# Fraud Case Management
# v15.0
service definition


IS 721821

Blackthorn

# Contents

## Introduction

Our Fraud Case Management (FCM) tool is an on-premises or cloud-based solution that ensures that all types of fraud investigation follow a structured and disciplined approach, and that the conduct of investigations does not compromise the outcome. Fraud investigations often prove difficult and time-consuming, as well as deliver unacceptable outcomes due to process irregularities, loss of confidentiality, poor handling of evidence, ill-informed decisions, etc.

Suitable for investigating both insider-fraud (fraudulent activity within the workplace) and misdemeanours conducted by the criminal fraternity against a corporate or civil entity, the Blackthorn Fraud Case Management system provides a framework for ensuring that investigations follow a considered and optimised plan, evidence is carefully organised and maintained and there is a case chronology. It also ensures that any hypothesis can be tested or rebutted until reasonable conclusions are drawn. Additionally, channels for whistleblowing are provided so that staff and/or citizens suspicious of wrongdoing can make disclosures easily and in-confidence.

Complex investigations, at least the successful ones, apply a ‘case theory’ approach where an initial evaluation of the available facts leads to conjecture over the likely approach taken to achieve the fraud. An investigative plan follows, setting out the actions necessary to orchestrate the strategy and prove whether the conjecture was right. In the execution of the plan, proof is gathered of the steps taken to commit the offence, or the plan adjusted to take account of new information, understanding and revised conjecture. Workflow within the Blackthorn Fraud Case Management system helps orchestrate the proposed investigative plan, ensuing that actions mandated by the plan (repeatable patterns of activity) are properly coordinated and achieved in predefined sequence. It also ensures that there is a recognised ‘gate keeper’ at all critical decision points.

The success of an investigation also depends on the treatment and custody of evidence. Strategy and operational information, along with evidence, is carefully recorded as the investigation unfolds, and a log maintained to provide an auditable paper trail of the sequence of enquiries. Blackthorn ring-fences evidence items to avoid careless disclosure, whilst maintaining effective chain of custody so that there is no doubt over the authenticity and reliability of evidence in court. Physical evidence logging capability ensures that effective custody can be applied to physical property as well as digital evidence artefacts.

Our strong focus on information management is further enforced by a digital file store that supports the structured organisation of investigation data and a search function that can look deep inside uploaded files. Data objects (e.g. suspects, witnesses, locations, evidence etc.) are saved in hierarchical case models that allow relationships between data artifacts to be established. All case information, including evidence, is ‘tagged’ to accelerate the speed of searches and their reach.

Anonymous tips by staff of suspicious information and/or activity account for approximately 40% of reported fraud[1]. Our online portal (free to use) provides one channel for reporting suspicion, reports going into a central collection pool for initial evaluation, possible further information gathering, and outturn decision on whether to launch a detailed investigation. The portal can be restricted to internal use only or *opened up* for reporting by both an internal and external audience. Our whistle-blowing hotline, manned by Blackthorn and therefore operated by completely autonomous agents, provides an additional (or alternative) channel for whistleblowing.

The benefits delivered by Fraud Case Manager include:

- orchestrated handling of cases following a proven sequence of actions and tasks aligned to investigation type
- clear accountability in terms of roles and responsibilities
- *paper trail*[2] ensuring provenance and court admissibility of records and evidence artefacts
- key information elevated to forefront for improved situational awareness, insight, and decision-making
- logical and structured organisation of case data with graphical interface for ease of navigation, storage and definition of relationships and dependencies
- authority management for effective, guaranteed *ring-fencing* of case information (access based on need-to-know)
- alerts and notifications for improved awareness of targets, deadlines and 'need-for-action' to move investigations forward
- keeps investigations on track by ensuring actions endure and not lost or diluted in *the fog* of investigative communication
- web-based and telephone hotlines for whistleblowing.

Our Fraud Case Management platform enables collaboration, allowing investigators, stakeholders and business functions to move through the multiple stages of an assessment quickly and easily, and to monitor progress and outcomes as appropriate. It supports the organisation of resources, both people and assets[3], and the creation of processes allowing repeatable patterns of activity to be defined and accomplished.

---

[1] Fraud reported through whistleblowing in financial institutions.

[2] record of the sequence of custody, control, transfer, analysis, and disposition of electronic evidence.

[3] Plans, programmes, checklists, audits, evidence, reports, actions etc.

***Fundamental axioms***

Our software is designed around three fundamental axioms: insight, accountability and control. This means actions are logical and intuitive, making adoption of our software easy. Powerful but simple to use set-up and configuration tools enable solutions to be quickly and easily tailored to a customer's specific requirements, and a range of business functions to be integrated into one cohesive package to meet a specific business or operational need. Customers have 'total say' over the look and feel of their solutions and, consequently, the resulting user experience!

Fraud Case Management is one of a range of solutions based on our eGRC (software) platform. Other 'standard' solutions include:

- (Security) Incident Management
- Risk and Threat Analysis
- Pre-employment Security Vetting
- Health & Safety Assessment
- Investigation Case Management
- Law Enforcement Case Management
- Audit Case Management
- Coroner Case Management
- FOI/SAR Case Management
- Skills and Competency Assessment.

Our cloud services[4] are delivered on scalable, secure infrastructure with the flexibility to deliver optimum performance at minimum cost. Customers can choose, based on risk appetite, between UK sovereign data centres[5] that meet the accreditation and assurance requirements of data at OFFICIAL (as per the Government's Security Classification), less expensive commercial cloud-hosting, or something in between. Full UK data sovereignty can also be assured no matter which hosting option is chosen. On-premises hosting is also an option. Our services can be accessed over standard Government networks (PSN, HNSC, N3) or via the Internet with appropriate channel encryption.



[4] solutions delivered as an online, subscription service with SaaS modality.

[5] sovereign data centres meeting the specification of the Baseline Control Set (BSC) and recommendations of the UK Security Policy Framework.

## Service Capability

The Blackthorn Fraud Case Management system provides enterprise-level capability for investigating cases of fraud, in particular insider-fraud and fraud carried out by third-parties intent on deception for financial gain. It provides a platform for conducting enquiries, gathering evidence, establishing whether there is sufficient factual basis to proceed to full investigation, widening enquiries, and taking relevant action where evidence of wrongdoing is unequivocal. It ensures that investigations follow an approved, pre-prepared strategy, decisions are traceable and have authority, and custody of evidence is beyond approach. It helps with follow-up actions such as disciplinary measures, sanctions or criminal referrals.

Our Fraud Case Manager supports every stage of an investigation, a typical investigation comprising the following high-level activities:

- recording of complaints or suspicion of wrongdoing (whistleblowing)
- due diligence and validation of allegations/suspicions (new case)
- full investigation decision
- development of investigation strategy and plan
- conduct of internal enquiries & evidence gathering
- determining whether adequate predication to proceed/continue
- continuation and expansion of enquiries including external investigations
- preparation of closure report with recommendations and details of any punitive actions.

The orderly conduct of fraud investigations is enforced by a Workflow system with the inherent flexibility to adapt to the specific and often unique needs of an individual fraud case. Workflow aids investigations by imposing discipline and structure on the conduct of enquiries, ensuring actions over the lifetime of an investigation are properly managed and controlled. Different workflow proformas can be defined for the different fraud investigation types, meaning that in most instances, there is immediate correlation with the proposed investigation strategy.

Our integrated Records Management capability ensures that case information including strategic, management, incident details, and evidence artifacts, is organised and controlled in manner guaranteeing both accessibility and discernability (a *home for everything, and everything in its home*), and the information is available only to those with authority.

Users have full visibility of their investigation projects and the ability to assimilate information from multiple ‘point-of-view for enhanced situational awareness and ultimately, improved decision making. This immediacy is achieved through dashboards giving real-time access to management, operational and analytical information, the latter supporting the discovery and interpretation of fraud trends.

