Sharing OFFICIAL Information

A description of how Kahootz meets the 14 Cloud Security Principles as defined by the UK Government

Published 21.07.2021

Author Peter Jackson, CTO, Kahootz

1 Executive Summary

1.1 Cloud Security

Organisations across the public and private sectors are realising the cost benefits, flexibility and agility that cloud computing provides. With the rapid growth and choice of cloud service vendors it is sometimes difficult to assess which ones to trust with your sensitive business information.

To solve this problem, and to make the adoption and use of cloud services easier, the UK Government's National Cyber Security Centre (NCSC) has set out 14 Cloud Security Principles that can be used to assess the suitability of cloud services.

This document explains, for each of these cloud security principles, the processes and security controls Kahootz has in place so that you can have total confidence in our cloud collaboration service.

1.2 The need for independent audit

Any security or business continuity statement made by a cloud vendor should be independently verified by a trusted and accredited third party. A key part of our evidence base is that:

- **Our ISO 27001 processes are inspected on an annual basis by an auditor from a UKAS accredited organisation.**
- **The Kahootz service goes through an annual IT Health Check by a CHECK accredited testing partner.**
- **Cyber security within our organisation is regularly tested via the Cyber Essentials Plus scheme, to prevent Internet-originated attacks against our IT systems.**
- **The service availability and uptime is continuously monitored by an independent third-party service and published in the public domain.**

1.3 Kahootz - Trusted by Government

Every organisation should perform their own audit before entrusting a cloud service provider with confidential or sensitive information.

It's reassuring that our security controls have already been assessed, and deemed acceptable, for storing and sharing OFFICIAL (including OFFICIAL-SENSITIVE) information, by many security conscious UK public sector organisations such as:

- **Ministry of Defence**
- **NHS England**
- **Department of Health**
- **Land Registry**
- **Parliament**
- **Legal Aid Agency**
- **National Offender Management Service**
- **Home Office**
- **Government Security Secretariat**
- **Cabinet Office**
- **NHS Digital**
- **Ministry of Justice**
- **Fire & Rescue Service**
- **Civil Service Learning**
- **High Speed 2 Ltd**
- **Criminal Justice System**
- **Youth Justice Board**
- **Crown Commercial Service**

2 Background

In April 2014, the Government Security Classifications Policy changed the way that the public sector classifies and protects its information assets.

There are now just three levels of security classification: OFFICIAL, SECRET and TOP SECRET. OFFICIAL replaces everything up to and including information that was previously marked as RESTRICTED, and that includes the vast majority – about 90% - of all information related to public sector day-today business activities.

OFFICIAL information does not need to be marked, aggregation does not automatically trigger an increase in protective marking, and it can include personal data.

With this change came recognition from CESG (now part of the National Cyber Security Centre) that business impact levels - such as IL2 and IL3 - were not an appropriate way to measure software security – and there is now clear mandate that previous business impact levels must not be used for that purpose.

According to the Cabinet Office: "*OFFICIAL information can be managed with good commercial solutions that mitigate the risks faced by any large corporate organisation."*

That's a pragmatic choice for modern government! It's recognition that, for most Government information, the security requirements are equivalent to a private sector enterprise.

How do you know when a commercial solution is a good commercial solution and is sufficiently secure and well-managed to hold OFFICIAL and confidential business information?

To help with this, the NCSC list 14 *"essential security principles to consider when evaluating cloud services"*[1].

Between them they cover all the security issues related to service provision. Supporting each principle is a set of guidance explaining what it means, why it is required, and a set of possible implementation approaches.

[1] 1 https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

These security changes are reflected in supplier Service Descriptions available via the G-Cloud Digital Marketplace[2]. From G-Cloud 6 onwards suppliers have been required to answer approximately 80 detailed security questions that highlight each supplier's implementation approach for each security principle, and the evidence they have to demonstrate that the approach is effective.

The sections that follow explain in detail the security controls behind Kahootz and specifically how we support the UK Government's 14 cloud security principles.

[2] https://www.digitalmarketplace.service.gov.uk/

3 Overriding Principles

Kahootz has been supplying cloud services to the UK Government since 2002 and we are absolutely committed to keeping your data secure and providing a well-supported, highly available service.

We were one of the first services to gain Pan-Government IL2 Accreditation for cloud collaboration, in March 2013, and Kahootz was successfully re-accredited in March 2014.

Kahootz offers a robust and evidenced implementation for each of the 14 cloud security principles.

The most important evidence that Kahootz offers this is through our independent annual ISO27001 certification, IT Health Check and Cyber Essentials Plus certification.

3.1 ISO27001 Certification

Kahootz has been certified to ISO27001 since December 2012. We have been audited annually since then and have an excellent record which includes zero failures, zero recommendations and zero observations.

