

G-Cloud 15 Lot2a Service Definition for Usecore Human Cyber-Security Risk Management



1 Introduction

Usecure is a **unified Human Risk Management (HRM) platform** focused on reducing human cyber risk — the risk that arises from employee behaviour, awareness gaps, credential exposure, and policy non-adherence. It goes beyond classical training to provide continuous risk measurement, tailored learning, simulated testing, policy enforcement, and breach detection. It emphasises **automation, personalisation, measurement, and compliance reporting** to help organisations transform their workforce into an effective defensive layer against modern threats, all fully supported by Quadris security professionals.

2 Key Capabilities & Functional Components

usecure's solution is modular yet integrated, delivered through four primary functional areas:

2.1 uLearn – Adaptive Security Awareness Training

Purpose: Deliver personalised, engaging training to improve security behaviour and awareness.

Capabilities:

- Automated course assignment based on individual risk profiles.
- Bite-sized, interactive, video and quiz-based modules tailored to learning gaps.
- Dynamic learning paths that adjust to user performance over time.
- Integration with identity sources (e.g., Microsoft 365, Google Workspace) for automated enrolment and lifecycle management.
- Training automation with reminders, scheduling, and progress tracking.
- Content library updated based on current threat trends.

Benefits:

- Reduces time to competency for new and existing employees.
- Improves training completion and knowledge retention through personalisation.
- Reduces administrative burden through auto-enrol and scheduling.

2.2 uPhish – Phishing Simulation & Testing

Purpose: Simulate real-world phishing attacks to evaluate user resilience and reinforce learning.

Capabilities:

- Automated and scheduled phishing campaigns.

- Large template library covering common and emerging phishing scenarios.
- Customisable/spear-phishing campaign builder.
- Real-time results dashboards showing click rates, report rates, and risk trends.
- Automatic follow-up assignments to users who fall for phishing simulations.

Benefits:

- Quantifies susceptibility to phishing and tracks behavioural improvement.
- Reinforces training with real-world exercises, closing knowledge gaps.
- Provides measurable performance data for compliance and risk reduction.

2.3 uPolicy – Policy & Compliance Management

Purpose: Centralise security policies and track acknowledgement/completion.

Capabilities:

- Central policy repository with ready-made templates.
- eSign capture and audit tracking for policy acceptance.
- Policy distribution workflows with automated reminders.
- Linkage between policy completion and training/assessment schedules.

Benefits:

- Simplifies enforcement of security policies and standards.
- Helps demonstrate regulatory adherence (audit evidence, acceptance logs).
- Reduces manual follow-up for policy uptake.

2.4 uBreach – Dark Web Monitoring

Purpose: Detect leaked credentials and compromised identity data to preempt account takeover.

Capabilities:

- Continuous scanning of user domains and accounts against known breach sources.
- Alerts when credentials are found in dark web data collections.
- Insights on breach origin and recommended remediation actions.

Benefits:

- Early warning of credential exposure.
- Reduces opportunity for attackers to exploit compromised accounts.

Feeds actionable events directly into training or security workflows.

3 Human Risk Scoring & Analytics

Risk Measurement

usecure continuously measures *human cyber risk* using:

- User performance against training benchmarks
- Phishing susceptibility scores
- Policy acceptance and compliance records
- Credential exposure status - generating both **individual and organisation risk scores** that evolve over time.

Reporting & Dashboard

Comprehensive dashboards and exportable reports provide:

- Progress trends by user, team, client (for MSPs), and overall organisation
- Audit-ready evidence of compliance with training and policy requirements
- Comparative metrics across periods and cohorts
- Benchmarks versus external threat landscapes (where available)

4 Technical Integration & Deployment

Identity & User Sync:

- Connectors for Microsoft 365 and Google Workspace support automated user provisioning.
- LDAP/SSO options where supported (via partner configuration).

Automation & Workflows:

- Scheduled training and phishing campaigns with auto-reminders and escalation.
- Risk-based triggers for adaptive learning and remediation assignments.

APIs & Extensibility:

- APIs support integration with SIEMs, LMSs, and MSP management platforms (via partner channels).

Security & Data Handling:

- Platform hosted in cloud with secure authentication, role-based access control, data export, and audit logs.

