

KitTick

Service Definition Document

Equipment Management, Compliance & Governance Solution

G-Cloud Framework

Contents

1. Service Overview
2. Service Features
3. Service Benefits
4. System Requirements
5. Service Constraints
6. Service Levels
7. Support
8. Onboarding and Training
9. Customisation
10. Data Backup and Disaster Recovery
11. Security
12. Hosting and Data Location
13. Contract Terms
14. End of Contract

1. Service Overview

KitTick is a mobile application for equipment management, compliance, and governance. It enables organisations to assign kit to personnel, enforce role-based requirements, and schedule mandatory checks. Real-time compliance monitoring, automated flagging, and comprehensive audit trails ensure accountability, regulatory adherence, and operational readiness across the entire workforce.

The solution comprises a mobile application for iOS and Android devices used by frontline staff, and a web-based administration dashboard for managers and administrators. Both interfaces synchronise in real-time, ensuring data consistency across all access points.

Target Users

KitTick is designed for public sector organisations and other entities requiring robust equipment compliance and governance. The system is particularly suited to organisations with large workforces where equipment compliance is critical to operational effectiveness and regulatory requirements.

2. Service Features

Feature	Description
Real-time compliance monitoring	Instant visibility of equipment compliance across all personnel.
Role-based kit requirements	Enforce mandatory equipment assignments automatically by job role.
Scheduled equipment checks	Automated reminders for mandatory inspection intervals.
Mobile-first remote access	Full functionality via iOS and Android apps.
Comprehensive audit trails	Complete history of all assignments and actions logged.
Push notification alerts	Instant alerts for compliance issues and overdue checks.
Multi-tenant architecture	Secure data separation for multiple organisations.
Custom metadata fields	Configure organisation-specific data capture fields.
Automated compliance flagging	Alerts when personnel lack required kit items.
Asset issue reporting	Staff report equipment problems with real-time escalation.

3. Service Benefits

Benefit	Description
Maintain regulatory compliance	Ensure personnel always have required role equipment.
Reduce administrative burden	Automate checks and eliminate manual tracking.
Manage equipment on the move	Complete kit checks from any location.
Identify compliance gaps instantly	View real-time dashboards showing outstanding requirements.
Demonstrate governance accountability	Produce audit-ready compliance reports anytime.
Respond quickly to issues	Receive instant alerts when problems reported.
Enforce consistent standards	Apply uniform kit requirements automatically.
Reduce equipment failures	Proactive checks identify issues before impact.
Empower frontline staff	Personnel manage kit and report issues directly.
Scale effortlessly	Onboard new teams without additional infrastructure.

4. System Requirements

KitTick requires an active internet connection for full functionality. The mobile application needs connectivity to synchronise data in real-time, ensuring compliance status and equipment assignments are always current across the organisation.

Mobile Application

- iOS 13 or later
- Android 10 or later
- Active internet connection
- Device notification permissions for real-time alerts
- Camera access for asset barcode scanning

Web Dashboard

- Google Chrome, Microsoft Edge, Apple Safari, or Mozilla Firefox (latest versions recommended)
- Active internet connection
- PDF reader for exported compliance reports

Optional Requirements

- Valid email addresses for user account activation
- Compatible SAML 2.0 provider for single sign-on integration
- HTTPS connectivity for third-party API integrations

5. Service Constraints

- Internet connectivity required for real-time synchronisation
- Supported on iOS 13+ and Android 10+ devices only
- Web dashboard optimised for Chrome, Edge, Safari, and Firefox
- Scheduled maintenance windows occur monthly with advance notification
- Data hosted on UK-based servers only
- Pricing based on active user count per organisation
- API integrations require technical implementation by buyer
- Single sign-on requires compatible identity provider
- Administrator training recommended for optimal configuration
- Bespoke development requests subject to separate agreement

6. Service Levels

Availability

KitTick guarantees 99.9% service availability, measured monthly excluding scheduled maintenance windows. Scheduled maintenance is performed during low-usage periods with a minimum of 48 hours advance notification to customers.

Service Level Agreement

Our SLA defines availability as the ability for authenticated users to access core platform functionality including the mobile app and web dashboard. Availability is monitored continuously and measured as a percentage of total minutes in each calendar month.

