

Law Enforcement Case Management

v15.0

service definition



Blackthorn

Contents

Introduction	2
Service Capability	5
Features and Benefits	13
eGRC Platform.....	14
Cloud Hosting.....	15
Service Architecture	15
Resilience	16
Protective Monitoring.....	16
Business Continuity.....	17
On-boarding	18
Service Provisioning Time	19
Service De-provisioning Time.....	19
Service Delivery	20
Off-Boarding.....	21
Response Times	23
Raising a Support Request.....	25
Terms & Conditions.....	26
About Us	27
Contact.....	27

Introduction

Our Law Enforcement Case Management (LECM) service is an on-premises or cloud-based solution that helps Government departments and Agencies handle sensitive enforcement cases such as immigration, food standards, boarder control and human slavery. Enforcement can often prove difficult and time consuming, with many concurrent threads of investigation, high numbers of contributors, and large volumes of data, including evidential items. Organising this data so that it is identifiable, accessible and searchable, while preserving confidentiality, is a permanent challenge. Maintaining evidence, including witness statements, and preparing files for court can also present a significant challenge.

With powerful data management, workflow and reporting capabilities, our LECM solution provides a platform for law enforcement agencies and other types of task force to investigate wrongdoing and prosecute those responsible. It shares much in common with our standard Investigation Case Management solution but incorporates extensions allowing information to be exchanged digitally with the courts. This avoids the need for paper files, file bundles and other types of data exchange media. Information sharing between the LECM system and Crown Prosecution Service (CPS) is achieved with the established and widely used TWIF (Two-Way Interface).

Our LECM system is optimised for law enforcement, with tools for tracking progress and advancement against pre-defined and pre-approved investigation strategies. A graphical user interface and 'drag-and-drop' functionality streamlines data handling, and integrated analytics helps accelerate the identification of associations across cases as well as unnecessary duplication. Both important for aiding investigations and efficiency. Tools for capturing case strategies, allocating work, generating reports and notifying users of pending actions, all help to improve investigation outcomes. Moreover, our LECM solution allows users to capture information pertinent to an investigation with full audit history and reporting capabilities.

The benefits delivered by Law Enforcement Case Manager include:

- orchestrated handling of cases, based on a set of pre-defined, choreographed and proven actions aligned to investigation type
- clear accountability in terms of roles and responsibilities
- *paper trail*¹ ensuring provenance and admissibility in court of case records and evidence artefacts
- key information elevated to forefront for improved situational awareness, insight, and decision-making
- control over the structure, processing and usage of case information

¹ record of the sequence of custody, control, transfer, analysis, and disposition of electronic evidence.

- authority management for effective and guaranteed *ring-fencing* of case information (assess based on need-to-know)
- digital information (case file) sharing with CPS
- 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 are not lost or diluted in *the fog* of investigative communication.

Our Law Enforcement Case Management service enables collaboration, allowing investigators, stakeholders and business functions to move through the multiple stages of assessment quickly and easily, and to monitor progress and outcomes as appropriate. It supports the organisation of resources, both people and assets², and the creation of processes allowing repeatable patterns of activity to be defined (workflow) and accomplished.

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!

Law Enforcement 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
- Fraud Case Management
- Audit Case Management
- Investigation Case Management
- Coroner Case Management
- FOI/SAR Case Management
- Skills and Competency Assessment.

² Plans, programmes, checklists, audits, evidence, reports, actions etc.

Our cloud services³ 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 centres⁴ 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, HSCN) or via the Internet with appropriate channel encryption.



³ solutions delivered as an online, subscription service with SaaS modality.

⁴ sovereign data centres meeting the specification of the Baseline Control Set (BSC) and recommendations of the UK Security Policy Framework.

Service Capability

The Blackthorn Law Enforcement Case Management system provides enterprise-level capability for investigating criminal acts and compiling evidence for criminal proceedings where a transgression of law has taken place. Criminal investigations often can be difficult and time-consuming, and deliver unfavourable results due to process irregularities, weak argument, poor handling of evidence, ill-informed decisions etc. Our system helps mitigate these risks by ensuring investigations follow an approved, pre-prepared strategy, decisions are traceable and have authority, and custody of evidence is beyond reproach.