The FCM system assists with the reporting and documentation of cases drawing on a library of standard, tailor-made or user defined reports and form templates. Email communications, notifications and alerts can also be template based, the choice of template under system or user control.

Our FCM solution includes, as standard, functionality allowing users to:

- report suspicions of fraud through dedicated web-interface
- lay down, in advance, workflow (repeatable patterns of activity) echoing the optimum response strategy for a given fraud case type (e.g. kickbacks, embezzlement, bribery, money laundering, etc.)
- define, capture and publish *ad-hoc* response strategies for extraordinary investigations (i.e. fraud investigations not presently catered for)
- log key decisions regarding determination of strategy and information that informed decisions
- upload and apply custody to evidence, suspect / witness interview recordings and statements, forensic evidence, subject matter experts' opinions and statements
- upload and apply custody to any file, picture or document associated with an investigation
- review and evaluate documents, data and evidence (material to investigation), record conclusions and formalise follow-up actions
- identify, assign and track actions to advance investigations, address wrongdoing, apply administrative sanctions, start a criminal referral, appraise authorities, prevent reoccurrence etc
- access key information and insight via strategic, operational and analytical dashboards
- create bespoke dashboards and customise supplied dashboards
- access the information behind the information (dashboards) using drill-down and hyperlinks for improved situational awareness
- create documents and reports using standard templates (.dotx) automatically filled with data from FCM case records (a.k.a. mail merge)
- add subjective content to auto-generated internal and statutory documents and reports
- create notifications and email alerts to raise awareness, prompt action, escalate issues.

Access to the Fraud Case Management System can be extended to business users, third-parties or other agencies for improved engagement and/or to facilitate information exchange. For example, user portals and temporary, discretional user accounts created for business use, could provide witnesses with interview timing information, file upload facilities, or facilities to digitally sign statements. Similarly, portals could be used to provide external consultants working in an advisory capacity

access to specific investigation cases. Blackthorn's 'Special Handling' functionality allows far more selective access to fraud cases, opening or locking down visibility at 'named' individual level. This might be advantageous where the sensitivity of an internal case demands very few people are aware of the investigation, or to extend the reach of a given case where the suspect is under investigation in more than one office or region.

With our Mobile App (cost option), elements of an investigation can be conducted offline and in environments where Wi-Fi network connectivity is poor or non-existent. Necessary resources, including templates and information relevant to the task in hand, are downloaded in advance, and the output from work activities (e.g. witness report) uploaded when permanent access to the central FCM system is re-established.

A calendar function makes the planning and scheduling of interviews, enquiries and other meetings straightforward and the re-allocation of activities between members of the investigating team just as easy. Automated notifications and alerts raise awareness of new and pending actions, up-and-coming targets and deadlines but can also be used for management escalation if slippage endures.

Our many years of experience working with public and private sector organisations has taught us that no two organisations are totally alike and whilst their underlying requirements might be the same e.g. insider threat, some deviation from our established product line is inevitable. This might be required to cater for circumstance, individual preferences, or the need to integrate with existing in-house applications and systems. Specific data collection, assessment or reporting needs might also be the catalyst for change. Whatever the reason, our data configurable software ensures that any additional bespoke coding is kept to a minimum and the dwell time between contract award and initial operating capability is measured in weeks rather than months.

All variants of our Fraud Case Management System are based on a technology platform (cloud or on-premises) that incorporates the following features and capabilities:

**a) Information capture**

High-fidelity eForms with embedded data validation and consistency checking help eliminate mundane and error prone data entry. eForms are context sensitive, only displaying the fields required for the operation in-hand. Documents, files, audio recordings, scanned papers etc. can be emailed to the system and automatically added to a case. Web services allow data transfer (input and output) to other digitally enabled, online systems, again reducing the necessity for manual data entry (see Interoperability below).

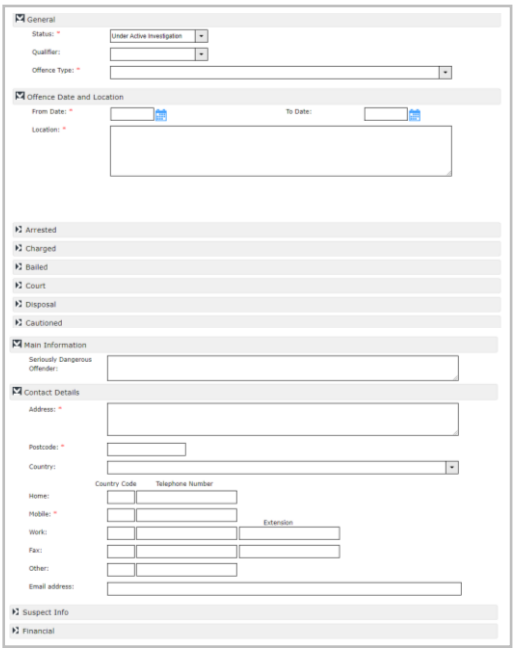



*Figure 1: Custom e-Form*

### b) Records Management

Our *records Manager* function provides real-time access to investigation records including evidence, statements & reports, suspect details, witness details, strategy, and operational data. Case records can also hold uploaded artifacts such as documents, photos, audio recordings, video files etc. A graphical user interface supports the organisation of this data, with subfolders for the classification of different types of case content. For example, statements prepared by subject matter experts could be archived in a dedicated subfolder under a case. Similarly, an evidence item could be stored as a child-object to a suspect, making clear to whom the evidence pertains. There is no restriction on the file types that can be uploaded and appended to a case.

Logical associations can be created between cases and the between records and artifacts across cases. For example, cases created to investigate case of fraud within a given business function or service operation could be linked.

The system is able to securely handle sensitive information and restrict access to only those with a genuine ‘need-to-know’.

### c) Search

A Search function employing ‘fuzzy logic’ allows searches to be conducted with partial or incomplete data. During data entry or file upload, the information presented to the FCM system is indexed prior to storage, creating meta-data files that accelerate future searches and look up. The search

results remain vigilant of any user access restrictions in force, ensuring the privacy of sensitive information.

### d) Dashboards

'At-a-glance' access to key information and insight needed to drive decisions. Operational dashboards provide directors, managers and seniors with a snapshot of the status of operations including capacity and progress. They provide investigators with fast changing information about their cases, workload, actionable tasks, overdue activities etc. Analytical dashboards enable a more detailed evaluation of cases, comparison between cases over time, or access to underlying details or trends. An example of a dashboard is provided in figure 2.0 & 2.1 below.

Filtering by case attribute, for example named investigator, team manager, reporting date, investigation status, etc. allows the 'window' on to case data to be narrowed and better focused. Filters can be also used for analytical reporting and detailed trend analysis.