Service Credits

If availability falls below guaranteed levels, customers are entitled to service credits applied to future invoices:

Availability	Service Credit
99.0% - 99.9%	10% of monthly fee
95.0% - 99.0%	25% of monthly fee
Below 95.0%	50% of monthly fee

Customers must submit credit requests within 30 days of the affected month. Credits are capped at 50% of the monthly subscription fee and do not apply where unavailability results from factors outside our control, scheduled maintenance, or customer-side connectivity issues.

7. Support

Standard Support (Included)

Standard support is included with all KitTick subscriptions at no additional cost. This provides email and web-based support seven days a week, including bank holidays. Response times are within 12 hours for all enquiries. Standard support includes access to our online knowledge base, user documentation, and video tutorials.

Enhanced Support (Additional Cost)

Enhanced support is available for organisations requiring telephone assistance. This tier includes telephone support during UK business hours (Monday to Friday, 9am to 5pm) in addition to standard email and web-based support. Enhanced support also includes priority handling for critical issues affecting service availability, onboarding assistance for new administrators, and configuration guidance during initial setup. Enhanced support is priced at 15% of the annual subscription value.

Reporting Outages

Customers are notified of any service outages via email. Alerts are sent to designated administrators when incidents are identified, with follow-up notifications providing status updates and resolution confirmation. Planned maintenance windows are communicated via email a minimum of 48 hours in advance. During outages, we provide regular updates until the issue is resolved.

8. Onboarding and Training

Onboarding Process

We provide a structured onboarding process to ensure organisations are operational quickly. Upon subscription, customers receive a dedicated onboarding session via video call to configure their tenant, establish department structures, and define initial kit requirements. This guided setup typically takes one to two hours depending on organisational complexity. Onsite setup is also available upon request for organisations preferring face-to-face implementation support.

Training

Online training is provided for administrators and end users. Administrator training covers system configuration, user management, compliance reporting, and ongoing maintenance. End user training focuses on the mobile app, completing checks, and reporting issues. Training is delivered via live video sessions and recorded tutorials accessible on demand. Onsite training is available upon request at additional cost.

Documentation

Comprehensive user documentation is available through our online knowledge base. This includes step-by-step setup guides, video tutorials, frequently asked questions, and best practice recommendations. Documentation is maintained and updated with each release. Administrator guides and end user quick-start guides are available as downloadable PDFs.

9. Customisation

What Can Be Customised

KitTick offers extensive customisation to meet organisational requirements. Organisations can define their own department and location structures, create custom roles with specific kit requirements, and configure mandatory check schedules per equipment type. Custom metadata fields allow organisations to capture additional data specific to their needs, such as serial numbers, warranty dates, or certification references. Compliance thresholds, notification preferences, and reporting parameters can all be tailored. Branding elements including organisation logo and name are displayed throughout the interface.

How Users Customise

All customisation is performed through the web-based administration dashboard. Administrators use intuitive forms and configuration screens to define structures, set requirements, and adjust settings. Changes take effect immediately and synchronise to all users in real-time. Bulk import functionality is available for organisations needing to configure large volumes of users, equipment, or locations during initial setup.

Who Can Customise

Customisation access is controlled through role-based permissions. Organisation administrators have full access to all configuration options. Managers can be granted limited customisation rights, such as managing their department's users or equipment. Standard users cannot access configuration settings, ensuring system integrity and governance controls are maintained.

10. Data Backup and Disaster Recovery

Backup Strategy

KitTick implements a comprehensive backup strategy aligned with public sector best practices. Automated backups are performed every 4 hours, with full daily backups retained for 30 days. Weekly backups are retained for 12 months to support compliance and audit requirements. All backups are encrypted at rest and stored in geographically separate AWS availability zones within the UK.

Recovery Objectives

Metric	Target
Recovery Time Objective (RTO)	4 hours
Recovery Point Objective (RPO)	4 hours

Infrastructure Resilience

KitTick is hosted on AWS infrastructure, leveraging multiple availability zones within a UK region. This ensures continued service operation if an individual datacentre experiences failure. Data is automatically replicated across availability zones, providing redundancy and rapid failover capability. Database replication ensures data durability and enables quick restoration in the event of failure.

Application Resilience

The application layer uses load balancing to distribute traffic across multiple servers. Auto-scaling provisions additional capacity during demand spikes. Health monitoring automatically removes unhealthy instances and replaces them without manual intervention.

Disaster Recovery

A documented disaster recovery plan is maintained and tested annually. The plan covers scenarios including datacentre failure, data corruption, and security incidents. Full details of our disaster recovery approach are available on request.

