

Feb 2026

CoreStream Counter-Fraud Manager

Services Definition Document



Introducing CoreStream

CoreStream is a UK based provider of Governance, Risk and Compliance (GRC) technology solutions focused on helping organisations manage risk, satisfy compliance obligations and ultimately operate more effectively.

Our aim is simple; to make technology intuitive.

Our leadership team has decades of combined experience in big 4 consultancies and has experience in procuring and implementing technology solutions as clients ourselves. We recognise the common frustrations of working with technology partners and use this understanding to ensure we structure projects to deliver quality output, on time and within budget.

CoreStream has experience operating in a wide range of industries, including a wealth of experience in the public sector and some of the largest organisations in the world. We have strong and long-running relationships with a number of blue-chip clients which sees us renowned for delivering line-of-business applications that yield immediate results.

CoreStream is not only a technology provider. Our industry experts help you to shape the optimal solution, with the benefit of a deep understanding of your business challenges, and experience of what works in the real world.

What is GRC?

With a single fully in-house built solution, CoreStream spans the full scope of GRC as defined by the OCEG capability model



Table of Contents	1	Overview
	4	
1.1	Sample Screenshots	8
1.2	Further Configuration and Development	9
2.	Service Management	9
3.1	Monitoring	9
3.2	Data Backup and Recovery	9
3.	On-boarding and Off-boarding	9
4.	Pricing Overview	10
5.	Service Constraints	11
6.	Support Arrangements	11
7.	Hosting and Security	11
8.	Accessibility	12
9.	Training	13
8.1	User Training	13
8.2	Super User Training	13
10.	Ordering and Invoicing Process	13
11.	Government ICT Blueprint Principles	14
10.1	Information Strategy	14
10.2	Environmental Policy	14

1. Overview

CoreStream Counter Fraud Manager is a flexible solution for creating and managing an effective counter fraud control environment across your organisation, within specific divisions or at departmental level.

The CoreStream solution provides for the proactive management of your fraud risk with capabilities that manage both fraud prevention and fraud investigations.

The CoreStream solution is aligned the to the [government functional standard 013 \[GovS013\]](#) which sets the expectations for the management of fraud, bribery and corruption risk in government organisations.

The Counter-Fraud manager includes the following features, each of which can be configured to our clients specific needs:

- Policy Management module
- Integrated Counter-Fraud training (or linkage to your existing LMS)
- Online Risk Assessments
- Audit feature, allowing full management of audit content, and creation of an organisation-wide audit programme.
- Tracking of audit findings, and associated action plans.
- Case management module for logging and processing Counter-Fraud cases
- Access to external fraud investigators to collaborate on fraud investigations
- Anonymous access feature allows for a central whistleblowing portal.
- KPI management

The following table shows the GovS013 components and the CoreStream capabilities providing coverage.

GovS 013 Counter-Fraud Component	Requirement	CoreStream Capability
GovS 013 component 1: Accountable individual	Have an accountable individual at board level who is responsible for counter fraud, bribery, and corruption.	- Disseminate key information through Policy documentation and integrated guidance pages. - integrated eLearning courses.
GovS 013 component 2: Counter fraud bribery and corruption strategy	Have a counter fraud, bribery and corruption strategy that is aligned to key objectives of the strategy, and locally identified risks	- Publish strategy, policies and procedures via a friendly intranet style interface. - Capture attestations from employees.
GovS 013 component 3: Fraud bribery and corruption risk assessment	Have a fraud, bribery and corruption risk assessment that is submitted centrally	- Capture 'bottom-up' and 'top-down' risks via online configurable risk assessments. - Monitor mitigating activity including controls and action plans. - Report on key insights.
GovS 013 component 4: Policy and response plan	Have a policy and response plan for dealing with potential instances of fraud, bribery and corruption.	- Publish strategy, policies and procedures via a web site like interface. - Utilise CoreStream process mapping capability to define and refine key Counter Fraud processes
GovS 013 component 5: Annual action plan	Have an annual action plan that summarises key actions to improve capability, activity and resilience in that year	- Capture actions and link to other areas of Counter Fraud activity. - Automatically prompt users based on due dates and update frequencies