Our embedded Workflow ensures that investigations follow a deterministic path from inauguration through to closure, and that ad-hoc activities identified during an investigation share the same rigour and visibility as the standard activities defining a particular course of enquiry. Our Workflow aids investigations by imposing discipline and structure on the conduct of enquiries, ensuring that actions, whether part of the main strategy development, evidence gathering and analysis, or facilitation of charge decision, are properly managed and controlled.

Our integrated Records Management capability ensures that case information including strategic, management, criminal and evidence artifacts, is organised and controlled in a manner guaranteeing both accessibility and discernability, and the information is available only to those with authority. Case information is ring-fenced to avoid any possibility of careless disclosure, while records are maintained of chain-of-custody so there is no doubt over the authenticity and reliability of information as evidence.

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 trends.

The LECM system assists with the reporting and documentation of cases drawing on a library of standard, tailor-made, user-defined report and form templates. This library includes the full range of MG-forms for reporting criminal acts at the point of charge decision or criminal proceedings.

Access to the LECM system can be temporarily or permanently extended to department users outside the immediate *sphere of operations*, third-party organisations or other government agencies. This might be necessary for reporting, to aid engagement, or for basic information exchange. Our TWIF (Two-Way Interface) with the CPS is one such example of extended access. However, online portals could be introduced to give external consultants working in an advisory capacity access to specific investigations, or discretionary access to upload, for example, witness statements or police reports. Online portals could also be used to provide witnesses with calendar information such as interview timings, the ability to upload files, or facilities to digitally sign statements.

With our Mobile App⁵ (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 LECM 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 provide awareness of new and pending actions, up-and-coming targets and deadlines but can also be used for management escalation if slippage endures.

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

- lay down, in advance, workflow (repeatable patterns of activity) aligned to the optimum response strategy for a given investigation type (e.g. illegal entry, people trafficking, slavery, financial crime etc.)
- define, capture and publish *ad-hoc* response strategies for extraordinary investigations (i.e. investigations not presently catered for)
- log key decisions and the information that informed the decision
- upload and apply custody to evidence, suspect or witness interview recordings/statements, forensic evidence, *subject matter expert* opinions and statements
- upload and apply custody to any file, picture or document associated with an investigation
- review and evaluate collected information (material to investigation), record reflections and formalise follow-up actions
- identify, assign and track actions assigned to other contributors to an investigation (both internal and external, with and without user accounts)
- access key information and insight using 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
- auto-complete standard reports by populating report templates with operational investigation data (a.k.a. mail merge)
- add subjective content to auto-generated management, operational, judicial, and/or regulatory reports
- supply digital files to support charge decision and/or court proceedings

⁵ iOS, Android and Windows devices supported.

- create notifications and email alerts to raise awareness, prompt action, escalate issues.

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. law enforcement, 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 Law Enforcement 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 to 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).

b) Records Management

Our records Manager function provides real-time access to investigation records including evidence, statements, suspects, witnesses, strategy, and case progress. Case records can also hold uploaded artifacts such as documents, photos, audio recordings, video files etc. A graphical 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. 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 between records and artifacts across cases. For example, cases created to investigate case of financial fraud within a given business function or service operation could be linked to a criminal investigation case.

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 LECM 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 or over time, or access to underlying details or trends. An example of a dashboard is provided in figure 1 below.

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

Charts							
Case	Task	Progress	Case Title	Case Type	Priority	Due Date	Case Status
	!		2892 SH Email Test	Asylum Fraud	Normal	25 Sep 2020	Under Active Investigation
	!		2894 My New Investigation	Human Smuggling - Other	Normal	09 Sep 2020	Under Active Investigation
	!		2900 Operation Hotel 2123	Human Smuggling - via Van / Car	Normal	20 Aug 2020	Under Active Investigation
!	!		2899 Ops Blue bird	Asylum Fraud	Normal	20 Jul 2020	Closed
!	!		2902 Hotel NAHMI	Identity Documents Offences – Level 1 Individual	Normal	16 Jul 2020	Under Active Investigation
!	!		2895 My New Investigation 2	Common Travel Area Abuse	Normal	16 Jul 2020	Re-opened
!	!		2893 Op Wick	Human Smuggling - via Van / Car	Normal	16 Jul 2020	Under Active Investigation
!	!		2942 201809121509 Operation VJHMI	Asylum Fraud	Normal	24 Oct 2018	Under Active Investigation
!	!		2941 201809051424 Operation Hotel	Asylum Fraud	Normal	17 Oct 2018	Under Active Investigation

Figure 1: Investigation Status Dashboard

Our LECM 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 needs. A graphical interface and a range of standard widgets (standard dashboard components) is available for this purpose.

e) Forms and Reports including MG Forms

Tool support for the creation of forms (.docx) and reports required by statute, regulation, policy and 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.

