

Phew Audit System - Service Definition (G-Cloud 15)

Audit System Service Specification

Product: Phew! Audit System (Standard and Advanced configurations)

Provider: Phew Design Limited

1. Service Overview

The Phew! Audit System is a cloud-based platform designed specifically for safeguarding professionals to efficiently create, manage, and analyze safeguarding audits and chronologies.

Available in two configurations:

- **Standard Audit System:** For organisation-based audits with standard security requirements
- **Advanced Audit System:** For audits involving sensitive personal data requiring enhanced security measures

1.1 Key Benefits

- **Efficiency:** Reduces audit completion time from 30+ hours to approximately 30 minutes
- **Consistency:** Standardised framework ensures thoroughness across all audits
- **Collaboration:** Multiple users can work on audits simultaneously with role-based permissions
- **Compliance:** Built-in data protection and security controls
- **Insight:** Analytics and reporting tools identify trends and inform strategic decisions

2. Core Features

2.1 Audit Creation and Management

- Create multiple audit types (thematic, self-assessment, and others depending on configuration)
- Template-based audit frameworks with customisable questions
- Multi-agency audit support with controlled partner access
- Document upload and attachment management
- Live audit tracking showing progress on ratings, action plans, and evidence
- Copy answers from previous audits to speed up completion
- Progress tracking and status monitoring

2.2 Collaboration Features

- Multiple user roles (Admin, Editor, Reviewer, Read-only)
- Concurrent editing with conflict prevention
- Comment and annotation capabilities
- Internal notes separate from reportable content
- Approval workflows

2.3 Analysis and Reporting

- Customisable report generation
- Data visualisation and trend analysis
- Cross-audit comparison tools
- Export reports in Word, PDF, and Excel formats
- Dashboard showing audit portfolio overview

2.4 Security and Access Control

- Role-based access permissions
- Audit-level access restrictions
- Activity logging and audit trails
- **Multi-Factor Authentication (Advanced only)**
- IP address restrictions (Advanced only)

3. Configuration Differences

3.1 Standard Audit System

Intended Use: Organisation-based audits with standard security needs

Security Features:

- Role-based access control
- SSL/TLS encryption in transit
- Activity logging
- Password policies

Access Control:

- Organisation-based access where users within an organisation automatically have access to their organisation's audits

- Access typically follows organisational boundaries with ability to remove specific user access where required

Best For:

- Internal organisational audits
- Practice reviews
- Self-assessments
- Thematic reviews with aggregated data

3.2 Advanced Audit System

Intended Use: Audits involving sensitive personal data requiring enhanced security

Additional Security Features:

- **Multi-Factor Authentication (MFA) via SMS** - mandatory for all Administrator Users and Respondents before accessing the Audit System when Advanced Audits are enabled
- IP address restrictions
- **AES-256 encryption at rest** for all audit data, user data, and uploaded evidence
- Advanced audit trail logging
- **Enhanced export security** requiring Multi-Factor Authentication and additional authorisation
- Additional compliance documentation

Access Control:

- **Explicit access provisioning** - System Administrators must specifically grant access to each Advanced Audit
- Users only granted access to specific Advanced Audits when permissions are explicitly assigned
- Implements security-by-design and least privilege principle for sensitive personal data

Export and Print Controls:

- Export functionality requires Multi-Factor Authentication and additional security authorisation
- Print functionality is disabled for security purposes

Advanced Audit Tools:

- **Case audit functionality** for individual safeguarding cases
- **Serious case review (SCR) follow-up audits**

- Automated chronology generation from audit responses
- Timeline visualisation of events and actions
- Export chronologies in multiple formats
- Link evidence documents to timeline events

Best For:

- Child safeguarding case audits
- Serious case reviews (SCRs)
- Audits containing identifiable personal information
- Multi-agency audits with sensitive content
- Any audit processing special category data under GDPR Article 9

4. Service Delivery

4.1 Access and Availability

- **Platform:** Cloud-based, accessible via web browser
- **Availability:** 24/7 access (subject to planned maintenance)
- **Supported Browsers:** Current versions of Chrome, Firefox, Safari, Edge
- **Mobile Access:** Responsive design works on tablets; limited phone functionality

4.2 Implementation

- System configuration to your requirements
- User account setup and permissions configuration
- Template and framework customisation
- Data migration support (if required)
- Integration with existing systems where feasible