11. Security

Certifications and Standards

KitTick is Cyber Essentials certified, demonstrating our commitment to cybersecurity best practices. Our hosting infrastructure on AWS benefits from extensive security certifications including SOC 1/2/3 (SSAE-18), ISO 27001, ISO 27017, ISO 27018, and CSA CCM. AWS holds UK government certifications and is listed on the G-Cloud framework. Our security approach aligns with the ISO 27001 framework and NCSC guidance.

Data Protection in Transit

All data transmitted between users and KitTick is encrypted using TLS 1.2 or higher. Internal communications between servers, databases, and services are also encrypted using TLS 1.2 or higher, protecting data in transit even within the network boundary.

Data Protection at Rest

Data at rest is protected through encryption of all physical media. AWS datacentres comply with SSAE-18 for physical access control, and AWS provides encryption at rest for all storage services. This combination ensures data is protected both physically and cryptographically.

Access Controls

Access to management interfaces is restricted through role-based access controls. Only authorised administrators can access system configuration and user management. Administrative access to the web dashboard requires Multi-Factor Authentication (MFA). All actions are logged for audit purposes. Access controls are tested at least annually.

Penetration Testing

Penetration testing is conducted at least annually by a CREST-approved service provider, ensuring independent validation of our security posture.

Vulnerability Management

We conduct regular vulnerability assessments using automated scanning tools. Critical security patches are deployed within 24 hours of release. High-severity patches are deployed within 7 days. We monitor NCSC advisories, AWS security bulletins, CVE databases, and vendor security notifications for emerging threats.

Incident Management

We maintain documented incident management procedures for common events including service outages, security breaches, and data incidents. Critical security incidents are responded to within one hour. Customers receive incident reports detailing timeline, root cause, impact, and corrective actions within 5 working days of resolution.

12. Hosting and Data Location

KitTick is hosted on Amazon Web Services (AWS) infrastructure within UK datacentres. All customer data is stored and processed within the United Kingdom and is not transferred outside UK jurisdiction.

AWS datacentres comply with multiple recognised standards including SOC 1/2/3 (SSAE-18), ISO 27001, ISO 27017, ISO 27018, and CSA CCM. Physical security controls include 24/7 monitoring, biometric access controls, and comprehensive environmental protections.

Multi-Tenant Architecture

KitTick uses a multi-tenant architecture with complete data separation between organisations. Each tenant's data is logically isolated, ensuring no organisation can access another's information. Load balancing distributes traffic across multiple servers, preventing any single organisation's usage from impacting others. API rate limits are applied per organisation to ensure fair access and consistent performance for all customers.

13. Contract Terms

Contract Duration

The minimum contract term is 12 months. Contracts automatically renew unless terminated with at least 1 month's written notice prior to the renewal date.

What is Included

The contract price includes:

- Full platform access for the agreed number of users
- Standard support with 12-hour response times
- Access to all standard features and updates released during the contract period
- Online training materials and documentation
- Initial onboarding session
- Data export at contract end

Additional Costs

Additional costs may apply for:

- Enhanced telephone support
- Onsite setup or training
- User numbers exceeding the contracted amount
- Bespoke development or customisation requests
- Optional integrations requiring dedicated implementation support

14. End of Contract

End of Contract Process

Prior to contract end, we provide written notification and offer the opportunity to renew. During the notice period, administrators retain full access to export all organisational data through the web dashboard or API. Our support team is available to assist with data extraction requirements at no additional cost.

Upon contract termination, user access to the mobile app and web dashboard is disabled. Data is retained securely for 30 days following termination to allow for any final extraction requests. After this retention period, all customer data is permanently and securely deleted from our systems. Written confirmation of data deletion is provided upon request.

Data Export

Administrators can export data directly through the web dashboard at any time during the contract. Built-in export functionality allows download of users, equipment, assignments, compliance histories, and audit trails in CSV and PDF formats. Customers with API access can extract data programmatically using standard endpoints. At contract end, our support team can provide a complete data package upon request at no additional cost. All exports use non-proprietary formats ensuring data remains accessible regardless of future system choices.

Data Sanitisation

Following the data retention period, all customer data is permanently erased. AWS uses cryptographic erasure for encrypted storage, meaning deletion of encryption keys renders data unrecoverable. At the application level, KitTick performs data erasure by permanently deleting all customer records from databases.