GovS 013 Counter-Fraud Component	Requirement	CoreStream Capability
GovS 013 component 6: Outcome-based metrics	Have outcome-based metrics summarising what outcomes they are seeking to achieve that year. For organisations with 'significant investment' in counter fraud or 'significant estimated' fraud loss, these will include metrics with a financial impact	• Utilise CoreStream 'KPI' manager to track performance of metrics. • Associate action plans to monitor continuous improvement activity.
GovS 013 component 7: Reporting routes for staff, contractors and members of the public	Have well established and documented reporting routes for staff, contractors and members of the public to report suspicions of fraud, bribery and corruption and a mechanism for recording these referrals and allegations	• A reporting route for all stakeholders to report suspicious activity and workflow to investigate each case. • The ability to report anonymously or with associated contact details.
GovS 013 component 8: Report identified loss	Report identified loss from fraud, bribery, corruption and error and associated recoveries to the centre in line with the agreed government definitions	• Capture identified losses independently or against the specific event that resulted in the loss. • Associate remedial actions to mitigate future losses. • Report on losses by type, Directorate and/or date range.

GovS 013 Counter-Fraud Component	Requirement	CoreStream Capability
GovS 013 component 9: Access to trained investigators	Have agreed access to trained investigators that meet the agreed public sector skill standard	- Associate investigators to counter fraud risks, incidents and cases. - Disseminate information on trained investigators and associated skill sets. - Empower investigators by providing a central repository of all Counter Fraud Activity.
GovS 013 component 10: Undertake detection activity	Undertake activity to try and detect fraud in high-risk areas where little or nothing is known of fraud, bribery and corruption levels, including loss measurement activity where suitable.	Fully featured audit module, allowing for auditor-driven programmes of fraud assessments with findings and action plan capture.
GovS 013 component 11: Access to and completion of training	Ensure all staff have access to and undertake fraud awareness, bribery and corruption training as appropriate to their role.	- Integrated eLearning to build awareness. - Report on training completion rates and outcomes alongside other counter fraud activity. - Utilise off the shelf training or tailor the content to your requirements.

GovS 013 Counter-Fraud Component	Requirement	CoreStream Capability
GovS 013 component 12: Policies and registers for gifts and hospitality and COI	Have policies and registers for gifts and hospitality and conflicts of interest	- A facility for employees to provide ad-hoc or mandatory returns for all areas of business conduct. - The facility to associate specific loss reports and/or action plans to individual declarations. - Please also refer to our dedicated Declarations Manager module on G-cloud.