Importantly, the scope of the Kahootz ISO27001 certification was agreed with a CESG Pan-Government Accreditor as part of our original IL2 Accreditation. It is:

The development, delivery and maintenance of collaboration and consultation software solutions. This includes the operation and support of Kahootz, information assets such as client data and all physical assets. This is in accordance with the Statement of Applicability Issue 1.0

One aspect of ISO27001 is to identify an organisation's assets and to assess the importance of these by giving them a score for confidentiality, integrity and availability.

The Kahootz service itself and the data we hold on behalf of our clients are afforded the highest possible scores. As such, the service dominates our well-documented security framework.

3.2 IT Health Check

Kahootz undertakes an annual IT Health Check (ITHC) by a CHECK accredited testing partner. This is an exhaustive and rigorous test, undertaken by security experts, to ensure that the service is secure against a determined hacker. It demonstrates that:

- **The service is protected against known attacks such as Cross Site Scripting (XSS), Cross Site Request Forgery (XSRF), Offsite redirection, Click-jacking and SQL Injection.**
- **The user authentication and session management are secure.**
- **Client data is secure and cannot be accessed by other clients' users, or by unauthenticated users.**

3.3 Cyber Essentials Plus

Kahootz's cyber security credentials are assessed via the UK Government approved Cyber Essentials Plus scheme.

This involves an independent third party assessing whether the procedures that we have in place to prevent Internet-originated attacks against our IT systems are sufficient.

The Cyber Essentials Plus test focuses on five key security controls:

- **Boundary firewalls and internet gateways - Ensuring that devices are set up to prevent unauthorised access to or from private networks.**
- **Secure configuration - Ensuring that systems are configured in the most secureway for the needs of the organisation.**
- **Access control - Ensuring only those who should have access to systems to have access and at the appropriate level.**
- **Malware protection - Ensuring that virus and malware protection is installed and up to date.**
- **Patch management - Ensuring that the latest supported versions of applications are used and all the necessary patches supplied by the vendor have been applied.**

3.4. Additional Documentation

The Kahootz Risk Management Accreditation Document Set (RMADS), and Residual Risk Register are available under a non-disclosure agreement.

4 The 14 Cloud Security Principles

The table below shows a summary of the cloud security principles:

1.	Data in transit protection	Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.
2.	Asset protection and resilience	Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.
3.	Separation between consumers	Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another.
4.	Governance framework	The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.
5.	Operational security	The service provider should have processes and procedures in place to ensure the operational security of the service.
6.	Personnel security	Service provider staff should be subject to personnel security screening and security education for their role.
7.	Secure development	Services should be designed and developed to identify and mitigate threats to their security.
8.	Supply chain security	The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.

9.	Secure consumer management	Consumers should be provided with the tools required to help them securely manage their service.
10.	Identity and authentication	Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals.
11.	External interface protection	All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.
12.	Secure service administration	The methods used by the service's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.
13.	Audit information provision to consumers	Consumers should be provided with the audit records they need to monitor access to their service and the data held within it.
14.	Secure use of the service by the consumer	Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected.

5 How Kahootz meets the Principles

This section explains how Kahootz meets each of the cloud security principles.

5.1 Data in transit protection

All communication between user devices and Kahootz uses a HTTPS / SSL connection which ensures that information is secured using a 256-bit RSA encryption. The service uses a certificate signed by GlobalSign, which provides server authentication. The same level of encryption is used whatever end-user device is used – desktop, mobile or tablet.

Kahootz uses TLS 1.2 (or above) with Forward Secrecy when supported by the browser. Insecure SSL3 is not supported. These settings will work with standard browsers without any changes by the end user. We follow all general updates to protocol support and have protected against SSL attacks such as BEAST, HEARTBLEED and POODLE.

The same level of encryption is used in order to access the Kahootz service via the Kahootz API, (Application Programming Interface.)

If clients ask for a bulk data export, the data is provided according to our ISO27001 processes for secure data transfer.

5.2 Asset Protection and Resilience

5.2.1 Legislation

Kahootz is wholly hosted, managed and supported in the UK. It is provided by a UK company, under UK legislation, which is protected by EU data laws and therefore exempt from the US Patriot Act.

Kahootz is registered under the UK Data Protection Act (registration reference: Z8289153). Kahootz maintains a strong privacy policy to protect customer data. Data within the service remains the property of our customers and we do not use your data or share it with any third parties.

We are fully committed to helping our clients to meet their FOI and GDPR obligations.

5.2.2 Data Centre Security

Kahootz uses modern and purpose-built Tier 3/4 data centres. Our hosting partner provides the world-class infrastructure necessary to keep our service up and running, uninterrupted around the clock.

