



Ideagen Incident Compliance

Service Definition Document

G-Cloud 15

Lot 2b Software as a Service (SaaS)

Table of Contents

Company Overview.....	4
Service Overview	4
Overview of the Service	4
Features and Benefits	5
Technical Requirements	7
Hosting Options and Locations	7
Data Back-Up and Restoration.....	8
Security	8
Information Assurance	8
Privacy by Design	9
Development Life Cycle	9
Buyer Responsibilities.....	10
Onboarding and Offboarding.....	11
Project Management Services.....	11
Service Constraints	15
Outage and Maintenance Management	16
Service Levels	17
After Sales Support	17
Access to Data (upon exit).....	18

Contact Details.....	18
-----------------------------	-----------

Company Overview

Ideagen brings clarity and confidence to those businesses that put resilience at the heart of their operations.

Trusted by over 18,000 organisations worldwide – including over 1000 government agencies, more than 2000 hospitals and healthcare settings, as well as education, blue light services, life science and not-for-profit – our AI enabled solutions are proven to keep people, products and processes safe, increase efficiencies and streamline operations.

By unifying decades of deep regulatory expertise and innovation with affordable, best-in-class software we provide trusted, meaningful intelligence to support regulated and high-compliance industries with their audit, risk, health and safety, quality and compliance needs.

We are committed to continually improving the quality of our solutions, the environmental impact of our operations, and the security of the information that we safeguard. This commitment is demonstrated by our company certifications to ISO 9001, ISO 14001, ISO 27001 and ISO 45001. Ideagen also follows the guidance provided by ISO 26000.

Service Overview

Overview of the Service

Ideagen Incident Compliance is a comprehensive, cloud-based Software as a Service solution built natively on Microsoft 365 and SharePoint. The platform enables organizations to efficiently capture, track, investigate, and resolve incidents, accidents, near-misses, and safety observations across their enterprise.

Designed specifically for highly regulated industries including healthcare, financial services, insurance, pharmaceuticals, energy, and manufacturing, Ideagen

Incident Compliance provides a centralized system of record for all incident-related activities while ensuring regulatory compliance, audit readiness, and continuous improvement of safety and risk management practices.

The solution leverages the familiar Microsoft 365 interface, ensuring rapid user adoption while providing enterprise-grade security, scalability, and integration capabilities. All data is hosted within Microsoft Azure UK regions (UK South and UK West), ensuring full UK data residency compliance.

Features and Benefits

Ideagen Incident Compliance delivers comprehensive functionality for end-to-end incident lifecycle management:

Incident Capture and Classification

- Multi-channel incident reporting including web forms, mobile access, anonymous reporting, and email submission
- Configurable incident types: accidents, near-misses, safety observations, security incidents, data breaches, quality issues, environmental incidents
- Automated incident categorization and severity scoring based on configurable business rules
- Location-based incident tracking with organizational hierarchy mapping
- Witness statement capture and attachment management

Investigation Management

- Structured investigation workflows with role-based assignments
- Root cause analysis tools including 5 Whys, fishbone diagrams, and fault tree analysis
- Evidence collection and documentation with secure audit trail
- Interview management and witness statement recording
- Timeline reconstruction and incident sequence mapping

Corrective and Preventive Actions (CAPA)

- Automated CAPA generation from investigation findings
- Action assignment with responsibility tracking and escalation workflows
- Progress monitoring with automated reminders and overdue notifications
- Effectiveness verification and validation processes
- Integration with existing action management systems

Reporting and Analytics

- Real-time executive dashboards with configurable KPIs and metrics
- Trend analysis across incident types, locations, departments, and time periods
- Regulatory reporting templates (RIDDOR, HSE, FDA, EMA compliance)
- Power BI integration for advanced analytics and data visualization
- Automated report scheduling and distribution

Workflow and Compliance

- Configurable approval workflows aligned to organizational policies
- Automated regulatory notification triggers based on incident severity
- SLA management with configurable time-based escalations
- Complete audit trail with immutable logging of all activities
- Electronic signatures for investigation closure and approvals

Integration Capabilities

- Native Microsoft 365 integration (Teams, Outlook, SharePoint, Power Platform)
- Single sign-on via Azure Active Directory with MFA support
- REST API for integration with HRIS, ERP, and other enterprise systems
- Microsoft Graph API utilization for enhanced collaboration
- Power Automate connectors for process automation

Technical Requirements

Ideagen Incident Compliance operates as a native Microsoft 365 SharePoint application and requires:

- Microsoft 365 subscription (E3, E5, or Business Premium)
- SharePoint Online environment
- Azure Active Directory for user authentication
- Modern web browsers: Microsoft Edge, Chrome, Firefox, or Safari (latest 2 versions)
- Internet connectivity with access to Microsoft 365 services
- No additional hardware or server infrastructure required

Hosting Options and Locations

Ideagen Incident Compliance is hosted on Microsoft Azure cloud infrastructure within UK data centres to ensure compliance with UK data residency requirements.