Document (template) library includes all MG Forms required for charge decision and criminal prosecution. Automated completion of MG Forms with editorial control remaining firmly in the hands of the Case Officer.

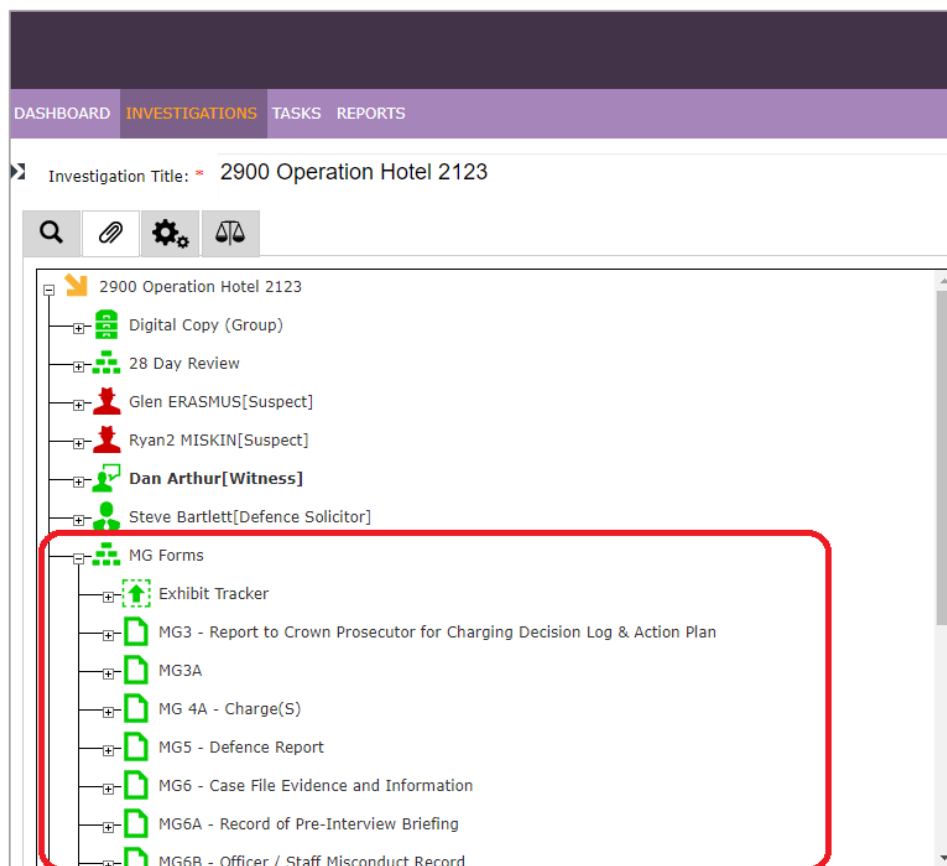


Figure 2: MG Forms Library

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 LECM 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.

Task Name	ManageTask	Task Owner	Task Created date	Associated Investigation	Status	Task Due Date
Youth aged under 18 Gra**** Smith (Sensitive content)		Nigel Adcock HMI	25 May 2016	2891 Ops Comcast Alpha		26 May 2016
Complete MG3 Form		Ian Hardman (HMI2)	16 Jul 2020	2892 Operation Gold Fish		18 Jul 2020
Perform a 28-Day Review HMI		Vikram Jalligama HMI	16 Jul 2020	2892 Operation Gold Fish		16 Jul 2020
Please Review CCTV from 15th June		FirstName656 LastName656	16 Jul 2020	2900 Operation Hotel 2123		06 Aug 2020
Complete Witness Statement MG11 for Dan Arther		Vikram HMI User2	16 Jul 2020	2900 Operation Hotel 2123		27 Jul 2020

Figure 3: Dashboard view showing Due Tasks by Case

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.

