

G-Cloud Service Definition – Omnitrack

Service Overview

Service name: Omnitrack

Supplier: VinciWorks

Service type: Cloud-based compliance workflow and data management platform

Omnitrack is a configurable compliance workflow system that enables organisations to collect, manage, and report on compliance-related data. It supports structured data collection via custom forms, automated approval workflows, risk flagging, dashboards, and full audit trails. The service is designed to streamline due diligence, enforce best practice, and evidence regulatory compliance.

Omnitrack can be used as a standalone platform or integrated with VinciWorks' e-learning services to capture and manage compliance data generated during training and assessments.

Service Features and Benefits

Features:

- Custom form creation and data capture
- Automated workflows and approvals
- Risk flagging and escalation
- Reminder and notification emails
- Real-time dashboards and reports
- API access for integrations
- Full audit logging

Benefits:

- Reduced compliance risk
- Improved operational efficiency
- Clear audit evidence
- Standardised processes
- Improved collaboration across teams

Service Scope

Omnitrack supports compliance, operational risk, policy tracking, case management, and regulatory workflows across public and private sector organisations. It is suitable for use in healthcare, education, social care, public safety, and general regulatory compliance environments.

Onboarding and Offboarding

Onboarding:

Implementation typically takes 6–8 weeks and includes:

- Requirements gathering and workflow mapping
- Configuration of forms and workflows
- Automation and notification setup
- Integration configuration (if required)
- User Acceptance Testing (UAT)
- Production deployment

Offboarding:

Customers can export all data in CSV format directly from the system or request assistance from support. After contractual retention periods, data is securely erased using recognised data sanitisation methods.

Service Constraints

The service is delivered as a shared cloud platform. Planned maintenance is scheduled outside peak hours where possible, with advance notification to customers.

Service Levels

Availability: >99.9% uptime

Support hours:

- Email/ticket support: monitored continuously, same-day response during business hours
- Phone support: Monday to Friday, 9am–5pm (UK time)

Performance is maintained through isolated, auto-scaling infrastructure and per-tenant limits to prevent one customer's usage impacting others.

After-Sales Support

Support includes technical assistance, configuration guidance, API support, and best practice advice. Support is included in the service cost and available via ticketing, email, and phone.

Technical Requirements

End users require an internet connection and a modern web browser. No software installation is required. The service is fully responsive and usable on mobile devices.

API access is available using REST endpoints with OpenAPI (Swagger) documentation and a sandbox environment.

Outage and Maintenance Management

Continuous monitoring and automated alerts detect service issues. Users can report incidents via support tickets or email. Email alerts are issued for significant outages. Post-incident reports are provided for major incidents, including root cause and remediation.

Hosting and Data Locations

The service is hosted in secure third-party data centres located in the UK and EEA. Public and private cloud deployment options are available by arrangement. Data remains within approved jurisdictions.

Data Backup, Restore and Disaster Recovery

Data is backed up as part of the managed cloud infrastructure. Backups support recovery from data corruption or system failure. Disaster recovery and business continuity arrangements are in place and aligned with industry standards. Resilient architecture ensures continued service during component failures.

Access to Data Upon Exit

Customers can export their data at any time during the contract and at exit. Data is provided in CSV format. Support can assist with large or complex exports. After exit and agreed retention periods, data is securely erased.

Security

Security governance is aligned to ISO/IEC 27001 with board-level accountability. The service uses role-based access control, least privilege principles, and multi-factor authentication. Identity federation is supported.

All access to management and support systems is restricted to authorised staff, logged, and regularly reviewed. Logs and audit trails are retained for at least 12 months and are accessible to customers.

Data is encrypted in transit using TLS 1.2+ and protected at rest. Annual penetration testing is conducted by approved providers. Continuous vulnerability scanning and monitoring are in place. Staff undergo background screening to recognised standards, with government clearance available where required.