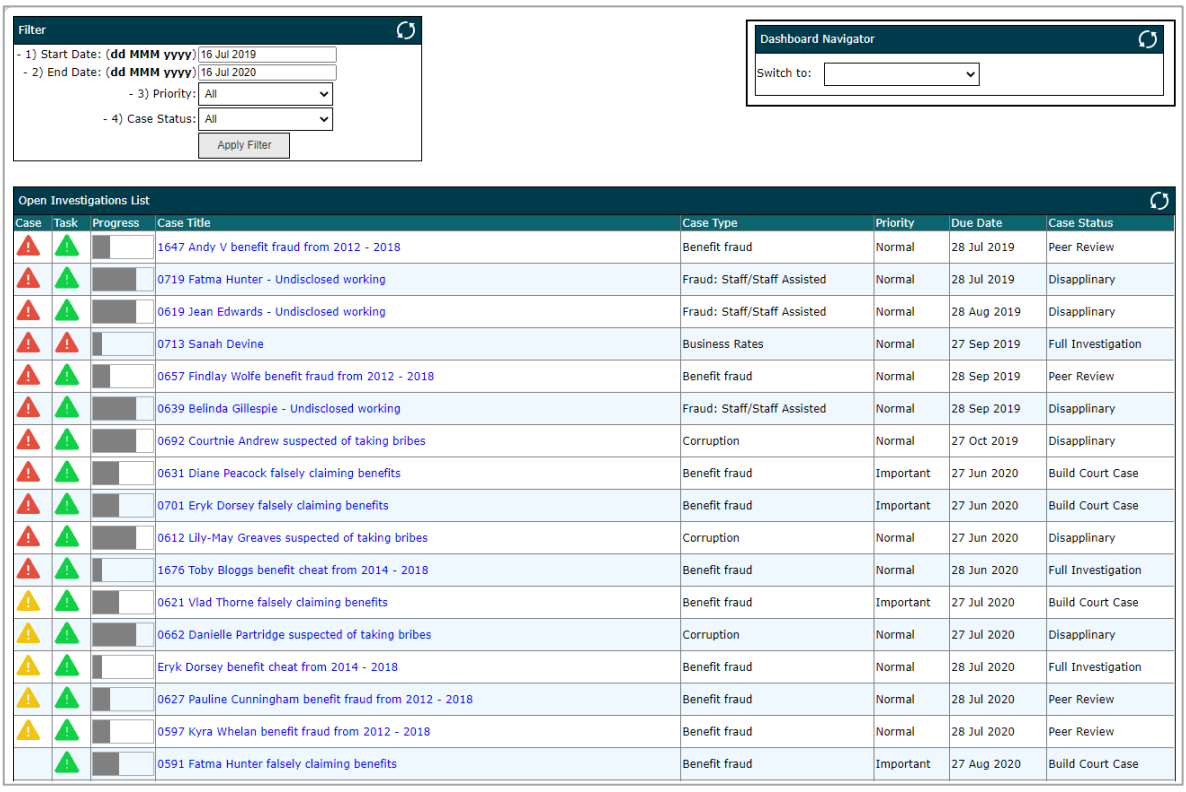
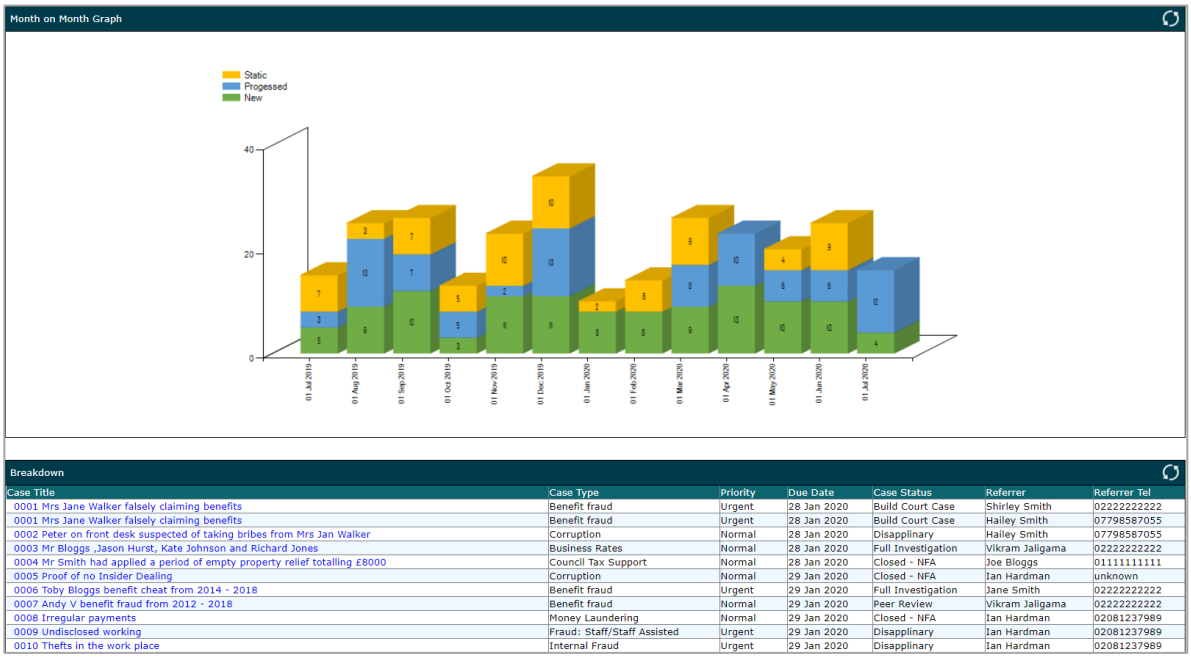



*Figure 2: Internal Investigation Cases*




Breakdown

| Case Title | Case Type | Priority | Due Date | Case Status | Referrer | Referrer Tel |
|---|---|---|---|---|---|---|
| 0001 Mrs Jane Walker falsely claiming benefits | Benefit fraud | Urgent | 28 Jan 2020 | Build Court Case | Shirley Smith | 02222222222 |
| 0001 Mrs Jane Walker falsely claiming benefits | Benefit fraud | Urgent | 28 Jan 2020 | Build Court Case | Hailey Smith | 07798587055 |
| 0002 Peter on front desk suspected of taking bribes from Mrs Jan Walker | Corruption | Normal | 28 Jan 2020 | Disapplinary | Hailey Smith | 07798587055 |
| 0003 Mr Bloggs ,Jason Hurst, Kate Johnson and Richard Jones | Business Rates | Normal | 28 Jan 2020 | Full Investigation | Vikram Jaligama | 02222222222 |
| 0004 Mr Smith had applied a period of empty property relief totalling £8000 | Council Tax Support | Normal | 28 Jan 2020 | Closed - NFA | Joe Bloggs | 01111111111 |
| 0005 Proof of no Insider Dealing | Corruption | Normal | 29 Jan 2020 | Closed - NFA | Ian Hardman | unknown |
| 0006 Toby Bloggs benefit cheat from 2014 - 2018 | Benefit fraud | Urgent | 29 Jan 2020 | Full Investigation | Jane Smith | 02222222222 |
| 0007 Andy V benefit fraud from 2012 - 2018 | Benefit fraud | Normal | 29 Jan 2020 | Peer Review | Vikram Jaligama | 02222222222 |
| 0008 Irregular payments | Money Laundering | Normal | 29 Jan 2020 | Closed - NFA | Ian Hardman | 02081237989 |
| 0009 Undisclosed working | Fraud: Staff/Staff Assisted | Urgent | 29 Jan 2020 | Disapplinary | Ian Hardman | 02081237989 |
| 0010 Thefts in the work place | Internal Fraud | Urgent | 29 Jan 2020 | Disapplinary | Ian Hardman | 02081237989 |

*Figure 3: Fraud Case Status by Month*

Our FCM is supplied with a range of standard, pre-configured dashboards which can be retrospectively and individually fine-tuned using filters and personal preferences. Custom dashboards can also be created (permissions allowing) to meet a specific, individual business need. A graphical interface and a range of standard widgets (standard dashboard components) is available for this purpose.

### e) Forms and Reports

Tool support is provided for the creation of forms (.docx) and reports required by statute, regulation, policy or internal protocol. Document templates can be added to the library of supplied templates allowing standard and bespoke forms and reports to be created digitally and auto completed with relevant case data. All system created documents can be annotated by the user before completion allowing subjective content to be added. Documents can be saved against a given case or to other (external) locations. Edit access to the library of standard document templates can be locked down to specific, authorised users.