UK Data Residency

All customer data is hosted exclusively within the United Kingdom to ensure full compliance with UK data protection and residency requirements. Ideagen Incident Compliance leverages Microsoft Azure UK datacentres:

- Primary Region: Microsoft Azure UK South (London)
- Secondary Region: Microsoft Azure UK West (Cardiff)
- Data never leaves UK sovereign territory
- Geo-redundant storage within UK regions for high availability
- Compliant with UK GDPR and Data Protection Act 2018

Infrastructure and Architecture

The service operates on Microsoft's enterprise-grade cloud infrastructure with:

- Multi-tenant architecture with logical data segregation
- Automatic scaling to meet demand
- Load balancing across availability zones
- Redundant power, cooling, and network connectivity
- 24/7 monitoring and infrastructure management

Data Back-Up and Restoration

Backups are configured through Microsoft Azure managed services to support our Recovery Time Objective (RTO) and Recovery Point Objective (RPO) requirements. Backups are stored redundantly across multiple facilities within the UK.

There is a documented Business Continuity and Disaster Recovery (BCDR) Plan for the solution which is tested at least annually. Findings from BCDR testing are tracked to ensure continuous improvement of the recovery procedures.

Security

Information Assurance

Ideagen maintains a suite of Corporate Security Policies cover the management of security for both its internal operations as well as the services Ideagen provides to its customers, and applicable to all Ideagen employees as well as any relevant third parties and stakeholders. These policies, which are aligned with the ISO/IEC 27001:2022 standard to which Ideagen is externally certified, govern all areas of security applicable to the services. All policies are formally reviewed and signed off by management at least annually or on significant change, in line with our ISO 27001 Certification.

Additionally, Ideagen is certified under both Cyber Essentials and Cyber Essentials Plus. A comprehensive overview of Ideagen policies, standards, and procedures, can be supplied upon request.

The information security of the business is currently overseen by our VP Global Cyber Security, who works closely with our IT Teams, our Product Managers and our Group DPO to ensure that all Technical and Organisational Measures are in place and maintained. Ideagen utilises the Microsoft Azure, M365 product suite and AWS cloud services and therefore has the benefit of the Microsoft and Amazon infrastructure and controls.

Privacy by Design

Ideagen has embedded privacy by design principles throughout its product and development lifecycle, prioritising the protection of User data throughout all processing activities. The service implements core privacy principles including data minimization, purpose limitation, and privacy by default, ensuring Users benefit from the highest privacy settings without additional configuration.

The service employs strong encryption and granular access controls to ensure Buyer Data remains secure. Privacy safeguards are integrated from initial design through to data deletion, with regular privacy reviews conducted as features evolve.

Ideagen has appointed a qualified and certified Data Protection Officer who oversees data protection compliance across the organisation and is registered with the Information Commissioner's Office in the UK.

Full details are available in [Data Protection Policy | Safeguarding your privacy](#)

Development Life Cycle

Ideagen delivers its software through agile methodologies and has adopted the core principles of the Scrum framework, as defined in the Scrum Guide at [Scrum.org](https://www.scrum.org), to achieve this.

Ideagen developers follow OWASP guidelines. There are Lead Developers who ensure that our development processes are followed, such as peer reviews, testing against the OWASP top 10, etc.

The Cyber Security Unit (CSU) actively undertake regular penetration testing and vulnerability scans to discover any potential vulnerabilities within Ideagen software.

Our Software Development Lifecycle (SDLC) Document forms part of our ISO 27001 and ISO 9001 Frameworks and is reviewed by the Document Owner and our Risk & Audit Team at least annually or on event of a change.

Buyer Responsibilities

Working Together for Success

To ensure you get the most from our Services, we'll need you to designate a primary contact person before we begin. This person will be our go-to for important updates like maintenance notifications and service requests, and should have the authority to handle matters such as data releases, restorations, and configuration changes. Just share their name and email address with us, and we'll make sure they stay informed on everything that matters.