1.1 Sample Screenshots

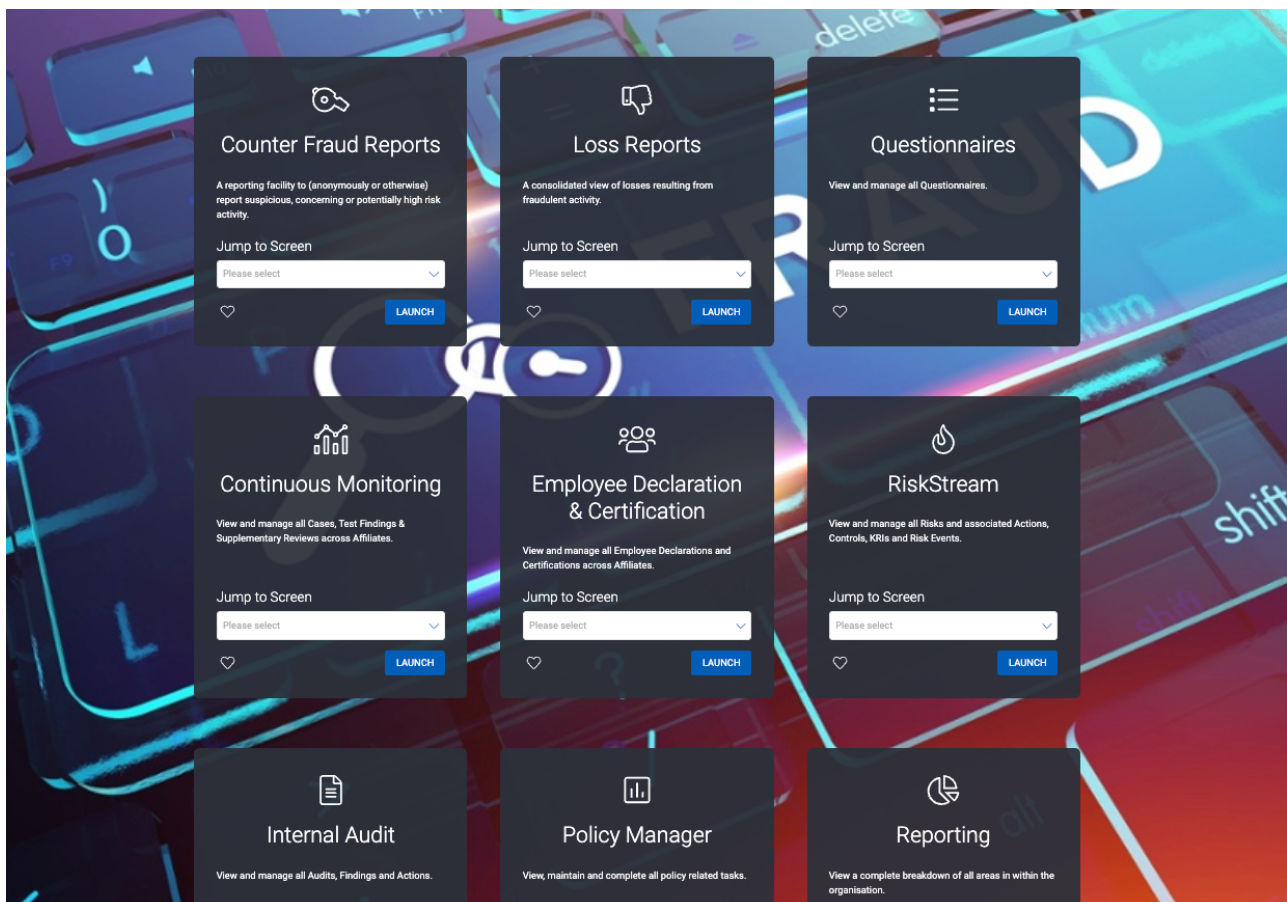


Figure 1: Home Page

1.2 Further Configuration and Development

Whilst containing a rich out-of-the-box feature set, the CoreStream platform can be easily adapted to satisfy more bespoke requirements. Additional configuration can be performed either on a time and materials or fixed-price basis.

2. Service Management

3.1 Monitoring

CoreStream hosting provides 24 hours a day and seven days a week monitoring of the computing, operating and networking infrastructure to detect and correct abnormalities. This includes environmental monitoring, network monitoring, load-balancing monitoring, web server and database monitoring, firewall monitoring, and intrusion detection.

3.2 Data Backup and Recovery

The backup schedule can be varied according to specific requirements. Our default offering provides for daily incremental backups and weekly full system backups. Backups are stored offsite in encrypted format as part of our standard offering.

3. On-boarding and Off-boarding

Each implementation of the CoreStream platform follows a standard process which our team of delivery managers will support you through:

- Requirements meeting and demonstration (FOC)
- Confirm order
- Design Workshops
- Consultancy and configuration (2 days included)
- Platform deployment and security hardening (included)
- User acceptance testing
- Training and Communications
- Launch

Data migration into the service can be supported using standard file formats (XLS, Raw Text, XML). Migration activities will be charged in accordance with our rate card unless accommodated within configuration days included with the license purchase.