Physical access to data centres is controlled by an Electronic Access Control System (EACS). All internal and external doors are linked to the EACS, which uses a zoned system to delineate between access rights to various areas. The EACS logs activity on the system. Appropriate alarm systems and perimeter fencing are in place to deter and detect unauthorised entry.

Appropriate CCTV monitoring is present at all sites with footage retained for at least 90 days. It is also secured with internal and external PIR intruder detection systems.

Physical security and visitor access to all data centres is controlled by an ISO27001, PCI-DSS and HMG Baseline Control Set compliant policy. All visitor access to site must be pre-approved by the security team. Visitors must provide government issued ID on arrival and are escorted at all times. Visitor access to the data halls is strictly forbidden.

5.2.3 Data Sanitisation and Equipment Disposal

We will commence data removal one month after your license to use Kahootz expires or earlier upon your request. When this happens, all the data we hold for a consumer will be permanently deleted. Data is removed from the live service within two days of being requested and can take one additional month to be removed from backup services.

The Kahootz ITHC specifically tests that data from expired Kahootz accounts cannot be accessed.

When equipment reaches end-of-life, it is securely erased and disposed of according to the data centre's ISO27001 processes.

5.2.4 Encryption at Rest

Client data is encrypted and stored on dedicated servers that are under the exclusive control of Kahootz technical staff.

All data is strongly encrypted at rest. Disks are encrypted with LUKSv2, using AES-XTS with a 512 bit keysize.

The decryption key is only held in memory, and must be entered manually each time a server is restarted. This means that data is secure against physical theft, and is automatically secure at end-of-life.

Kahootz never uses mobile or removable media to store client data.

5.2.5 Service Availability

The service level agreement for Kahootz is as follows:

- **The minimum availability for the service is 99.95% per month.**
- **The minimum performance is for the server to process 99% of page requests (excluding bulk operations and reports) within 0.75 seconds.**
- **The minimum availability excludes up to 6 hours per quarter annum of scheduled downtime (between 10pm and 6am on weekdays or between 7pm and 6am on weekends).**

To demonstrate that we meet our SLA, we use an independent 3rd party service (Pingdom) to monitor the site and create a public record of availability.[3]

5.2.6 Ensuring Availability

The Kahootz service is provided by a number of independent application servers and uses a load balancer to ensure that the service is not affected by the failure of a single server.

Data within Kahootz is replicated in near real-time to hot standby servers, which can take over in the event of any problem. The Support Team has secure access to the service in order to provide 24/7/365 infrastructure support.

[3] http://stats.pingdom.com/3as4us3d6yr7/674246/history

The Kahootz data centres have at least two entirely geographically diverse network connections and significant network capacity overhead is maintained. The cooling systems, UPS and generator backup are all at least N+1 resilient.

Traffic volume and network flow are monitored to enable an appropriate response to disruptive events such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

5.2.7 Backup

To minimize any interruption due to hardware failure or any other disaster, data within the service is backed up as follows:

- **Near real-time replication of the database and file store to secondary servers.**
- **Hourly backup of the database.**
- **Daily backup of the configuration, database and file store to online storage, stored for up to a month.**
- **Daily encrypted backup of the configuration, database and file store to a separate remote backup server.**

5.2.8 Ensuring Availability

Kahootz operates a comprehensive disaster recovery program.

This is tested annually as part of our ISO27001 certification.

5.3 Separation Between Consumers

Kahootz operates as a multi-tenanted Software-as-a-Service within the Public Cloud. The service is shared by a number of different consumers, in the Public and Private sector.

Our ITHC specifically tests that consumers' data is protected from access by other consumers of the service.

At the network level, the Kahootz servers operate within their own private network, protected by a firewall.

At the compute level, Kahootz uses a mixture of dedicated servers and virtual servers.

The virtual servers use the industry standard XEN platform.

At the application level, separation of consumers is ensured by software architecture and design. The Kahootz Admin Application allows authorised users to manage just their own users and data.

5.4 Governance Framework

Kahootz is wholly hosted, managed and supported in the UK. It is provided by a UK company, under UK legislation, which is protected by EU data laws and therefore exempt from the US Patriot Act.

Kahootz is registered under the UK Data Protection Act (registration reference: Z8289153). Kahootz maintains a strong privacy policy to protect customer data.

Data within the service remains the property of our customers and we do not use your data or share it with anyone else.

5.5 Operational Security

Our ISO27001 framework is modelled on the concept of ‘continuous improvement’ and contains a comprehensive set of policies and procedures to effectively manage security.

5.5.1 Incident Management

Our ISO27001 compliance ensures we have a documented process for incident reporting and management.

All incidents are assigned an owner who is responsible for tracking the incident through to resolution. For each incident, in addition to corrective actions, we identify preventative actions to ensure that the incident does not happen again. The same process is used to track potential vulnerabilities in the service.