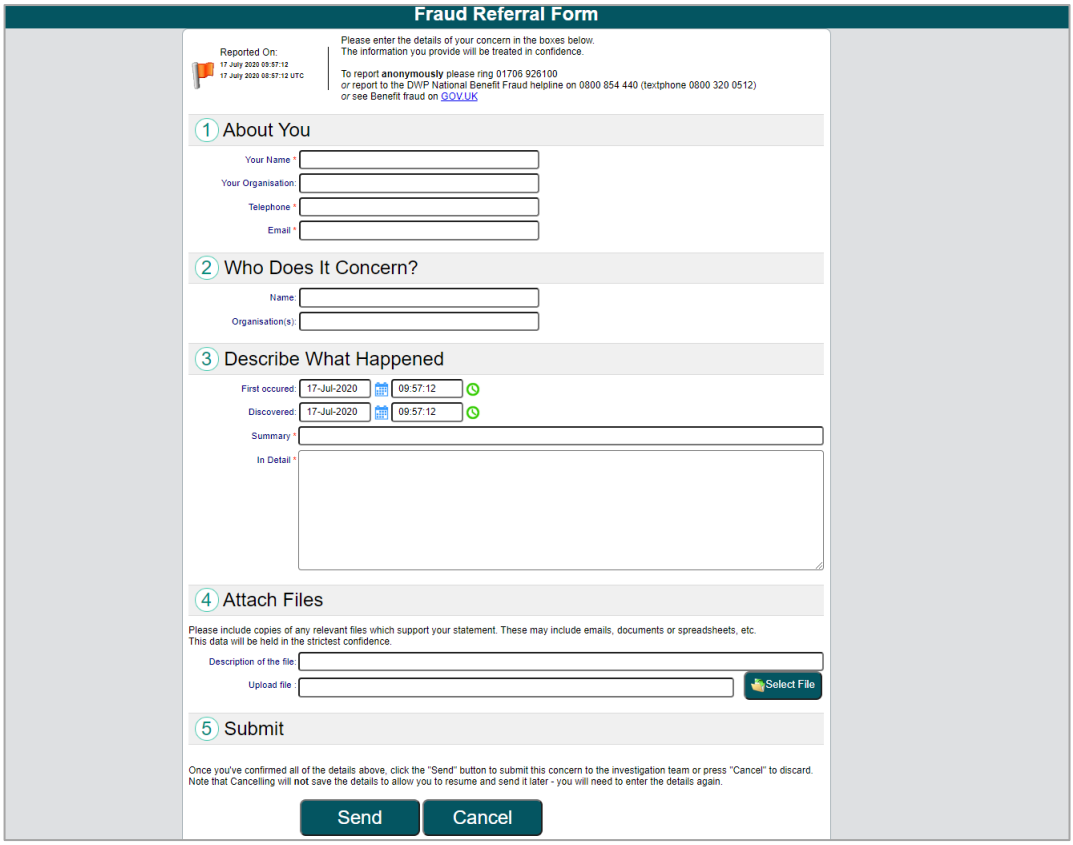



*Figure 4: Fraud Referral Form (example)*

## f) Data extraction

Data export (in either .xlsx or .csv file formats) is supported by a 'wizard' giving users complete control over the extraction process. This function might be used to facilitate statistical data analysis outside the standard analysis and reporting that is integral to the FCM system. The wizard also provides the ability to navigate around dynamic database content and structures.

## g) Tasking & Workflow

Workflow allows a set of actions with a defined outcome to be defined, organised and accomplished in prearranged order. After an assessment, typically there are a number of follow-up activities (tasks) that must be completed within a set timeframe; some of these tasks are related and interdependent and require completion by two or more people, possibly even external departments or agencies. Workflow coordinates the conduct of such

tasks, sequencing as appropriate; the work only commencing when conditions allow. Task owners are notified at the appropriate time and reminders issued before, at, and after the 'due date' if the task is late.

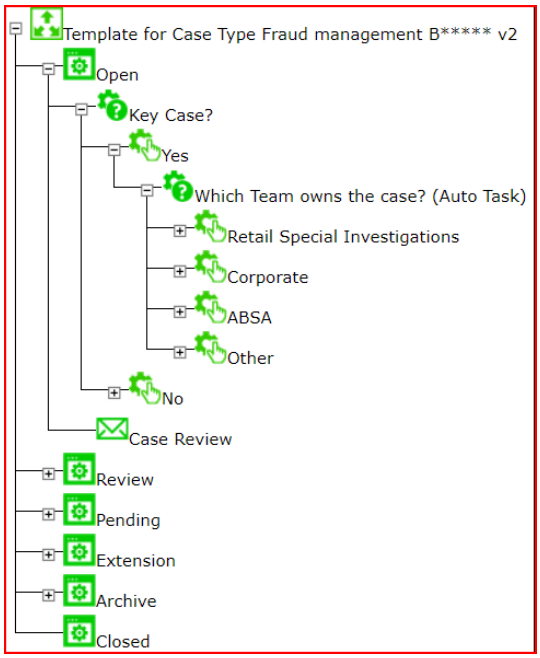



*Figure 5: Example Fraud Workflow Stages and associated tasks*

Whilst 'Tasking' is integral to the Workflow function, additional 'ad-hoc' tasks can be created as part of workflow, or independently, to address the specific and often unique needs of an investigation case. Work activities and tasks can be dynamically assigned to member of the investigation team or a wider group. Tracking tools provide fully visibility of the status of tasks, including child tasks, highlighting lateness and/or overrun.

Workflow definitions are created and published by users with Administrative user privileges using a graphical user interface and drag and drop functionality.

### h) Case Allocation

Case records have a number of attributes that are used solely by the FCM system. The 'Pool' attribute allows investigation case records to be segregated into sub-groups (i.e. pool 'A', pool 'B' etc.) and access to a sub-group restricted to a specific group or community of users. The most obvious benefit of pools is the ability to establish Chinese walls between different investigation teams or between business functions. Conversely, pools can be used to widen access, giving individual users or groups of users, access to case records (i.e. cases with a common pool ID) that previously they might not have had visibility or access to.

The segregation of users might be appropriate where two or more departments are using a single FCM platform for different types of investigation (with different privacy requirements), or where the sensitivity of investigations means that access must be locked down and restricted to a specific cohort within a wider investigation team.

Pools also allow new investigation cases to be initially allocated to an 'unassigned' category. Often due diligence needs to be performed and the results evaluated before the true nature of the events giving rise to the investigation are known. The *unassigned* category affords this opportunity, allows time to properly establish 'what' and 'when', and 'how' and with 'whose' oversight the investigation can best be moved forward. At this point the case can be allocate to a team (specific pool ID) and assigned an owner.

**i) Alerting and Notification**

Multiple channels are available for alerting and notification. Dashboards provide assessors, team-leaders, manager etc. with details of actionable tasks awaiting attention. The task list can be case centric or list actionable tasks from all cases assigned to an individual. Email alerts and notifications can be triggered manually or by workflow, raising awareness without the need to log-on. Internal messaging is a succinct method of communicating with other FCM users and has the advantage of keeping the content of the communication within the confines of the system (avoids possibility of data leakage or creep).

**j) Collaboration and communication management**

Effective collaboration depends on good team communications but a team operating without accountability is unlikely to collaborate in a helpful way. A centralized database and Role-Based Access Control (RBAC) ensure case records are reachable and access controlled, with segregation based on an individual user's profile and team hierarchy. The ability to assign access privileges to individual data assets further enhances access control, increasing the level of granularity and allowing access policy to model extant team, department, office or regional hierarchical structures. Accountability is enforced by user rights and permissions but also the process management paradigm embodied in the implementation (a function of configuration and setup).

All user actions are logged providing an admissible record of system and user actions. Log entries cannot be deleted or amended. This audit trail helps enforce accountability.

**k) Compliance and data retention (GDPR)**

Compliance is a key issue for all organisations, be it regulatory, legislative, or alignment with internal policies, procedures and rules. Compliance is addressed in a multitude of ways:

- workflow ensures authorised processes are followed
- changes to records, evidence and internal communications are evidenced by an auditable digital record, and
- strong user account rights ensure effective segregation of duties.

Compliance with the new EU Data Protection regulation is ensured by a powerful security regime that works with process management to ensure personal information is only used for its stated purpose and retained no longer than necessary.

As your service provider, Blackthorn has in place established processes for handling FOI and SAR requests where prior authorisation has been given by you (a.k.a. Data Controller).