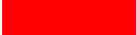
Tasks in Last 30 days Split by Status		
Not allocated	 46	30.67%
Allocated	 99	66.00%
In Progress	 5	3.33%
Completed	 0	0.00%
Closed	 0	0.00%
Closed Incomplete	 0	0.00%

Figure 4: Dashboard giving a Task summary by status.

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 LECM 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 LECM 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 some basic, rudimentary information needs to be gathered and evaluated before the true nature of events leading to the investigation are known. The *unassigned* category affords this opportunity, allowing 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 allocated 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 LECM 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) Two-Way Interface

Bi-directional link supporting digital communications with Crown Prosecution Service. Service avoids the need to prepare paper files or bundles supplied in support of charge decision or criminal prosecution. Interlocks to ensure the supply of MG forms to CPS is correctly sequenced and the supplied information is complete and consistent. Message queuing (inbound and outbound) ensures reliability of the CPS 'link' and file transfer process. Case records automatically updated with court judgement post judicial process.

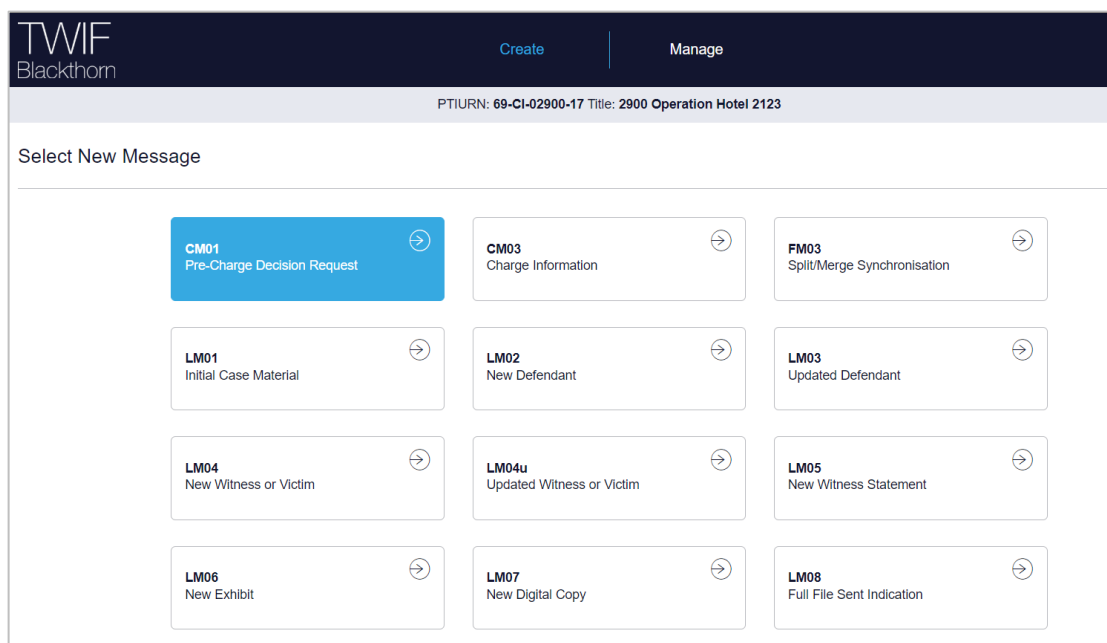


Figure 5: CPS message selection

l) 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).

m) Interoperability

A library of pre-existing web services (Open API compliant and RESTful⁶) 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 SMTP⁷, the vehicle enabling email, is ubiquitous, making it a very open and accessible channel for information exchange.

Features and Benefits

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

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.

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. Incident Response 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 us 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.