Incidents are reported to GovCert if appropriate. Consumers and other parties can report security incidents using the Kahootz support desk or by telephone.

Security incidents are regarded as a Priority 1 request and will be acknowledged within 1 hour and we aim to mitigate any security problem within 4 hours.

5.5.2 Configuration and Change Management

Our ISO27001 compliance requires that we have a documented process for configuration and change management.

All major changes are well-documented, risk-assessed and managed from inception to completion.

5.6 Personnel Security

All Kahootz staff are security screened to the BS7858 standard.

This is a detailed background check that includes:

- **5-year employment verification**
- **Criminality Check**
- **ID Verification**
- **Right to Work Assistance**
- **Character reference checks**
- **6 Year Credit Search, County Court Judgment Search, Insolvency Search, Bankruptcy Search, Voters' Roll Check, Aliases Check**

Access to consumer data by Kahootz staff is only provided to key support personnel on a need-to-know basis and all such access is audited.

Within our ISO27001 procedures, all new staff are trained in security, and all staff are given regular refresher training.

5.7 Secure Development

The Kahootz software is designed and developed in line with software industry best practice.

Each software release is comprehensively tested using a mixture of automated and manual tests until it meets our standards.

New and evolving threats are regularly reviewed and appropriate actions taken.

Configuration management is used to ensure the integrity of the service through development, testing and deployment.

5.8 Supply Chain Security

We have a detailed set of IS27001 procedures to ensure that our supply chain is secure and well-managed. These include:

- **A comprehensive appraisal of potential suppliers to ensure they can meet oursecurity requirements.**
- **A regular review of key suppliers to monitor service levels and ensure that security procedures are being followed.**
- **A contractual requirement on suppliers to follow security procedures.**

Where possible, we choose suppliers that are themselves ISO27001 and independently security accredited.

The data centre staff do not have any access whatsoever to the service or the data it contains.

In addition to our hosting partner, Kahootz uses the following software services:

- **DeskPro – Helpdesk and knowledgebase SaaS (manned by Kahootz staff)**
- **Pingdom – Server monitoring SaaS**

5.9 Secure Consumer Management

The management interface to Kahootz is only available to authorised Site Administrators.

Site Administrators can only view information and perform actions that affect their own service. The permissions provided to each Site Administrator are configurable. Users cannot elevate their own permissions.

The Kahootz support staff are only permitted to update a consumer's service – such as changing user permissions or providing access to data - when the support request is from an authenticated and authorized Site Administrator.

5.10 Identity and Authentication

5.10.1 User Authentication

Each user has a unique username and password that must be entered each time they log on.

Passwords are totally under user control and are never sent by email. Passwords are stored in the database using one-way encryption so it is not possible to read a user's password – even for Kahootz administrators.

The service allows users to reset their own password using a secure-token 'forgot password' facility.

To manage user sessions, Kahootz uses a secure cookie – which does not contain the user's username or password.

5.10.2 Two-Step Verification

For added security, Kahootz Enterprise clients can optionally enable two-step verification.

This strengthens the login process by requiring users to enter a numeric code that's sent to a pre-authenticated phone number whenever they log in.

Two-factor security can be enabled for all users, or just a subset of users that have greater permissions.

Site Owners can also enable two-step verification that uses phone-based Authenticator Apps for all the users on their site.

5.11 External Interface Protection

Kahootz conducts an annual CHECK IT test to ensure that all interfaces to the service are secure.

5.12 Secure Service Administration

The service is managed by Kahootz staff using a secure HTTPS connection, secure telnet and secure FTP.

All Administrative access to the servers is audited.

5.13 Audit information provision to consumers

Audit information is available to Site Owners within the Kahootz service.

Audit information is available to Site Administrators within the Kahootz Admin Application.

5.14 Secure use of the Service by the Consumer

The Kahootz service is available from any Internet connected device. Users are authenticated by username and password.

Kahootz enforces password complexity rules to ensure that users choose strong passwords and displays a ‘password strength’ indicator wherever users set or change their password.

Kahootz Enterprise clients can optionally enable two-step authentication and control their own policy for:

- Minimum password length and complexity
- Maximum and minimum password age
- Prevention of password re-use
- Lockout after incorrect logon attempts
- Automatic logout on inactivity

It is the consumer’s responsibility to ensure that their users follow good security practices such as:

- Devices should be free from spyware and viruses
- Devices should automatically lock on inactivity
- Users do not write down or disclose passwords to others

Kahootz consultants are available to provide training on the use of the service, the Admin Application and good security practices.

For more information with regard to how we protect your information please contact:

Kahootz
Weston Farm Barn
Newbury Road
Weston
RG20 8JA
info@kahootz.com