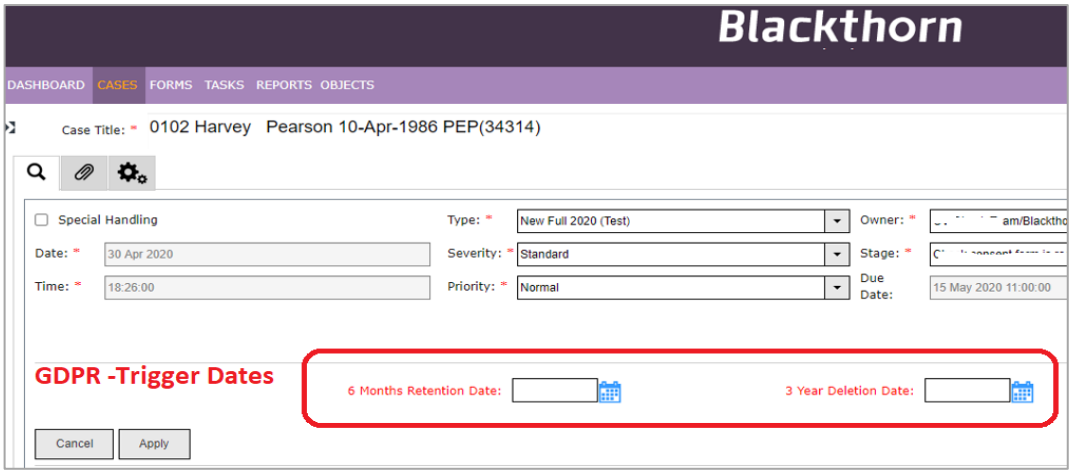



*Figure 6: Setting data deletion trigger dates*

### I) Interoperability

A library of pre-existing web services (Open API compliant and RESTful[6]) are available for standard interfacing needs. OLEDB services are available allowing direct interaction with our data storage medium. Additionally, data can be exchanged digitally via email - both inbound and outbound. This has many advantages as SMTP[7], the vehicle enabling email, is ubiquitous, making it a very open and accessible channel for information exchange.

[6] RESTful API is an application programming interface (API) that uses HTTP (Hyper-Text Transfer Protocol) to GET, PUT, POST and DELETE data, which is stateless.

[7] Secure Mail Transfer Protocol.

# Features and Benefits

| Features | Benefits |
| --- | --- |
| •Centralised management and handling of 'case' information<br>•Context sensitive eForm for data collection<br>•Graphical tools to construct and organise case data and evidence<br>•Role based security for secure partitioning of information<br>•Workflow management for process automation<br>•Evidence tracking<br>•Automatic creation of papers and files for court (option)<br>•Case accountability follows the advancement of the case and is dynamically allocated<br>•User configurable dashboards providing fast access to key case & management information<br>•RESTful interfaces for interoperability<br>•Powerful search engine for accessing cases<br>•Analysis tools to help identify associations across cases. | •Clean, intuitive user interface reducing any training requirements<br>•Simplifies and automates complex processes<br>•Collates and centralises data for improved collaborative working<br>•Automation and workflow improve efficiency and access to data<br>•Full visibility of pending, critical, overdue tasks etc.<br>•Full audit trail making users fully accountable for their actions<br>•Secure storage of data with channel encryption on remote links<br>•Wide range of supported platforms including tablets, laptops, desktops<br>•Reduces need for paper-based documents<br>•Improves data quality by eliminating human error. |

## eGRC Platform

Our eGRC platform is the workhorse behind all our case management, audit and survey solutions. It is an integrated software offering that combines core capability (modules) with extensions (wrappers) to create a suite of ready-made solutions aligned to familiar operational and/or business needs e.g. Law Enforcement Case Management, Audit Case Management etc. Set-up tools integrated into the platform enable further configuration and tailoring, and the adaption of solutions to meet specific, and often very individual, operating needs. The supply of pre-configured solutions means our software can be up and running in virtually no time, while built-in configuration tools afford the flexibility required to ensure optimal alignment with functional, as well as visual and branding preferences.

As our set-up and configuration tools are part of the supply, such work can be undertaken by ourselves or by you with a minimum amount of training. Investment in training will see an immediate return as, thereafter any through-life enhancement and update work can be completed in-house, lowering the cost of ownership.

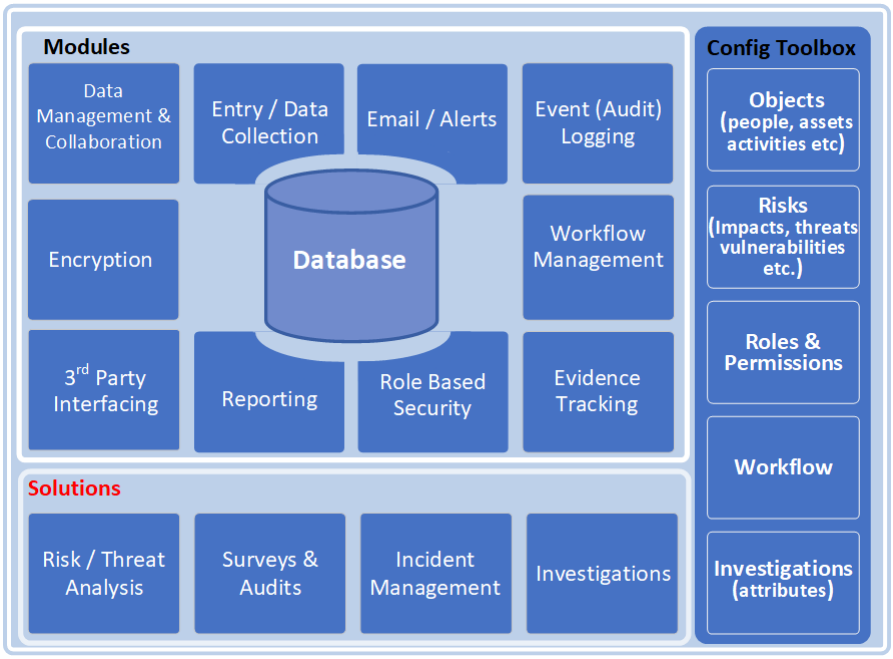



*Figure 7: eGRC Platform Architecture*

The web technologies employed by our eGRC platform are all traditional and well proven for reliability and performance. We use Xamarin, ASP.NET and MS-SQL for server-side processing, which are regularly refreshed and updated by Microsoft.

Our GUIs employs HTML & JQuery and works with Chrome, Microsoft Edge, Internet Explorer IE11 (IE9 and IE8 if there is a genuine necessity) and Firefox. This ensures our solutions work with the widest range of client devices and are backwards compatible.

## Cloud Hosting

Whilst offering government many benefits, cloud hosting introduces potential data sovereignty and security challenges. Our Fraud Case Management solution is available with full database encryption, as well as channel encryption (secure link between browser and cloud infrastructure). We have established relationships with several hosting providers and can offer different hosting options based on risk appetite, budget, and the sensitivity of the data you need to store.

We can offer single tenant or multi-tenanted hosting environment suitable for keeping data secure up to IL3/OFFICIAL. Alternatively, we can offer hosting in a commercial cloud, again with requisite levels of security.

A further option is self-hosting, either on-premises or with an infrastructure provider directly contracted. In this scenario, the supply would be on a 'software only' basis.

Regardless of provider, our service availability is better than 99.95% meaning access to reliable and secure data, without compromise.

## Service Architecture

Our standard offering is single tenanted with dedicated, virtualised infrastructure, ensuring your data is accessible only by you and any other parties you so authorise.