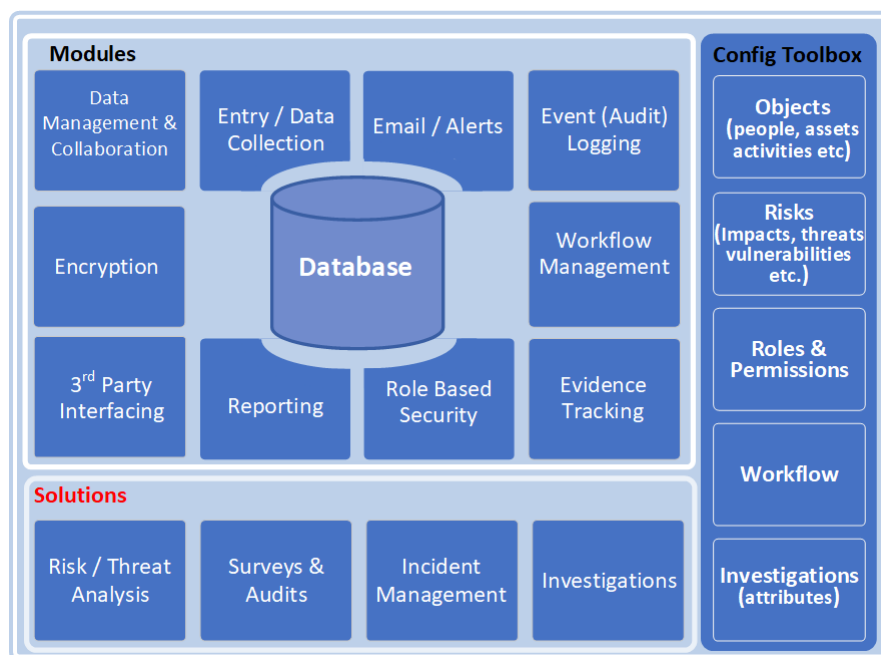


Figure 6: eGRC Platform Architecture

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 work 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 Law Enforcement 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.

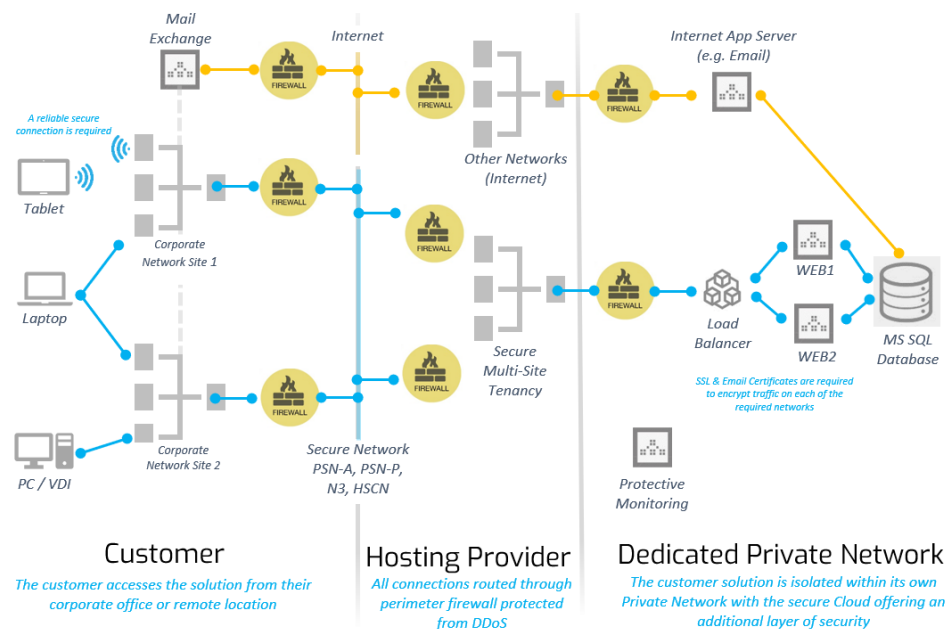


Figure 7: Dual Web Server suitable for hosting Official Sensitive Information

Our standard Government hosting solution (figure 7) 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.

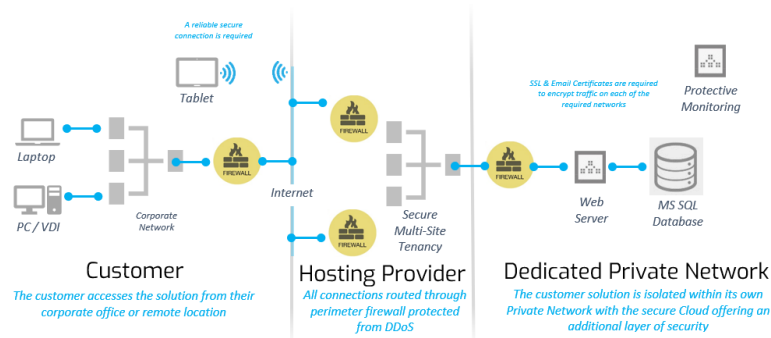


Figure 8: Single Web Server suitable for hosting Commercial Information

Where data security targets are less demanding, we can provide hosting with a commercial hosting provider (figure 8). The service is accessed over the internet with channel and database encryption as required. Figure 8 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.