Upon termination of this service, the relevant framework and call-off contract terms apply. Data repatriation will be provided free of charge (in raw text and PDF formats) unless additional requirements are specified for delivery of the data in non-standard file formats or with transformations applied. In these cases time and materials will be chargeable per the standard rate card. Following repatriation, all customer data will be purged and destroyed.

4. Pricing Overview

We only offer 'enterprise licenses', with no variable fees. The license fees are based on the complexity of the solution, with no per-user charges.

- Fixed Annual platform license fee.
- Full support included (see support section)
- Please refer to our pricing document for full details

Managed Service License Fees (excl VAT)					
Module	Platform License Fee*	Implementation Fee	Discount	Per User Charges	Includes
Counter Fraud Manager	Bronze: £18,000	£5,000	N/A as all licenses are for unlimited users.	None*	6 days implementation effort*
	Silver: £25,000	£20,000			As above, with 20 days
	Gold: £35,000	£35,000			As above, with 30 days
	Platinum: £60,000	£50,000			As above, with 50 days

Additional configuration can be performed either on a time and materials (please refer to the CoreStream pricing document for details) or on a fixed-price basis.

A minimum 1-year contract tenure applies. Pilot implementations can be arranged for a minimum 6-month period, with associated consultancy and configuration will be charged per our rate card.

We can also offer access to trial environments for limited periods, free of charge

5. Service Constraints

Deployments of new functionality will result in short outages to the service. CoreStream will provide 48 hours notice and (unless unavoidable) ensures that deployments are managed out of normal business hours.

There is a standard weekly maintenance window from between midday Saturday to midday Sunday to allow for server maintenance, though this can be varied by negotiation.

6. Support Arrangements

Standard user-support over an online support ticketing system and email is available during UK working hours (Monday to Friday, 9am to 5pm). Out of hours support is available upon request.

7. Hosting and Security

CoreStream is hosted exclusively in the UK in a Tier 3 data centre with multiple resilience and security arrangements. We guarantee in excess of 99.9% availability and service credits are payable in the event that this is not achieved.

We also offer (costed) options for hosting in the public cloud, or on-premise if required.

CoreStream is ISO27001 certified via the British Assessment Bureau (fully UKAS certified) and holds the Cyber Essentials Plus certification.

We also hold SOC2, Type2 (Security, Availability) accreditation.

Security features:

- All client environments reside on dedicated web applications and database instances. Higher levels of environment isolation are available on request

- Hosting is established in a highly resilient 'always on' configuration, meaning individual physical component failure cannot lead to a service outage.
- All data is encrypted in transit and at rest using strong protocols / cyphers
- Full daily backups held off-site in encrypted format.
- Options for real-time failover (Disaster Recovery as a Service)
- 24x7 Security Operations Centre (via Sophos MDR) means that the platform is continually being monitored for signs of breach, with trained security specialists available to contain any such incidents should they occur.
- CoreStream staff all background checked, and we can establish entire teams with UK Government 'SC' clearance where required.
- Penetration testing of the CoreStream platform is completed at least annually, by a CREST / CHECK accredited third party.
- Full time vulnerability scanning is in place for all our internet points of presence.
- We utilise the latest generation of firewalls which include deep packet inspection and intrusion detection protection.