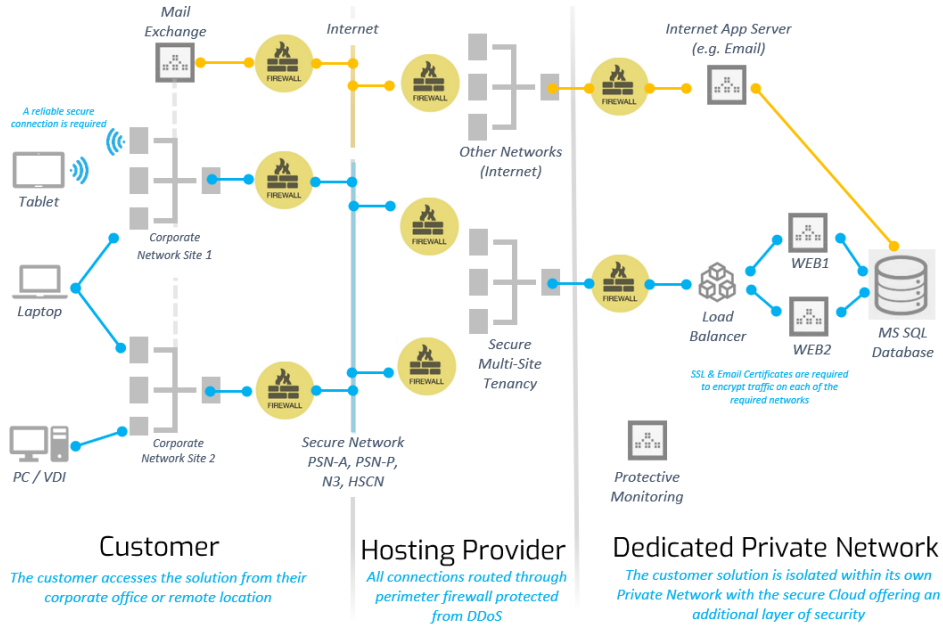



*Figure 8: Dual Web Server suitable for hosting Official Sensitive Information*

Our standard Government hosting solution (figure 8) leverages data centres meeting the accreditation and assurance requirements of data at OFFICIAL. They are reached via secure corporate and wide area networks (e.g. PSN, HSCN) and meet all Government code-of-connection requirements. An air-gapped connection to an internet facing application service provides options for email over internet (GDS

preference), reducing the demand on the Government's wide area networks. Dual webservers behind a load balancer provide the capacity to handle large quantities of HTTPS traffic but this configuration is obviously scalable, both up and down.

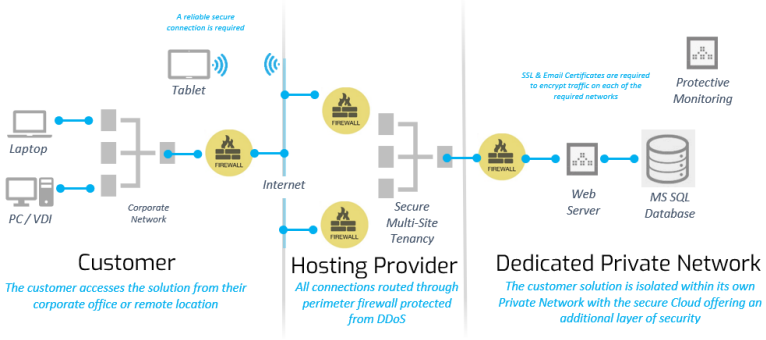



*Figure 9: Single Web Server suitable for hosting Commercial Information*

Where data security targets are less demanding, we can provide hosting with a commercial hosting provider (figure 9). The service is accessed over the internet with channel and database encryption as required. Figure 9 shows a single webserver, but again, this infrastructure is scalable both in terms of machine capacity and performance and the number of virtualised machine instances used to host our web-Application software.

## Resilience

All our providers' data centres, along with their failover sites, are within the UK, and data centre staff security vetting is commensurate with the data protection inherent in the service being procured.

Typically, data centres have geo-redundant disks to aid resilience. Data is replicated between data centres over secure links and held within each data centre (production and failover) on 'live' disks. No data is off-loaded to tape or moved off-site from data centres.

As standard, we perform hourly incremental backups and full daily backups so in the unlikely event of data loss or corruption, we can complete the full restoration of data to an earlier point in time. The minimum time to recover data (Recovery Time Objective - RTO) is less than 30 minutes depending on the size of your dataset. With hourly incremental backups, our recovery point objective is no more than 60 minutes. Other back up strategies can be implemented at additional cost.

Backup files are retained for a maximum of 1 calendar month in order to comply with the sentiment of the new GDPR (General Data Protection Regulation).

## Protective Monitoring

We employ our own protective monitoring solution within the virtualised cloud environment. This aggregates and analyses relevant data from multiple sources for evidence of persistent threats (at the boundary) and other types of unauthorised activity. Our protective monitoring solution polls the servers and other network appliances in its vicinity for security-related event information. Any exceptions or patterns of behaviour deviating from 'normal' will automatically trigger an alert once a pre-set threshold is reached. Alerts are routed directly to our Help Desk staff and in-house Security Incident Management System (SIMS) so an appropriate and measured response can be dispensed. As well as helping to coordinate any response effort, the SIMS also escalates security events internally within Blackthorn's management hierarchy if progress resolving the incident falls behind response time targets.

## Business Continuity

Business Continuity plans are separately maintained for each tenant of our cloud-hosting environment. The plans share a common backbone, but each plan is unique to ensure the resilience strategy is properly aligned to a given customer's needs. Separate plans also ensure that contact and escalation information is relevant and falls readily to hand.

The plans are regularly tested to ensure weaknesses are identified before the plan is used in anger. Plans are normally tested on an annual basis.

## On-boarding

A Blackthorn GRC Account Manager will make early contact to start the engagement process and create the necessary communication paths between senior users (or equivalent) and Blackthorn GRC's Business Analyst Team. Our Business Analysts will liaise with users to capture and consolidate our understanding of your requirements, filling in any holes or gaps in specifications and documents provided during procurement. This necessary precursor to initial system configuration and set-up ensures there is a common vision and Blackthorn has all the information required to proceed with the supply.

