCat has a documented Information Security Policy, and it is reviewed at least annually. Any changes or updates made to this policy are documented and communicated.		DSP-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.	Security and Privacy Policy and Procedures	
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	All Information Security Policies have a policy owner. Each policy is reviewed at least annually and approved by the owner(s) of the policy.					
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	NA	3rd-party outsourced	ConfigCat services reside within Linode and DigitalOcean; data disposal for cloud-hosted storage media is performed by their respective parties under contract.		DSP-02	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.	Secure Disposal	
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Yes	CSP-owned			DSP-03	Create and maintain a data inventory, at least for any sensitive data and personal data.	Data Inventory	
DSP-04.1	Is data classified according to type and sensitivity levels?	Yes	CSP-owned	ConfigCat's information classification policy classifies data based on its type and sensitivity as Highly Confidential, Confidential and Public.		DSP-04	Classify data according to its type and sensitivity level.	Data Classification	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Yes	CSP-owned	We have a detailed data flow diagram for the ConfigCat services which accounts for all system connections and data flowing through the connections.		DSP-05	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.	Data Flow Documentation	
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Yes	CSP-owned	Documentation of data flow is reviewed on an annual basis by policy.					
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Yes	CSP-owned	They are documented in ConfigCat's Privacy Policy: https://configcat.com/policies/privacy/		DSP-06	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.	Data Ownership and Stewardship	
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	Yes	CSP-owned	Reviewed annually and additionally on need-basis.					
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Yes	CSP-owned	ConfigCat's s security governance framework is aligned with ISO 27002 framework and it is strictly based on ISO 27001 security objectives.		DSP-07	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.	Data Protection by Design and Default	

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Yes	CSP-owned	ConfigCat incorporates "Privacy by Design" to ensure that privacy concerns are taken into account from the beginning while designing systems, products, and business practices.		DSP-08	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	Data Privacy by Design and Default	Data Security and Privacy Lifecycle Management
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	Yes	Shared CSP and CSC	ConfigCat follows the laws and rules that apply to our services and business location. We offer subscribers tools and features to help them regulate data correctly.					
DSP-09.1	Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations and industry best practices?	Yes	CSP-owned	ConfigCat performs DPIA with respect to applicable laws, regulations, and industry best-practices annually or as needed.		DSP-09	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.	Data Protection Impact Assessment	
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	Yes	CSP-owned	ConfigCat has defined, implemented, and evaluated processes, procedures, and technical measures to protect personal or sensitive data during transfer and ensure that such data is only processed within the permissible scope as allowed by applicable laws and regulations.		DSP-10	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Sensitive Data Transfer	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	Yes	CSP-owned	See ConfigCat's Privacy Policy here: https://configcat.com/policies/privacy/		DSP-11	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.	Personal Data Access, Reversal, Rectification and Deletion	
DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?	Yes	Shared CSP and CSC	We ensure that (when applicable) our product and internal processes comply with and enable customers to comply with General Data Protection Regulation(GDPR), a European Union regulation that establishes commercial standards for data protection and privacy for all individuals within the	Customers have the option to sign a DPA with ConfigCat	DSP-12	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	Limitation of Purpose in Personal Data Processing	
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	Yes	CSP-owned	ConfigCat has an internal Supplier/Data processor Policy which is an overall organizational program for achieving a level of awareness and readiness for Supplier/Data processor relationships.		DSP-13	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	Personal Data Sub-processing	
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	Yes	CSP-owned	Customers of ConfigCat have the option to participate in a Data Processing Agreement (DPA), which outlines the parties' mutual understanding regarding the handling of personal data.		DSP-14	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.	Disclosure of Data Sub-processors	
DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	NA		ConfigCat maintains separate environments for development, testing, and production systems. This question is essentially N/A to ConfigCat because we have procedures in place		DSP-15	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.	Limitation of Production Data Use	