4.3 Training

Mandatory Training: System Administrators and Administrator Users MUST complete Phew!-delivered training before accessing support services

For Advanced Audit System: Additional security and Multi-Factor Authentication setup training is required

Training Options:

- Live online training sessions

- On-site training (additional costs apply)
- Recorded training materials for reference
- User guides and documentation
- Refresher training as needed

Training Coverage:

- System navigation and basic features
- Creating and managing audits
- Collaboration tools
- Report generation
- Security and data protection best practices

5. Support Services

5.1 Technical Support

Eligibility: Available to System Administrators and Administrator Users who have completed Phew!-delivered training

For Advanced Audit System: Additional security and MFA setup training required before support eligibility

Support Channels:

- Email support
- Telephone support
- Online help documentation
- Video tutorials

Support Hours: 09:00-17:00, Monday-Friday (excluding English public holidays)

Response Times: We aim to respond to support requests within one business day

Fair Use Policy: Support is subject to fair use. We'll contact you if usage becomes excessive (typically over 20% of contract value). Most clients use 5-10% of this threshold.

Support Covers:

- Technical issues and bug reports
- How-to questions about system features
- Account and access issues
- Report generation assistance

- General system guidance

5.2 What's Not Included

- Custom development or feature requests
- Third-party software support
- Training for untrained users
- On-site support (available separately)
- Audit methodology advice

6. Updates and Maintenance

6.1 Platform Updates

- Regular feature enhancements and improvements
- Security patches and updates
- Bug fixes
- All updates deployed automatically - no action required from you

6.2 Planned Maintenance

- Scheduled during low-usage periods where possible
- Advance notice provided for major maintenance
- Most maintenance completed with minimal service disruption

6.3 Emergency Maintenance

- Unscheduled maintenance may occur for critical security or operational issues
- We'll communicate as quickly as possible when this happens

7. Pricing Structure

7.1 License Types

Standard Audit System:

- Annual per-user license fee
- Tiered pricing based on number of licenses
- Volume discounts available

Advanced Audit System:

- Higher annual per-user license fee

- Reflects enhanced security infrastructure, compliance requirements, and specialised features
- Tiered pricing based on number of licenses

7.2 Included in License Fee

- Platform access for licensed users
- Standard feature set
- Technical support (for trained System Administrators and Administrator Users)
- Platform updates and improvements
- Data storage within reasonable limits
- Standard reporting tools

7.3 Additional Costs

- **Training:** Charged separately per the Training Rate Card
- **Additional Storage:** If you exceed reasonable data storage limits
- **Custom Development:** Bespoke features or integrations
- **On-site Support:** Travel and time charged separately
- **Data Migration:** Complex migration projects charged separately

7.4 Payment Terms

- Annual license fees paid in advance
- Payment due within 30 days of invoice
- Auto-renewal unless terminated per contract terms

8. Your Responsibilities

8.1 Data Management and Security

- You're responsible for accuracy and appropriateness of audit content
- You control who has access to your audits through appropriate permission management
- We process data only on your instructions as Data Processor
- We don't use your data for any other purpose

8.2 Data Retention

- Active data retained while contract is active
- Post-termination: retention per implementation agreement

- **Important:** Export any required data before contract ends
- We're not responsible for data recovery after termination

8.3 Appropriate Use

Configuration Selection Based on Data Sensitivity:

Standard Audit System:

Suitable for organisation-based audits with standard security needs where no identifiable personal information is processed

Advanced Audit System:

MUST be used for:

- Individual case audits (child or adult safeguarding)
- Any audit containing identifiable personal information
- Special category data under GDPR Article 9
- Serious case reviews involving named individuals

Important: Only the Advanced Audit System provides appropriate security controls (encryption at rest, Multi-Factor Authentication, explicit access provisioning) for sensitive personal data. Using Standard configuration for sensitive data would breach GDPR obligations.

Other Phew! Products:

Do not use other Phew! Digital Products to store or publicly share confidential or sensitive data - the Advanced Audit System is specifically designed for sensitive data handling.

Document Version: 2.1

Last Updated: 24 January 2026

Next Review: January 2027

Changes from v2.0: Updated terminology (Multi-Factor Authentication, System Administrator), enhanced security specifications, clarified configuration selection requirements, improved support eligibility descriptions, moved case and SCR audit types to Advanced configuration

For questions about configuration selection, security features, or compliance requirements:

Phew Design Limited

Email: support@phew.org.uk

Phone: 01234 779050