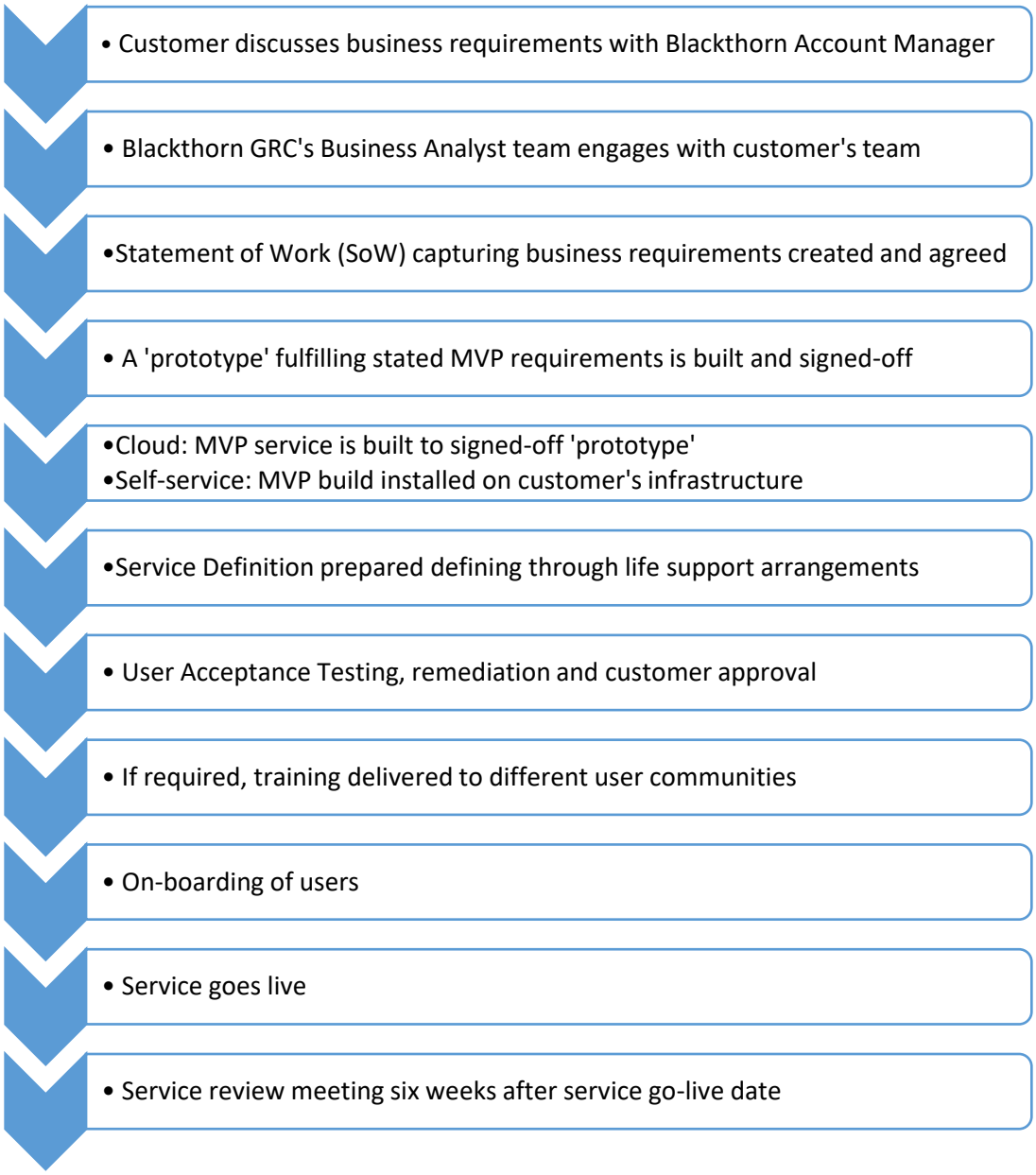



*Figure 10: On-boarding stages*

Initial engagement is followed by a phase of rapid system configuration and development work creating the forms, screens, templates, workflows, reports and dashboards necessary to tailor our standard solutions/products to your specific, and often unique, requirements. This work follows an 'Agile' style methodology where your engagement team of senior users works closely with our commissioning team on the set-up and configuration. Being on-hand (figuratively) users can critique, influence and shape the evolving design. Planned senior user contact normally occurs at the end of each Agile 'Sprint' (Sprints comprising 5-10 days of setup and development activity).

Figure 10 provides a high-level overview of the steps taken to ensure the supplied solution is the perfect fit for your organisation.

We normally aim to implement and supply the Minimum Viable Product (MVP) i.e. the minimum functionality required to get your service up and running; the residual capability (difference between the procured capability and MVP) is delivered thereafter. This approach ensures the system enters operational service soonest. It also provides users with early exposure and the opportunity to influence the latter stages of implementation.

Next, we build out the production hosting infrastructure (cloud solutions) or assist with the installation of the solution on the chosen 'self-host' infrastructure. Supply of the production hosting environment might be accelerated if data security requirements dictate that initial trials (MVP) cannot proceed using lower-grade, commercial cloud-hosting.

A period of User Acceptance Testing (UAT) follows but as customers have been directly involved throughout the set-up and configuration phase, it is unusual for UAT to uncover significant issues. The UAT phase is really intended to give a broader user audience time to evaluate the system and to identify possible performance or operational issues not previously picked up.

Finally, the wider user community is onboarded (community supplied with user accounts) and training provided (if part of the supply).

## Service Provisioning Time

Service provisioning times will vary as they are dependent on the customer's business and operational requirements.

Delivery timescales will be agreed based on the information gathered during requirements capture and the preparation of the Statement of Work.

## Service De-provisioning Time

De-provisioning time will be determined during the Off-Boarding process. Please refer to the Off-Boarding section of this document.

## Service Delivery

During the set-up and configuration phase, regular contact is maintained (daily) but as the solution enters service the level of support contact will abate to the agreed (contracted) background level.

The cloud (or on-premises) service is available 24 x 7 and mainly self-administered by the customer - at least from a day-to-day business operations perspective.

Blackthorn's Operations Team will undertake regular technical service reviews to ensure that the cloud hosting environment has the resources and compute power needed to function correctly and deliver the expected user experience (i.e. user responsiveness).

Checks will be also made to ensure that operating system and security patches are being applied to the infrastructure in accordance with vendor's maintenance schedules. If the support agreement requires additional service assurance checks, such as checking the status of 'comms' with third-party systems, these will be carried out alongside the routine checks.

Service Review Meetings will be arranged at a frequency to suit the customer, typically once every 4 - 6 weeks. These provide an opportunity to discuss service availability, performance, upkeep, resilience, patching, maintenance etc.

Day-to-day service delivery issues and functional queries are handled by our Help Desk which is available 9 x 5 or 24 x 7 according to the support package purchased. Support is delivered in accordance with our standard service SLA (see section on Response Times).

Support enquiries typically range from assistance resetting passwords through to configuration changes, or the set-up of new reports, dashboards or custom forms. If functional changes are required and the level of configuration/development effort, together with background support effort, is likely to exceed the monthly support hours allowance, we will execute the required functional changes under the auspices of a separate and dedicated 'mini project' which will be individually priced (i.e. additional cost). This approach is taken to ensure there is always sufficient 'headroom' (cost cover) to provide Help Desk support to users throughout the month (and up to the start of the following month when allowances are renewed).

During the On-boarding phase, we will prepare a Service Definition document defining through-life support arrangements. This document will include key service delivery information such as:

a. Contact points
b. Escalation processes
c. Support arrangements
    - Incident Management
    - Problem Management
    - Change Management

d. Service Desk response SLAs
e. Reporting frequency
f. Meeting schedules.

Service Delivery can also include provisions for regular security auditing - which is a key element of our Protective Monitoring solution (if purchased).

Protective Monitoring analyses audit log information from a number of key sources for evidence of malicious or unauthorised activity, whether attributable to support staff, data centre staff or external threats. Whilst this monitoring is largely machine based (Blackthorn GRC's own proprietary solution) there is a need for Blackthorn's Operations team to manually audit the monitoring system each month to ensure the system is working as intended and to carry out other checks that are beyond the capabilities of the automated system. These manual checks will be integrated into the monthly service reviews.

All of Blackthorn's support staff have been security vetted to SC Level.

## Off-Boarding

The off-boarding process considers data migration from the incumbent Blackthorn solution, as well as measures for successful engagement with the new solution provider. The process starts by defining the scope of the work and work allocation between the customer, Blackthorn GRC and the new provider. Blackthorn will participate in workshops, frequency as required, to define and agree the mechanics of commuting the data to the new provider. Key to a successful data migration is a mapping specification translating old to new data fields, possibly via an intermediary schema.

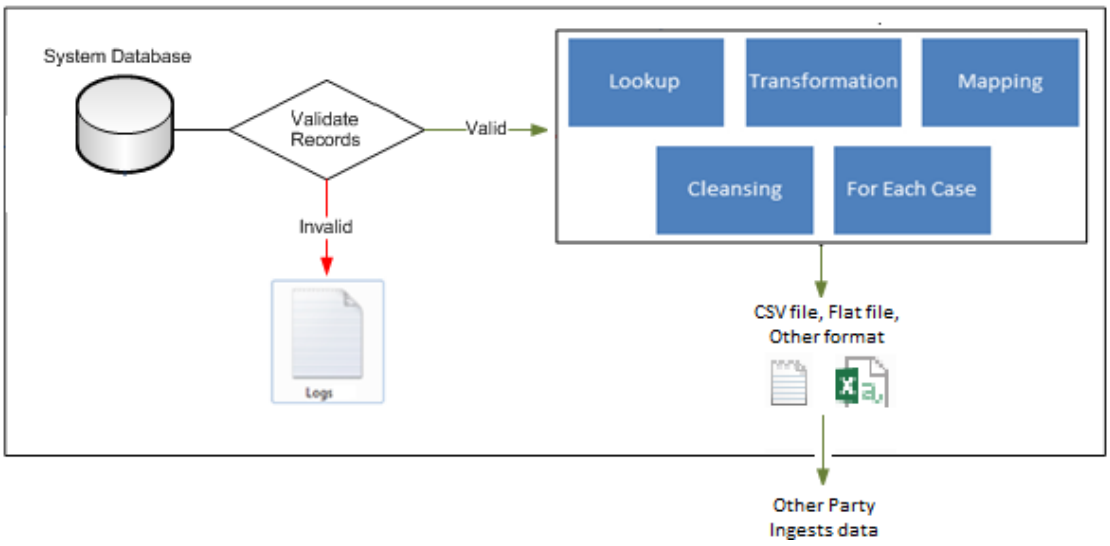



*Figure 11: Data migration process*

The data migrating process could involve:

g. Extracting all textual data to a ‘flat’ or .csv file of agreed format, the file acting as the interface between the two systems, or

h. Writing bespoke scripts and processes to manage the migration and to commute data (including non-textual items such as photos) direct from the old to new system.