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes	CSP-owned	The data retention, archiving, and deletion processes at ConfigCat follow business requirements, applicable law, and regulations, including GDPR principles. ConfigCat's Privacy Policy: https://configcat.com/policies/privacy/		DSP-16	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	Data Retention and Deletion	
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Yes	CSP-owned	ConfigCat details the processes, procedures, and techincal measures defined and implemented to protect sensitive data throughout it's lifecycle in the Data Processing Agreement and		DSP-17	Define and implement, processes, procedures and technical measures to protect sensitive data throughout it's lifecycle.	Sensitive Data Protection	
DSP-18.1	Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations?	Yes	CSP-owned	Please review ConfigCat's Privacy Policy at https://configcat.com/policies/privacy/		DSP-18	The CSP must have in place, and describe to CSCs the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations. The CSP must give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.	Disclosure Notification	
DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?	Yes	CSP-owned	Please review ConfigCat's Privacy Policy at https://configcat.com/policies/privacy/					

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	Yes	Shared CSP and CSC	To ensure high availability and low response times all around the globe ConfigCat provides data centers at multiple global locations. ConfigCat uses Cloudflare Edge	Customers can control the geographic location where their config JSONs get published to. Currently available geographical areas: Global and EU Only (compliant with	DSP-19	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.	Data Location	
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	All of ConfigCat's Information Security and Privacy policies and procedures are reviewed on an ongoing basis. They are being communicated to all employees, and approved by senior management as part of our compliance requirements.		GRC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.	Governance Program Policy and Procedures	
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	All of ConfigCat's Information Security and Privacy policies and procedures are reviewed on an ongoing basis. They are being communicated to all employees, and approved by senior management as part of our compliance requirements.					
GRC-02.1	Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?	Yes	CSP-owned	ConfigCat has a documented Risk Assessment Plan that is made available to all employees in the organization.		GRC-02	Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.	Risk Management Program	

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Yes	CSP-owned	Policies and procedures are reviewed at least annually. Updates are typically based on changes in business and regulatory requirements and must be approved by management.		GRC-03	Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.	Organizational Policy Reviews	Governance, Risk and Compliance
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Yes	CSP-owned	Exceptions are being managed and reviewed as part of ConfigCat's internal compliance processes.		GRC-04	Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.	Policy Exception Process	
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Yes	CSP-owned	ConfigCat has a comprehensive set of information security policies based on industry standards and best practices. ConfigCat has mapped its policies and standards to ISO27001 and this covers		GRC-05	Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.	Information Security Program	
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes	CSP-owned	All leadership and security roles, and responsibilities are defined and documented.		GRC-06	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	Governance Responsibility Model	
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Yes	CSP-owned	ConfigCat has implemented a collection of information security policies that adhere to industry standards and best practices, including ISO/IEC 27001, and regulatory		GRC-07	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.	Information System Regulatory Mapping	
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	Yes	CSP-owned	ConfigCat collaborates with external special interest groups to leverage their knowledge on the latest security standards and best practices.		GRC-08	Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.	Special Interest Groups	

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
HRS-01.1	Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Background checks are performed to the extent permitted by local laws.		HRS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually.	Background Screening Policy and Procedures	
HRS-01.2	Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?	Yes	CSP-owned	ConfigCat's background check include inquiries regarding educational background, work history as permitted by applicable law.					

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Our policy undergoes an annual review and is updated as needed to ensure its relevance and effectiveness.					
HRS-02.1	Are policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	ConfigCat has established a Device Policy to govern the use of privately and company-owned devices, such as desktops, laptops, mobile phones, tablets that can connect to ConfigCat resources.		HRS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually.	Acceptable Use of Technology Policy and Procedures	
HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually?	Yes	CSP-owned	The policies and standards are reviewed by relevant stakeholders and approved by document owners at least annually.					