Your Role in Managing the Solution

To help you maintain control and get the best results from our Software and Services, you'll take care of:

- Managing user security and permissions within the Software
- Setting up and maintaining your user desktops and network access
- Implementing, testing, and configuring your database as your needs evolve
- Providing us with accurate information as outlined in our guidance
- Keeping us updated on any operational changes that might affect the Services
- Creating and configuring user accounts

- Meeting your obligations on time and in line with applicable laws

Access and Collaboration

To deliver great service, we may occasionally need access to your equipment, information, data, personnel, or systems. We'll always keep our requests reasonable and work around your schedule. If our Team visits your premises, we ask that you help us maintain a safe and secure working environment, we'll do the same if you visit us!

Onboarding and Offboarding

Project Management Services

45-Day Onboarding Process

Ideagen Incident Compliance is delivered through a structured 45-day implementation programme (9-10 weeks) designed to ensure successful deployment, user adoption, and operational readiness. The programme follows a proven five-phase methodology:

Phase 1: Project Introduction and Planning (Week 1)

- Project kick-off meeting with all key stakeholders
- Introduction to the team and escalation procedures
- Review of project scope, timelines, and success criteria
- Requirements gathering and workflow design workshops
- Configuration planning for incident types, classifications, and approval workflows
- User role definition and access control planning

Deliverables: Project plan, configuration specification, stakeholder communication plan

Phase 2: System Deployment and Configuration (Weeks 2-3)

- SharePoint site collection provisioning within customer's Microsoft 365 tenant
- Azure Active Directory integration and SSO configuration
- Custom incident forms and workflow configuration
- Dashboard and reporting template setup
- Email notification configuration and testing
- User acceptance testing environment preparation

Deliverables: Configured incident management system, UAT environment access

Phase 3: Super User Training (Week 4)

- Administrator training (4 hours): System configuration, user management, workflow design
- Super user training (3 hours): Incident reporting, investigation management, CAPA workflows
- Power user training (2 hours): Advanced reporting, analytics, and integration features
- Hands-on configuration exercises and Q&A sessions
- Train-the-trainer materials and knowledge transfer

Deliverables: Training materials, recorded sessions, super user certification

Phase 4: End User Training and Go Live Preparation (Week 8)

- End user training sessions (1.5 hours per session): Basic incident reporting and tracking
- Investigator training (2 hours): Investigation workflows, root cause analysis, CAPA management
- Manager training (2 hours): Approvals, oversight, reporting, and analytics
- Go Live readiness assessment and final configuration review
- Communication plan execution for organization-wide rollout

Deliverables: Training completion certificates, Go Live checklist, user quick reference guides

Phase 5: Go Live and Post-Implementation Support (Weeks 9-10)

- Production Go Live with enhanced support coverage
- Hypercare support period (first 2 weeks post-Go Live)
- Daily check-in calls during first week of operation
- Issue resolution and optimization adjustments
- Project wrap-up meeting and lessons learned review
- 60-day follow-up meeting: Success metrics review, optimization recommendations, ongoing support transition

Deliverables: Go Live report, hypercare summary, 60-day health check report

Implementation Success Metrics

The implementation is considered successful when the following criteria are met:

- All planned system configurations completed and tested
- Minimum 250 historical incidents successfully migrated with data integrity verification
- All identified super users and administrators trained and certified
- 80% of end users completed training sessions
- User acceptance testing sign-off received from business stakeholders
- All critical and high-priority issues resolved prior to Go Live
- Communication and change management plan successfully executed

Offboarding and Data Portability

Service Exit Procedures

Ideagen provides comprehensive offboarding procedures to ensure smooth service transitions with complete data portability. Upon service termination, the following exit procedures are executed:

Notice Period and Planning (30 Days Prior to Termination)

- Customer provides written notice of intent to terminate service
- Offboarding project plan developed with key milestones and responsibilities
- Data export format and scope confirmed with customer requirements
- Transition support requirements identified and scheduled

Data Export and Validation (Final 30 Days)

- Complete data extraction in customer-specified formats
- Data integrity verification and quality assurance checks
- Secure transfer of data extracts to customer-designated location
- Export documentation including data schemas, relationships, and metadata

Data Formats and Deliverables

All customer data is provided in open, industry-standard formats:

- Incident Records: CSV, Excel (XLSX), or SQL database dump format
- Attachments and Evidence: Original file formats within organized folder structure
- User and Metadata: JSON or XML format with complete schemas
- Audit Logs: CSV format with complete timestamp and user activity records
- Reports and Dashboards: PDF exports of all custom reports
- Configuration Settings: JSON export of all system configurations and workflows

Knowledge Transfer and Support

- Documentation of all custom configurations and integrations
- Up to 10 hours of consulting support for data interpretation and migration assistance
- Answers to technical questions about exported data structures
- Verification support to ensure data completeness and accuracy

Data Retention and Secure Deletion

Post-Termination Data Handling: 30-day retention period following service termination during which customer data remains accessible for final export verification

Secure Data Deletion: After the 30-day retention period, all customer data is permanently deleted using secure deletion methods aligned to ISO 27001 standards. Confirmation of data deletion is provided in writing upon request.