Data cleansing might also be necessary to remove anomalies or convert data structures that are incompatible with the data schemas used by the new system. Any significant data cleansing is likely to generate a need for additional data testing and validation.

Figure 11 illustrates the process at high level.

## Response Times

Blackthorn GRC operates a standard Support SLA which prioritises all incidents based on an assessment of the severity of the reported problem. There are 4 priority levels for response. The priority levels, a description of the types of incidents that correspond to a priority level, and the strategy for initial evaluation and subsequent remediation, and response times (RT) are provided in the table below.

| Priority | Description | Initial Response | Resolution |
|---|---|---|---|
| **P1**<br><br>**Major Business Impact** | Product/service defect has a substantial effect on business operations with no available work-around. Results in complete loss of service for end-users, immediately impacting the clients of end-users.<br><br>An error or failure where:<br>• User(s) unable to access service<br>• Necessary work unable to proceed<br>• No immediate work-around available. | RT: < 2 hours<br><br>Acknowledgement of receipt of Support Request and supply of Case Reference No.<br><br>If there is an obvious and tenable workaround, this will be proposed as a short-term fix to enable necessary work to continue.<br><br>If 'work-around' acceptable, priority level of support request might be reduced to P2 (only with customer's approval). | RT: Initial Response + < 8 hours<br><br>Restoration of service to its previous operational state giving access to all normal 'end-user' services.<br><br>Caveats:<br>a) Recovery involving fail-over to secondary data centre – 24 hrs RTO<br>b) Recovery action that addresses symptoms rather than cause (i.e. work-around) might require follow-up investigation, analysis, and remediation. This work will be carried out under the auspices of separate Remediation Plan and progressed as a P2 incident<br>c) Assistance will be provided with networking issues between data centre and end-users but RT does not apply. |
| **P2**<br><br>**Significant Business Impact** | Business operations impacted with a significant reduction in performance or capacity (processing or bandwidth).<br><br>Business operations able to continue but if defect not resolved there will be medium to longer term consequences. | RT: < 6 hours<br><br>Acknowledgment of receipt of Support Request and supply of Case Reference No.<br><br>Supply of initial diagnosis.<br><br>If there is an obvious and tenable work-around that provides a stop-gap solution, this will be proposed. | RT: Initial Response + < 5 working days<br><br>Supply of work-around to as temporary means of recovering business operations.<br><br>Supply of interim release (or scheduled maintenance release) to remediate issue and return service to full operational state. |

| | | | |
|---|---|---|---|
| | Possible 'workarounds' are labour intensive affecting performance and productivity but offer an acceptable short-term solution.<br>An error or failure where:<br>• Users still able to access service<br>• Performance reduced<br>• No Workaround available. | Agree plan that addresses cause and provides permanent fix. | Plan any further software releases necessary for permanent fault correction. |
| **P3**<br>**Minor Business Impact** | Non-essential business function is unavailable causing a degree of inconvenience but without any significant impact on operations.<br>An isolated error or issue where:<br>• Users still able to access service<br>• Loss of some specific capability<br>• No loss of system performance<br>• Workaround is available. | RT: < 2 working days<br>Response as for P2 incidents. | RT: Initial Response + < 10 working days<br>Response as for P2 incidents. |
| **P4**<br>**No Discernible Business Impact** | All other types of issue including:<br>• 'How-to' questions<br>• Supply of documentation<br>• Cosmetic changes to GUI, dashboards or reports. | RT: Best Endeavours<br>Acknowledgment of receipt of Support Request and supply of Case Reference No. (if matter cannot be immediately resolved).<br>Agree nature and timeframe for resolution of issue. | RT: Best Endeavours<br>Deliver outlined solution within agreed timeframe. |

*Table 1: Blackthorn standard SLA for support*

## Raising a Support Request

There are several routes to raising a support ticket with Blackthorn's Help Desk. These include telephone, email and via Blackthorn's support portal – see Figure 12.

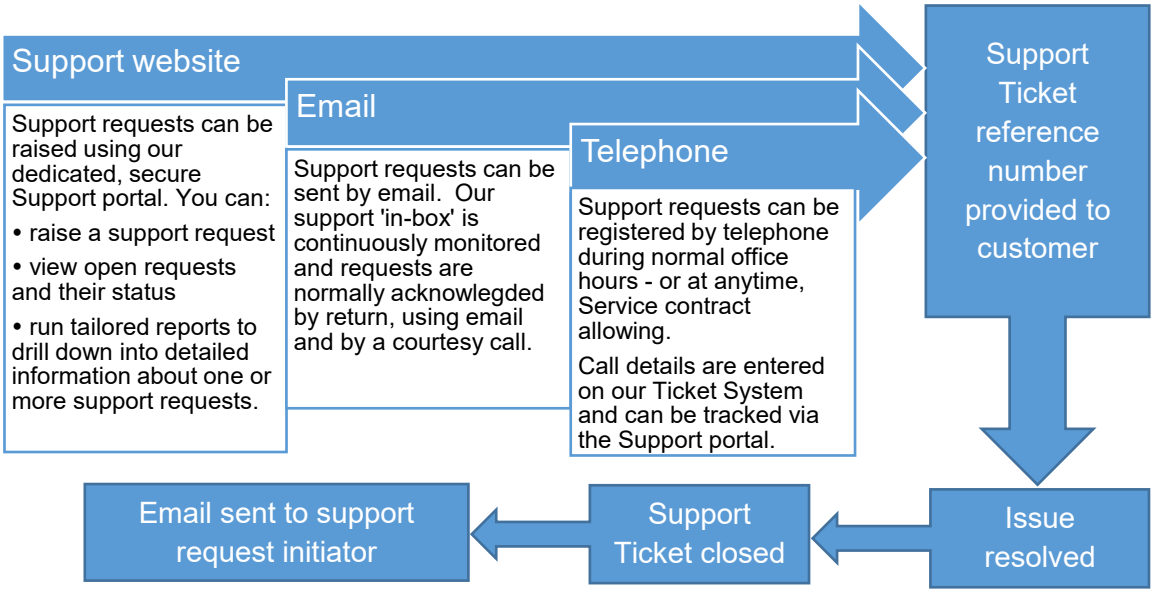



*Figure 12: Raising Support Requests*

## Terms & Conditions

See our standard Terms and Conditions document.

## About Us

Blackthorn GRC provides security-based solutions and services. We are the force behind the Blackthorn ‘admissible’ case management tool, and we have a long history of working with Law Enforcement agencies, Government and Defence. Our innovative business solutions have been in the marketplace since 2005 and enabled many of our existing customers to manage complex tasks, including internal governance activities.

We pride ourselves in developing strong relationships with our customers and helping them achieve their strategic goals. Blackthorn invests in talented staff who help to drive our organisation and enable us to continue to innovate.

## Contact

Email: g-cloud@blackthorn.com

Telephone: +44 (0) 208 123 7989