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Our Cyber Hygene Policy outlines requirements for achieving a level of awareness and readiness for security events. Sets the minimal level of security measures to be taken to ensure business continuity. All employees are responsible for the hygiene of their own devices they are		HRS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually.	Clean Desk Policy and Procedures	Human Resources
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes	CSP-owned	The Cyber Hygene Policy is reviewed by relevant stakeholders and approved by document owners at least annually.					
HRS-04.1	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	ConfigCat is a remote-only company, and all our assets are utilized remotely. We have established and documented policies and procedures that outline the requirements for maintaining information security at remote sites and locations.Our Cyber Hygene Policy outlines requirements for		HRS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually.	Remote and Home Working Policy and Procedures	
HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	Yes	CSP-owned	The Cyber Hygene Policy is reviewed by relevant stakeholders and approved by document owners at least annually.					
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	CSP-owned	ConfigCat has a well-defined exit process including asset return procedures for terminated employees. Company-owned assets must be returned when the employee leaves		HRS-05	Establish and document procedures for the return of organization-owned assets by terminated employees.	Asset returns	

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Yes	CSP-owned	ConfigCat has an Employee Onboarding and Offboarding Procedure in place that defines termination processes. Termination processes cover all		HRS-06	Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment.	Employment Termination	
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Yes	CSP-owned	Employees must be familiar with internal processes and policies and pass a security test in addition to a confidentiality agreement upon hire before gaining access to information		HRS-07	Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.	Employment Agreement Process	
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes	CSP-owned	ConfigCat ensures that its employees understand their obligations to comply with published security policies, procedures, and standards. As part of the onboarding process, all newly hired employees are required to take a		HRS-08	The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.	Employment Agreement Content	
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Yes	CSP-owned	Security roles and responsibilities with detailed functions are communicated through ConfigCat Wiki.		HRS-09	Document and communicate roles and responsibilities of employees, as they relate to information assets and security.	Personnel Roles and Responsibilities	
HRS-10.1	Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?	Yes	CSP-owned	This is included in our overall Information Security Policy which is reviewed annually.		HRS-10	Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details.	Non-Disclosure Agreements	
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Yes	CSP-owned	A comprehensive security awareness training program is established, documented, approved, communicated, applied, evaluated, and maintained for all employees of the organization. In addition to quarterly		HRS-11	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.	Security Awareness Training	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
HRS-11.2	Are regular security awareness training updates provided?	Yes	CSP-owned	Throughout the year, all employees are consistently provided with regular communications to ensure they remain attentive to the best security practices.		HRS-11		Security Awareness Training	
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	CSP-owned	Prior to being granted access to organizational data, ConfigCat employees are educated about their responsibilities in maintaining compliance with published security policies, procedures, and standards.		HRS-12	Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Personal and Sensitive Data Awareness and Training	
HRS-12.2	Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	Yes	CSP-owned	When applicable, recipients of sensitive information receive regular security awareness updates. Security education is an ongoing and regularly conducted process aimed at minimizing risks.					
HRS-13.1	Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?	Yes	CSP-owned	As part of the employee onboarding program, ConfigCat employees are provided with clear guidance on their responsibilities and security best practices. Furthermore, ConfigCat employees are actively informed about their role in upholding compliance with published security policies, procedures, and standards.		HRS-13	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.	Compliance User Responsibility	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	ConfigCat's Access Control Policy is an overall organizational program for achieving a level of awareness and readiness for accessing our Assets and Third-party services securely. All employees are responsible for		IAM-01	Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually.	Identity and Access Management Policy and Procedures	
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	We review our policy annually and additionally on a need-basis.					
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	ConfigCat has a company-wide Password Policy that collects the general requirements for all existing and new passwords generated. Our Password Policy follows industry standards and best practices.		IAM-02	Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.	Strong Password Policy and Procedures	
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	ConfigCat reviews and updates its information security policies at least once a year. These policies cover guidelines for accessing and verifying user identities, which involve using strong passwords.					
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes	CSP-owned	Every employee of ConfigCat must have the appropriate privileges for their job, and privileges should be determined based on employment status, job role, regulatory and		IAM-03	Manage, store, and review the information of system identities, and level of access.	Identity Inventory	
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes	CSP-owned	The Owner of a system is responsible to ensure that access restriction configurations of a system are appropriate for the classification of information held within and to be able		IAM-04	Employ the separation of duties principle when implementing information system access.	Separation of Duties	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes	CSP-owned	Access to applications, operating systems, databases, and network devices are provisioned according to the principle of least privilege.		IAM-05	Employ the least privilege principle when implementing information system access.	Least Privilege	
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes	CSP-owned	Users are given appropriate access rights based upon their role and profile.		IAM-06	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	User Access Provisioning	
IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	Yes	CSP-owned	ConfigCat has an established Access Control Policy and Offboarding Procedure that oversees the granting, modifying, and terminating of access to the ConfigCat systems.		IAM-07	De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.	User Access Changes and Revocation	
IAM-08.1	Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?	Yes	CSP-owned	ConfigCat performs reviews of privileged and regular user access to production critical systems on a regular basis to determine access appropriateness.		IAM-08	Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.	User Access Review	
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	Yes	CSP-owned	System access rights are granted or modified on a business-need basis depending on the employee's job role and/or specific management request.		IAM-09	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated.	Segregation of Privileged Access Roles	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Yes	CSP-owned	ConfigCat conducts quarterly evaluations of privileged user access to crucial systems in production.		IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.	Management of Privileged Access Roles	Identity & Access Management
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	Yes	CSP-owned	ConfigCat implements strict access controls and follows the principle of least privilege when it comes to granting access to internal systems. Prior to granting access, authorization is obtained from an authorized					
IAM-11.1	Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?	No	CSP-owned	We do not provide admin level access to our customers		IAM-11	Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.	CSCs Approval for Agreed Privileged Access Roles	
IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated?	Yes	CSP-owned	As per our Logging and Monitoring Policy, administrator and operator logs must be kept locally on all servers and machines. The logs must not be deleted. Only the Security Team has access to viewing the logs.		IAM-12	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.	Safeguard Logs Integrity	