5 Compliance & Standards Support

Usecure's platform supports evidence collection and reporting aligned with:

- ISO 27001 (A.7.2.2 Security awareness, education and training)
- Cyber Essentials / NIS2 awareness requirements
- GDPR security training evidence
- Industry-specific regulatory training mandates

Usecure's reporting and audit logs make it easier to demonstrate compliance with various frameworks by providing traceable proof of completed training and policy acknowledgements.

6 Service Outputs & Outcomes

Output	Outcome
Personalised training assignments	Increased employee cyber awareness and behaviour change
Phishing campaign results	Measurable reduction in susceptibility to phishing attacks
Policy acceptance records	Stronger adherence to organisational security standards
Dark web breach alerts	Early detection and mitigation of compromised credentials
Risk scoring & analytics	Quantifiable human risk posture for governance and compliance reporting

7 Quadris Support Services

Buyers have the following service options:

- Licence only – no support
- Usecure administrator support
- Quadris Managed Service

Service Comparison Summary

Feature	Usecure Administrator Support	Quadris Managed Service
Platform operation	Buyer-operated	Quadris-operated
Named Quadris contact	✓	✓
Administrator training	✓	N/A (Quadris operated)
Campaign execution	Buyer	Quadris

Feature	Usecure Administrator Support	Quadris Managed Service
Risk monitoring & tuning	Advisory	Proactive
Reporting	Guidance	Delivered
Operational overhead	Medium	Low

7.1 Usecure Administrator Support

This support service is designed for Buyers who wish to operate the usecure platform internally, while receiving structured onboarding, training, and ongoing named-administrator support from Quadris. This service provides assurance, guidance, and escalation support without transferring day-to-day operational responsibility to Quadris.

Included Services

- Initial onboarding and platform configuration support
- Named Quadris administrator contact for the Buyer
- Administrator training covering:
 - User onboarding and identity integration
 - Training campaign configuration and scheduling
 - Phishing simulation setup and reporting
 - Policy creation, distribution, and attestation tracking
 - Interpretation of dashboards and human risk scoring
- Guidance on best-practice campaign design and risk reduction approaches
- Support for platform configuration changes and feature enablement
- Incident and issue escalation to usecure where required
- Periodic service review meetings (remote)

Buyer Responsibilities

- Day-to-day operation of the usecure platform
- Creation and scheduling of training and phishing campaigns
- Monitoring of dashboards and user performance
- Internal communications to end users
- Actioning remediation activities based on risk insights

Service Outcomes

- Buyer retains operational control with expert oversight
- Reduced learning curve for internal administrators
- Improved effectiveness of training and phishing programmes
- Access to specialist support without full outsourcing

7.2 Quadris usecure Managed Service

Service Description

The Quadris usecure Managed Service provides a fully outsourced operating model where Quadris manages and operates the usecure platform on behalf of the Buyer. This service is designed for organisations seeking to reduce internal resource burden while maximising the effectiveness and consistency of their human cyber risk management programme.

Included Services

- End-to-end platform onboarding and configuration
- Identity source integration and ongoing user lifecycle management
- Design, scheduling, and execution of:
 - Security awareness training campaigns
 - Adaptive learning programmes
 - Phishing simulation campaigns
 - Policy distribution and attestation cycles
- Continuous monitoring of:
 - Human risk scores
 - Phishing susceptibility trends
 - Training completion and effectiveness
 - Dark web breach alerts
- Risk-based tuning of campaigns and learning pathways
- Monthly or quarterly management reports summarising:
 - Risk posture and trends
 - Compliance metrics
 - Recommended remediation actions
- Service review meetings and continuous improvement planning
- Incident coordination and escalation with usecure support
- Named Quadris service delivery manager

Buyer Responsibilities

- Provide policy content and organisational context where required
- Approve campaign strategies and reporting outputs
- Act on strategic recommendations where organisational change is required

Service Outcomes

- Reduced internal operational overhead
- Consistent, professionally managed security awareness programme
- Improved and measurable reduction in human cyber risk
- Clear governance and audit-ready reporting
- Alignment with compliance and regulatory requirements

8 Value Proposition

Strategic Benefits

- Reduces human-related security incidents

- Automates security awareness workflows at scale
- Provides measurable, auditable evidence for compliance
- Improves security culture across teams
- Supports MSP growth with scalable multi-client deployment

Operational Benefits

- Reduces administrative time through automation
- Enables MSP-centric management across clients
- Delivers consolidated, actionable insights in one pane

9 Pricing

Framework Prices for this service are in the Service Pricing attached document to this Lot 2a listing.