

Data security assurance

Finance Function Maturity Assessment and Diagnostic

Understand how your information is handled, from registration and payment through to report preparation, storage and removal. This factsheet covers the complimentary snapshot and the paid diagnostic; payment and nomination steps apply to the paid service.

Our core assurances

HHS does not see, record or store credit card details. Senior practitioners review and compile your maturity report. Client data used with AI tooling is retained within HHS Work systems and is not shared for AI model training or used to train AI models.

01 Registration and assessment information

Your business contact and organisation details are used to establish and administer your assessment. Your responses describe finance processes, controls, technology and ways of working. The diagnostic covers Record-to-Report (RTR), Order-to-Cash (OTC) and Purchase-to-Pay (PTP).

Provide process-level information relevant to the questions. Do not include passwords, bank credentials, payment-card details, payroll records or identifiable customer and supplier transaction listings in your responses. This helps limit the sensitive information held during the assessment.

02 Payment security

HHS does not see, record or store credit card details. Card details are entered directly into the Stripe hosted payment service. Stripe documents PCI DSS Level 1 service-provider certification [1].

Payment administration is separate from assessment analysis. Order, billing, transaction-reference and payment-status information supports the commercial engagement. Stripe certification relates to its payment services; it is not a certification of the complete HHS service.

03 Nominations and participation

The Finance Leader nominates the relevant tower participants. Nominee names and business email addresses are used to route assessments and operational reminders. Engagement and tower references associate responses with the intended diagnostic.

Nominate authorised colleagues and use their business email addresses. Keep assessment invitations private. If a nomination is incorrect or a participant changes, contact HHS so that the reassignment can be managed through the engagement process.

Your information and report

Provider safeguards and senior practitioner oversight

04 Data storage and encryption

Airtable supports assessment and engagement records and report attachments. Airtable documents encryption in transit and AES-256 encryption at rest, together with encrypted provider backups [2]. HHS has enabled two-factor authentication for Airtable account access.

These protections describe the Airtable platform. Other parts of the service, including payment processing, email and report preparation, use their respective provider systems. A downloaded report becomes a copy within your own organisation and should be protected under your information-security policies.

05 Practitioner-led report preparation

Senior HHS practitioners review and compile the maturity report. They assess participant responses, evaluate findings and develop recommendations. AI tooling may support this work; senior practitioners retain responsibility for the final report.

Where AI is used, client data is retained within HHS Work systems. It is not shared for AI model training or used to train AI models. OpenAI publishes supporting business data privacy commitments [3]. Use of a hosted business service involves processing by that service provider; the training assurance does not mean that no provider processing or retention occurs.

06 Review, approval and delivery

Reports pass through review and approval before client issue. The process records stages including Under review, Approved for issue and Sent. The report is provided to the Finance Leader through the engagement delivery process. Client consent is required before sharing it with an introducing agent.

Keep report links and attachments confidential. Ordinary email attachments can be forwarded and are not inherently end-to-end encrypted. Contact HHS promptly if a report or invitation reaches an incorrect recipient or you suspect unauthorised disclosure.

Retention, removal and support

Information to support your organisation's review

07 Retention and removal

Different records serve different purposes: assessment responses and reports support the diagnostic, contact information supports engagement administration, and payment records support accounting. This factsheet does not specify a standard retention period or promise automatic deletion on a particular date.

To request removal or discuss a retention requirement, contact HHS using the address below. Ask HHS to confirm the applicable period and removal arrangements before submitting information if your organisation requires a fixed schedule. Requests need to distinguish active records, report attachments, working files, emails and provider-held copies.

Removal from an active system is different from expiry of provider backups. Accounting obligations and provider retention arrangements can affect what may be removed and when. Copies already downloaded or forwarded by your organisation remain under your control.

08 Technology providers and enquiries

The service uses a hosted assessment application, Airtable for assessment administration, Stripe for payments, email services for communications and OpenAI AI tooling for assisted report preparation. This factsheet does not make a UK-only or EU-only data-residency commitment.

If your procurement or IT team needs details of processing locations, provider arrangements or specific security requirements, contact HHS before participation. This factsheet complements the HHS Privacy Notice and the terms applicable to your engagement.

Security, data handling and removal enquiries

diagnostics@hamptonheadwaysolutions.com

Provider references | [1] Stripe security | [2] Airtable security practices | [3] OpenAI business privacy
Hampton Headway Solutions Ltd | Version 1.0 | 26 October 2026