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IAM-12.2	Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?	Yes	CSP-owned	Only the Security Team has access to viewing the logs.		IAM-12		Safeguard Logs Integrity	
IAM-13.1	Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?	Yes	CSP-owned	ConfigCat's access, authentication and monitoring standard includes requirements for unique user accounts to identify individuals.		IAM-13	Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.	Uniquely Identifiable Users	
IAM-14.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?	Yes	CSP-owned	Access to all organizational core services requires multifactor authentication. Multifactor authentication should be turned on for all third-party service access where possible.		IAM-14	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	Strong Authentication	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Yes	CSP-owned	Our access control measures enforce multifactor authentication as a requirement for accessing critical information systems, ensuring an equivalent security level for system identities.		IAM-14		Strong Authentication	
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Yes	CSP-owned	We have a Password policy in place that defines the minimum requirements for passwords across all systems, including computers, servers, network devices, and services. These		IAM-15	Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.	Passwords Management	
IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Yes	CSP-owned	Every employee of ConfigCat must have the appropriate privileges for their job, and privileges should be determined based on employment status, job role, regulatory and		IAM-16	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	Authorization Mechanisms	
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	Yes	CSP-owned	While ConfigCat provides comprehensive information about the use and functionality of its APIs, there are currently no established policies or procedures specifically dedicated to governing communications between application services (e.g., APIs). For detailed information on the ConfigCat APIs, including their usage and functions, please refer to the documentation available at https: //configcat.com/docs/advanced/public-api/			Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually.		

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Yes	CSP-owned	ConfigCat provides documentation on the interoperability of customer data. See ConfigCat's Terms of Service: https://configcat.com/policies/		IPY-01		Interoperability and Portability Policy and Procedures	
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	NA	CSP-owned	The mentioned risk considerations do not apply to ConfigCat as it is a Software-as-a-Service (SaaS) provider. Therefore, ConfigCat does not have specific policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained solely for application development portability.					