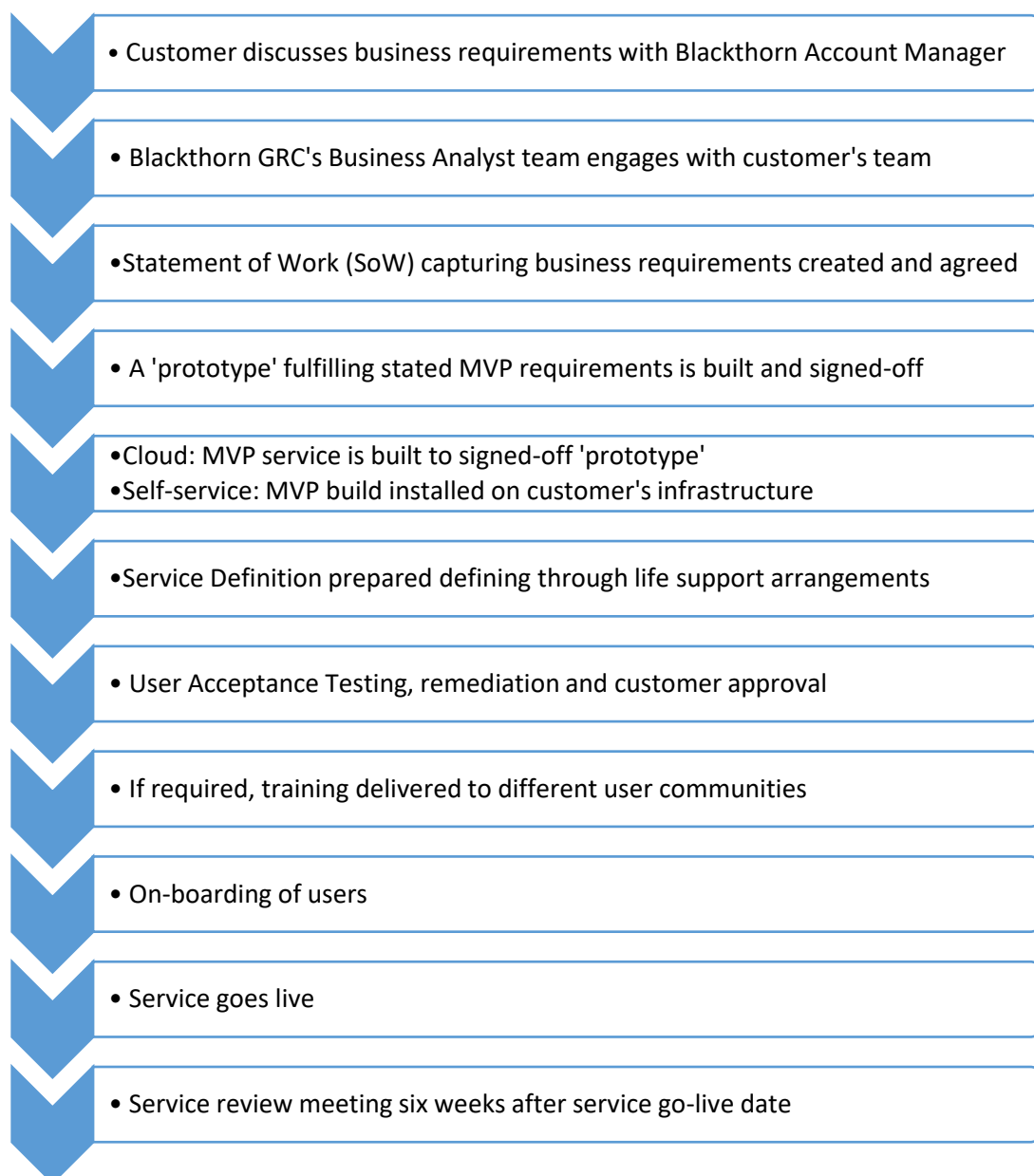


Figure 9: On-boarding stages

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 9 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.