Backup Deletion: All backup copies are identified and securely deleted within 60 days of service termination

Transition Assistance

Ideagen Incident Compliance provides reasonable assistance to facilitate smooth transition to alternative systems:

- Consultation on data migration strategies for common target platforms
- Technical documentation explaining data structures and relationships
- API access during transition period for automated data extraction (if required)
- Recommendations for data validation and quality assurance post-migration
- Optional professional services for accelerated migration (available at additional cost)

Service Constraints

Maintenance Windows

Scheduled maintenance is performed during defined windows to minimise business impact:

- Standard Maintenance Window: Sundays 02:00–06:00 GMT
- Frequency: Monthly for routine updates

- Notification: 5 business days advance notice via email
- Emergency Maintenance: May occur outside window for critical security patches
- Expected Impact: Service unavailable during maintenance; average duration 2 hours

Customisation Limitations

As a SaaS platform, Ideagen Incident Compliance operates within defined customisation boundaries:

- Configurable disclosure forms and workflows within standard framework
- Custom fields and dropdown values supported
- Branding customisation (logos, colours) available
- Source code modifications not permitted
- Extensive customisation may require professional services engagement

Outage and Maintenance Management

Ideagen is notified of vulnerabilities through our own internal testing along with independent external assessments and system patch monitoring. Each vulnerability is reviewed to determine if it is applicable to Ideagen's hosting environment and its potential impact. If a zero-day vulnerability is discovered, we will assess its impact to the system and if required patch at the earliest opportunity.

Backups are configured through Microsoft Azure managed services to support our Recovery Time Objective (RTO) and Recovery Point Objective (RPO) requirements. Backups are stored redundantly across multiple facilities within the UK.

All products are monitored using a managed SIEM/UEBA parsing. If any thresholds are met, alerts are presented via our ticketing system to our Cloud and Cyber Operations Team with automatic escalation procedures. Ideagen operate a

formal Incident Management Policy and confidential processes that form part of our ISO 27001:2022 programme and as such is reviewed and externally audited at least annually. This area is further evidenced through the Ideagen ISO 27001:2022 Certificate and the Statement of Applicability.

Service Levels

We will be available for support through our online support portal, email or phone for the term of this Agreement, Monday through Friday, please refer to the SLA available at: [Ideagen Support Service Level Agreement \(SLA\) – Help | Ideagen Luminare](#)

In the event there are errors with the Software, the Company will endeavour to solve the issue within 72 hours of receipt of the problem. However, the Client acknowledges that some issues may require longer to resolve.

Ideagen offer three levels of Customer Success Plans which can be purchased offering three levels of support; Premier, Standard and Essential, full information can be found at: [Plan comparisons – Ideagen Customer Excellence \(Standard\)](#)

After Sales Support

You will be assigned a designated Account Manager who will be the primary contact point for any questions post implementation. The Premier Success Plan also provides access to an in-region Buyer Success Manager as well as a dedicated phone number for directly contacting the Support Team.

The Account Manager / CSM will actively seek to contact you to establish monthly and quarterly reviews at a mutually convenient time to ensure that you are maintaining value from your solution, and happy with the service provided by Ideagen.

For all service level information, please refer to: [Ideagen Support Service Level Agreement \(SLA\) – Help | Ideagen Luminare](#)

Access to Data (upon exit)

We want to make sure you have everything you need when our Contract comes to an end. Please remember to download and save any of your data from the Software before the termination date, this is important because your data will be permanently deleted from our systems after that point.

Once the Contract ends, and unless otherwise agreed, we won't be able to maintain your data or other information you've submitted, and we'll proceed with deleting all copies from our systems (unless we're required by law to keep them).

If you'd like our assistance extracting your data from the Software, just let us know at least 30 days before your termination date, we'll do our best to help. Please note that any assistance we provide will be subject to our standard professional services rates to cover our time and costs.

Contact Details

Please email g-cloud@ideagen.com with a brief description of your requirements and include the following contact details:

- Name
- Role
- Contact e-mail
- Telephone number
- The solution you are interested in

Ideagen will pass your enquiry to the most appropriate Team Member who will contact you to contact you to gather any additional information.