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	Yes	CSP-owned	Our Privacy policy provides detailed information regarding how we handle information/data exchange, usage, portability, integrity, and persistence: https://configcat.com/policies/privacy/					Interoperability & Portability
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	ConfigCat performs annual reviews of its privacy and security policies.					
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes	Shared CSP and CSC	Interoperability is facilitated through APIs, which are thoroughly documented at https://api.configcat.com/docs/. All API connections take place over a secure HTTPS protocol, ensuring the confidentiality and integrity of data exchange.		IPY-02	Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability.	Application Interface Availability	
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	Yes	CSP-owned	For data transit and replication between nodes using TLS 1.2/1.3 and data at-rest using standard AES (CBC) algorithm with built-in MySQL plugin.		IPY-03	Implement cryptographically secure and standardized network protocols for the management, import and export of data.	Secure Interoperability and Portability Management	

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IPY-04.1	Do agreements include provisions specifying CSC data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Yes	CSP-owned	ConfigCat's agreements with CSCs include provisions that specify CSC data access upon contract termination. The required information regarding data access, format, duration of data storage, scope of retained data available to CSCs, and the data deletion policy can be found in ConfigCat's Terms of Service Agreement and Privacy Policy.		IPY-04	Agreements must include provisions specifying CSCs access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Data Portability Contractual Obligations	
IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	ConfigCat has established and documented infrastructure and virtualization security policies and procedures. These policies and procedures are outlined in ConfigCat's Information Security Policy. They have		IVS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.	Infrastructure and Virtualization Security Policy and Procedures	
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Our policies undergo an annual review and is updated as needed to ensure its relevance and effectiveness.					
IVS-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?	Yes	CSP-owned	We use monitoring software to identify ongoing system performance concerns, capacity, changing resource utilization needs, and unusual system activity. When specific predefined thresholds are met, personnel are		IVS-02	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	Capacity and Resource Planning	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IVS-03.1	Are communications between environments monitored?	Yes	CSP-owned	ConfigCat's engineering team continuously monitors communications between environments .		IVS-03	Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.	Network Security	Infrastructure & Virtualization Security
IVS-03.2	Are communications between environments encrypted?	Yes	CSP-owned	For data transit and replication between nodes using TLS 1.2/1.3 and data at-rest using standard AES (CBC) algorithm with built-in MySQL plugin.					
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes	CSP-owned	ConfigCat's environments are separated and customers' data is not transferred between the production and lower environments.					
IVS-03.4	Are network configurations reviewed at least annually?	Yes	CSP-owned	Our policies undergo an annual review and is updated as needed to ensure its relevance and effectiveness.					

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Yes	CSP-owned						
IVS-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	Yes	Shared CSP and 3rd-party			IVS-04	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.	OS Hardening and Base Controls	
IVS-05.1	Are production and non-production environments separated?	Yes	CSP-owned	Production environments are segregated from non-production environments.		IVS-05	Separate production and non-production environments.	Production and Non-Production Environments	
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	Yes	CSP-owned			IVS-06	Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants.	Segmentation and Segregation	

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IVS-07.1	Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?	Yes	CSP-owned			IVS-07	Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.	Migration to Cloud Environments	
IVS-08.1	Are high-risk environments identified and documented?	Yes	CSP-owned	High risk environments are identified and protected from access to only authorized users using access control lists.		IVS-08	Identify and document high-risk environments.	Network Architecture Documentation	
IVS-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?	Yes	CSP-owned	For the cloud-based environment where the ConfigCat services are hosted. ConfigCat does not maintain any control of or access to the network layer.		IVS-09	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.	Network Defense	
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	ConfigCat has a Logging and Monitoring Policy in place that provides accurate and comprehensive logs and monitoring in order to detect and react to unexpected events and to provide information for error investigation.		LOG-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.	Logging and Monitoring Policy and Procedures	
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Our policies undergo an annual review and is updated as needed to ensure its relevance and effectiveness.					