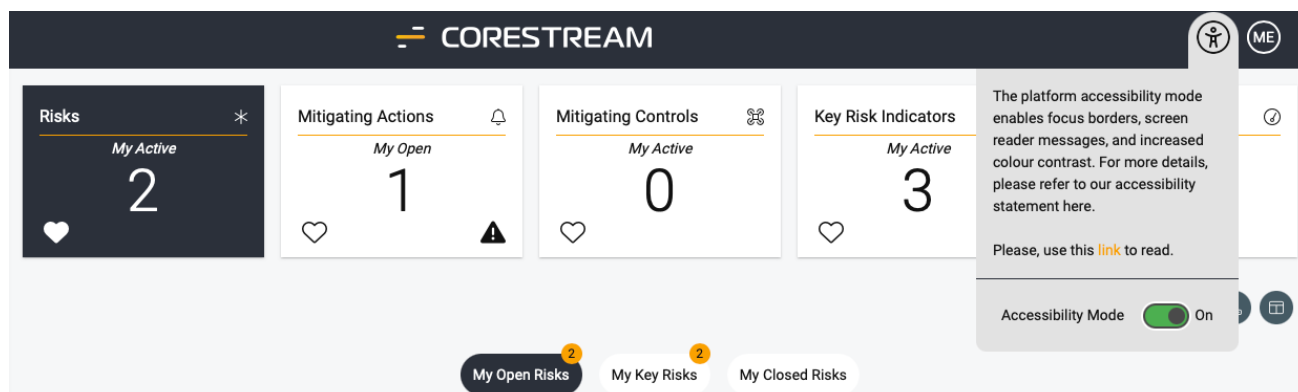
Disaster Recover and Business Continuity

- CoreStream regularly practices its disaster recovery processes and shares results with its clients.
- Business Continuity plans are typically shared as part of the client onboarding process, including incident management processes.

8. Accessibility

For users with additional accessibility needs, we largely comply with the relevant WCAG (2.2 AA) requirements, and subject our platform to an annual accessibility audit, completed by an independent accessibility specialist firm.

A dedicated 'accessibility mode' is available from all parts of the system, as is an accessibility statement describing our accessibility credentials in detail, including any known issues.



9. Training

8.1 User Training

User training will depend on the complexity of any platform modifications specified by the customer, and the number of users to be trained. Due to the in-built contextual help prompts and configurable guidance pages, training roll-out can almost always be accomplished on a “train the trainer” basis. In the unlikely event that additional training is charged on a time and materials in accordance with our standard rate card.

Large scale, multi-channel training programme design and delivery including video guides, and webinar broadcasts can be devised as required. Please refer to the CoreStream training service offering on Digital Marketplace for details.

8.2 Super User Training

Super users can be trained to be able to configure aspects of the GRC platform themselves, reducing the need for additional configuration expenditure. This training typically takes 3-5 days, depending on the skills profile of the recipients of the training.

10. Ordering and Invoicing Process

- Upon receipt of a purchase order, CoreStream will provision the environment.
- All license fees are to be paid 12 months in advance, from the point of UAT commencement.

- 50% of the first 12 months fee is due upon ordering the environment.
- The remaining 50% is due at the point of go-live.
- If additional services, or blocks of users are purchased mid-contract, the relevant fee is payable up the end of the current 12-month period, after which fees revert to 12 months in advance.
- Time and materials (Consultancy, Training etc) are invoiced monthly in arrears. Invoices are due for payment within 30 days of the invoice date.
- Please refer to our full terms and conditions for details.

11. Government ICT Blueprint Principles

10.1 Information Strategy

- CoreStream SaaS services are designed and built to align with government Information and Communications Technology (ICT) information strategy principles, ensuring information is effectively managed, protected and made accessible through the use of open standards technology. Our focus on information governance is underpinned by our ISO27001 certification.

10.2 Environmental Policy

- CoreStream takes its environmental responsibilities seriously, aligning its operations to the published ICT government greening principles. In support of these principles, CoreStream guarantees:
 - All hosting services are powered from renewable sources.
 - Non-essential travel will be minimised using technology, such as video conferencing.
 - To continue to donate monthly to the World Land Trust, helping plant trees in deforested areas.
 - To remain paper-free wherever possible.
 - To reduce waste or to recycle wherever possible.
 - Hot-desking in its office locations to reduce its overall office footprint.

Further details of our Environmental Strategy are available on request.

For more information please contact:

Melissa DSouza

Melissa.DSouza@corestream.co.uk

tenders@corestream.co.uk