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Yes	CSP-owned			LOG-02	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.	Audit Logs Protection	
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes	CSP-owned	ConfigCat uses a set of Cloud-native tools that monitor activities, and mitigate risks and configuration mistakes.		LOG-03	Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.	Security Monitoring and Alerting	
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	Yes	CSP-owned	ConfigCat uses a set of Cloud-native tools that monitor activities, and mitigate risks and configuration mistakes.					
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes	CSP-owned	Access to audit logs are restricted to authorized personnel based on job roles and responsibilities. Audit logs are stored locally on all		LOG-04	Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.	Audit Logs Access and Accountability	
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Yes	CSP-owned	ConfigCat employs tools that detect unusual activity and measure processing queues to ensure the timely handling of incoming data. These tools also enable real-time monitoring of results to maintain effective data processing		LOG-05	Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.	Audit Logs Monitoring and	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes	CSP-owned	Our engineers receive warning from our monitoring tools which are then reviewed and appropriate actions are taken without any delay.		LOG-05		Response	Logging and Monitoring
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes	CSP-owned	ConfigCat uses a synchronised time protocol in order to ensure that all systems have a common time reference.		LOG-06	Use a reliable time source across all relevant information processing systems.	Clock Synchronization	
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Yes	CSP-owned	ConfigCat's applicable standards to logging and monitoring include a defined listing of required security events to support audit and investigations.		LOG-07	Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment.	Logging Scope	
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	Yes	CSP-owned	Our policies and scopes undergo an annual review and is updated as needed to ensure its relevance and effectiveness.					
LOG-08.1	Are audit records generated, and do they contain relevant security information?	Yes	CSP-owned	ConfigCat's applicable standards to logging and monitoring include a defined listing of required security events to support audit and investigations.		LOG-08	Generate audit records containing relevant security information.	Log Records	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Yes	CSP-owned	Access rights to audit records are managed based on the principle of least privilege.		LOG-09	The information system protects audit records from unauthorized access, modification, and deletion.	Log Protection	
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	Yes	CSP-owned			LOG-10	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.	Encryption Monitoring and Reporting	
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Yes	CSP-owned			LOG-11	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.	Transaction/Activity Logging	
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	NA	CSP-owned	ConfigCat is a remote-only company, we do not have a physical office. Our services rely on Microsoft Azure, Digital Ocean, and Linode cloud		LOG-12	Monitor and log physical access using an auditable access control system.	Access Control Logs	
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Yes	CSP-owned	Service anomalies must be reported to the DevOps Team.		LOG-13	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.	Failures and Anomalies Reporting	
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Yes	CSP-owned	Service anomalies must be reported to the DevOps Team.					

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
SEF-01.1	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	As part of our disaster recovery plan, ConfigCat has implemented a comprehensive security incident response practice. This practice encompasses policies, procedures, and processes that span from incident		SEF-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually.	Security Incident Management Policy and Procedures	
SEF-01.2	Are policies and procedures reviewed and updated annually?	Yes	CSP-owned	All of ConfigCat's Information Security and Privacy policies and procedures are reviewed annually or on an as-needed basis. They are communicated to all employees, and approved by senior management as part of our					
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	As an integral component of our disaster recovery plan, ConfigCat has implemented security incident management policies, procedures, and standards. These protocols have been established, approved by		SEF-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually.	Service Management Policy and Procedures	
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Yes	CSP-owned	We ensure regular review and updates of these policies on an annual basis.					
SEF-03.1	Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	We have an Incident Communication Plan in place that ensures that ConfigCat customers, business-critical relationships, authorities and insurance companies are informed of the event of an incident, the progress of the ongoing investigation, and the resolution of the issue. Regardless, ongoing service related		SEF-03	'Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted.'	Incident Response Plans	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	Yes	CSP-owned			SEF-04	Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.	Incident Response Testing	Security Incident Management, E-Discovery, & Cloud Forensics
SEF-05.1	Are information security incident metrics established and monitored?	Yes	CSP-owned	Key security program metrics are reviewed monthly.		SEF-05	Establish and monitor information security incident metrics.	Incident Response Metrics	
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Yes	CSP-owned	A dedicated team analyzes diverse security data sources to identify suspicious activity. They continuously monitor for indicators of attacks. Emphasis is placed on developing attack hypotheses and gathering		SEF-06	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.	Event Triage Processes	
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes	CSP-owned	Notification requirements are usually defined in the contract, and our incident and notification procedures follow industry best practices.		SEF-07	Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.	Security Breach Notification	
SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	Yes	CSP-owned	ConfigCat complies with all relevant breach notification obligations and is committed to safeguarding your data and being transparent in the event of a data breach.					

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Yes	CSP-owned			SEF-08	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.	Points of Contact Maintenance	
STA-01.1	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	Please review ConfigCat's Terms of Service and Privacy policy in that regards.		STA-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually.	SSRM Policy and Procedures	
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Yes	CSP-owned	ConfigCat continually reviews its Information Security and Privacy policies and procedures, ensuring they remain up-to-date. These policies are communicated to all employees and undergo approval by senior management to meet our compliance requirements."					
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes	CSP-owned	ConfigCat has a Supplier/Data processor policy in place that is an overall organizational program for achieving a level of awareness and readiness for Supplier/Data processor relationships.		STA-02	Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.	SSRM Supply Chain	

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	Yes	Shared CSP and CSC	ConfigCat's supply chain could be reviewed in its subprocessors page: https://configcat.com/policies/subprocessors/. ConfigCat does not engage in any		STA-03	Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.	SSRM Guidance	Supply Chain Management, Transparency, and Accountability
STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	Yes	Shared CSP and CSC	ConfigCat's supply chain could be reviewed in its subprocessors page: https://configcat.com/policies/subprocessors/. ConfigCat does not engage in any		STA-04	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.	SSRM Control Ownership	
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Yes	CSP-owned	Policies and procedures are reviewed at least annually. Updates are typically based on changes in business and regulatory requirements and must be approved by management.		STA-05	Review and validate SSRM documentation for all cloud services offerings the organization uses.	SSRM Documentation Review	
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes	CSP-owned	These are being reviewed as part of ConfigCat's internal audit processes and workflows.		STA-06	Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.	SSRM Control Implementation	
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	Yes	CSP-owned	ConfigCat maintains public subprocessor lists for transparency: https://configcat.com/policies/subprocessors/		STA-07	Develop and maintain an inventory of all supply chain relationships.	Supply Chain Inventory	
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Yes	CSP-owned	The Security Team is responsible for monitoring changes in Supplier/Data processors' services and re-checking the Supplier/Data processors security-related policies and certifications		STA-08	CSPs periodically review risk factors associated with all organizations within their supply chain.	Supply Chain Risk Management	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
STA-09.1	Do service agreements between CSPs and CSCs (tenants) incorporate at least the following mutually agreed upon provisions and/or terms? • Scope, characteristics, and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third-party assessment • Service termination • Interoperability and portability requirements • Data privacy	Yes	CSP-owned	All mutually agreed provisions listed are incorporated within the ConfigCat's and CSCs' mutual contracts.		STA-09	Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third party assessment • Service termination • Interoperability and portability requirements • Data privacy	Primary Service and Contractual Agreement	
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	Yes	CSP-owned	Our policies undergo an annual review and is updated as needed to ensure its relevance and effectiveness.		STA-10	Review supply chain agreements between CSPs and CSCs at least annually.	Supply Chain Agreement Review	
STA-11.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	Yes	CSP-owned	ConfigCat adheres to a yearly internal assessment process to validate the adherence and efficiency of standards, policies, procedures, and SLA activities.		STA-11	Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually.	Internal Compliance Testing	
STA-12.1	Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Yes	Shared CSP and 3rd-party	ConfigCat establishes contractual agreements that require the applicable external vendors to adhere to ConfigCat's security policies and change management requirements.		STA-12	Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards.	Supply Chain Service Agreement Compliance	

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	Yes	CSP-owned	At least annually, ConfigCat reviews the provision of services from its suppliers		STA-13	Periodically review the organization's supply chain partners' IT governance policies and procedures.	Supply Chain Governance Review	
STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	Yes	CSP-owned	ConfigCat has a Supplier/Data processor policy in place that is an overall organizational program for achieving a level of awareness and readiness for Supplier/Data processor		STA-14	Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.	Supply Chain Data Security Assessment	
TVM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation?	Yes	CSP-owned	We have a dedicated vulnerability management process that actively scans for security threats using the certified third-party scanning tools. Also, we have a bug bounty program for those individual researchers in the security community that provide		TVM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually.	Threat and Vulnerability Management Policy and Procedures	
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	ConfigCat reviews, at least annually and on an as-needed basis, its internal security and privacy policies and makes them available to all employees.					
TVM-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	We have a dedicated vulnerability management process that actively scans for security threats using the certified third-party scanning tools.		TVM-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually.	Malware Protection Policy	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	ConfigCat reviews, at least annually and on an as-needed basis, its internal security and privacy policies and makes them available to all employees.		TVM-02		and Procedures	
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk)?	Yes	CSP-owned	We have a dedicated vulnerability management process that actively scans for security threats using the certified third-party scanning tools. Every two months, we have a Security Week, where our Core Team conducts thorough system audits, provides		TVM-03	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.	Vulnerability Remediation Schedule	
TVM-04.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	No	CSP-owned	To ensure comprehensive protection, we have established robust 3rd party dependency security vulnerability procedures.These procedures involve continuous monitoring and evaluation of third-party dependencies, software libraries, and integrations that we use within our products and services. We		TVM-04	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.	Detection Updates	Threat & Vulnerability Management
TVM-05.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the organization's vulnerability management policy)?	Yes	CSP-owned	To ensure comprehensive protection, we have established robust "3rd party dependency security vulnerability procedures." These procedures involve continuous monitoring and evaluation of third-party dependencies, software libraries, and integrations that we use within our products and services. We		TVM-05	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.	External Library Vulnerabilities	
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Yes	CSP-owned	We manage a Security Bug Bounty program (https://configcat.com/bounty/). This initiative involves ethical hackers and researchers worldwide who help us identify and address vulnerabilities continuously, strengthening our security posture		TVM-06	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.	Penetration Testing	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Yes	CSP-owned	We have a dedicated vulnerability management process that actively scans for security threats using the certified third-party scanning tools.		TVM-07	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.	Vulnerability Identification	
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	No	CSP-owned			TVM-08	Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.	Vulnerability Prioritization	
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes	CSP-owned	Our vulnerability management program consolidates all vulnerabilities, regardless of how they are discovered. Each vulnerability undergoes validation, risk-ranking, and is then assigned to the relevant stakeholders for remediation.		TVM-09	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.	Vulnerability Management Reporting	
TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Yes	CSP-owned			TVM-10	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.	Vulnerability Management Metrics	
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes	CSP-owned	ConfigCat has implemented a collection of information security policies that adhere to industry standards and best practices, including ISO/IEC 27001, and regulatory requirements.		UEM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually.	Endpoint Devices Policy and Procedures	
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Our policies undergo an annual review and is updated as needed to ensure its relevance and effectiveness.					

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
UEM-02.1	Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?	No	CSP-owned			UEM-02	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.	Application and Service Approval	Universal Endpoint Management
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	No	CSP-owned			UEM-03	Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.	Compatibility	
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Yes	CSP-owned	We closely track company-issued devices and their status. This includes laptops, smartphones, and tablets.		UEM-04	Maintain an inventory of all endpoints used to store and access company data.	Endpoint Inventory	
UEM-05.1	Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?	Yes	CSP-owned	ConfigCat has policies in place which define the security control requirements for endpoints permitted to access systems or handle organizational data.		UEM-05	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.	Endpoint Management	
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	No	CSP-owned			UEM-06	Configure all relevant interactive-use endpoints to require an automatic lock screen.	Automatic Lock Screen	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	No	CSP-owned			UEM-07	Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.	Operating Systems	
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	Yes	CSP-owned	ConfigCat requires endpoints to be full disk encrypted as the default configuration.		UEM-08	Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.	Storage Encryption	
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	No	CSP-owned			UEM-09	Configure managed endpoints with anti-malware detection and prevention technology and services.	Anti-Malware Detection and Prevention	
UEM-10.1	Are software firewalls configured on managed endpoints?	No	CSP-owned			UEM-10	Configure managed endpoints with properly configured software firewalls.	Software Firewall	
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	No	CSP-owned			UEM-11	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.	Data Loss Prevention	
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	No	CSP-owned			UEM-12	Enable remote geo-location capabilities for all managed mobile endpoints.	Remote Locate	
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	No	CSP-owned			UEM-13	Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.	Remote Wipe	

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
UEM-14.1	Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?	No	CSP-owned			UEM-14	Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets.	Third-Party Endpoint Security Posture	
End of Standard									