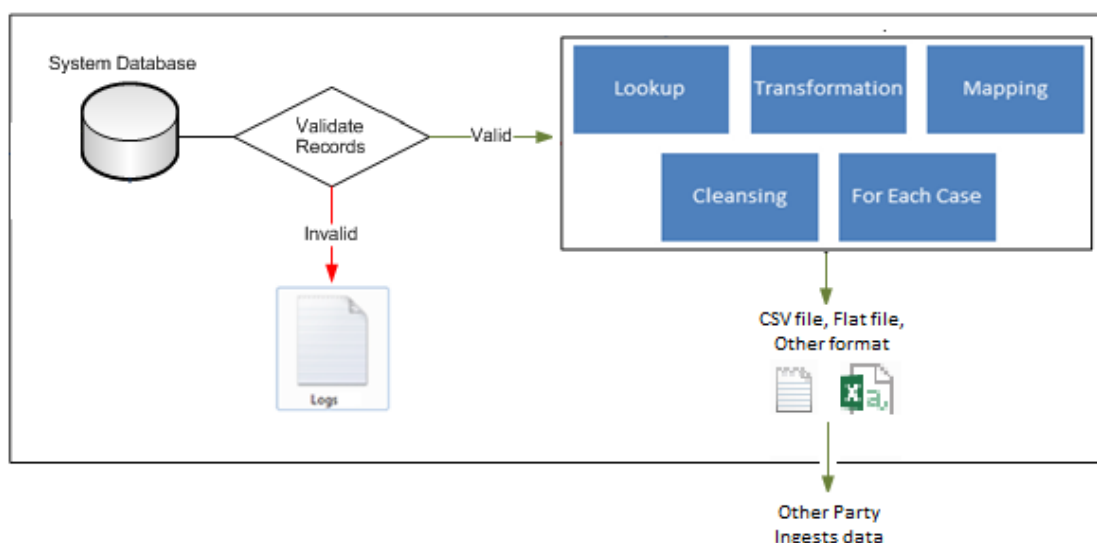


Figure 10: Data migration process

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 10 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 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. An error or failure where: • User(s) unable to access service • Necessary work unable to proceed • No immediate work-around available.	RT: < 2 hours Acknowledgement of receipt of Support Request and supply of Case Reference No. If there is an obvious and tenable workaround, this will be proposed as a short-term fix to enable necessary work to continue. If 'work-around' acceptable, priority level of support request might be reduced to P2 (only with customer's approval).	RT: Initial Response + < 8 hours Restoration of service to its previous operational state giving access to all normal 'end-user' services. Caveats: a) Recovery involving fail-over to secondary data centre – 24 hrs RTO 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 c) Assistance will be provided with networking issues between data centre and end-users but RT does not apply.
P2 Significant Business Impact	Business operations impacted with a significant reduction in performance or capacity (processing or bandwidth). Business operations able to continue but if defect not resolved there will be medium to longer term consequences.	RT: < 6 hours Acknowledgment of receipt of Support Request and supply of Case Reference No. Supply of initial diagnosis. 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 Supply of work-around to as temporary means of recovering business operations. 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. An error or failure where: • Users still able to access service • Performance reduced • No Workaround available.	Agree plan that addresses cause and provides permanent fix.	Plan any further software releases necessary for permanent fault correction.
P3 Minor Business Impact	Non-essential business function is unavailable causing a degree of inconvenience but without any significant impact on operations. An isolated error or issue where: • Users still able to access service • Loss of some specific capability • No loss of system performance • Workaround is available.	RT: < 2 working days Response as for P2 incidents.	RT: Initial Response + < 10 working days Response as for P2 incidents.
P4 No Discernible Business Impact	All other types of issue including: • 'How-to' questions • Supply of documentation • Cosmetic changes to GUI, dashboards or reports.	RT: Best Endeavours Acknowledgment of receipt of Support Request and supply of Case Reference No. (if matter cannot be immediately resolved). Agree nature and timeframe for resolution of issue.	RT: Best Endeavours 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 11.

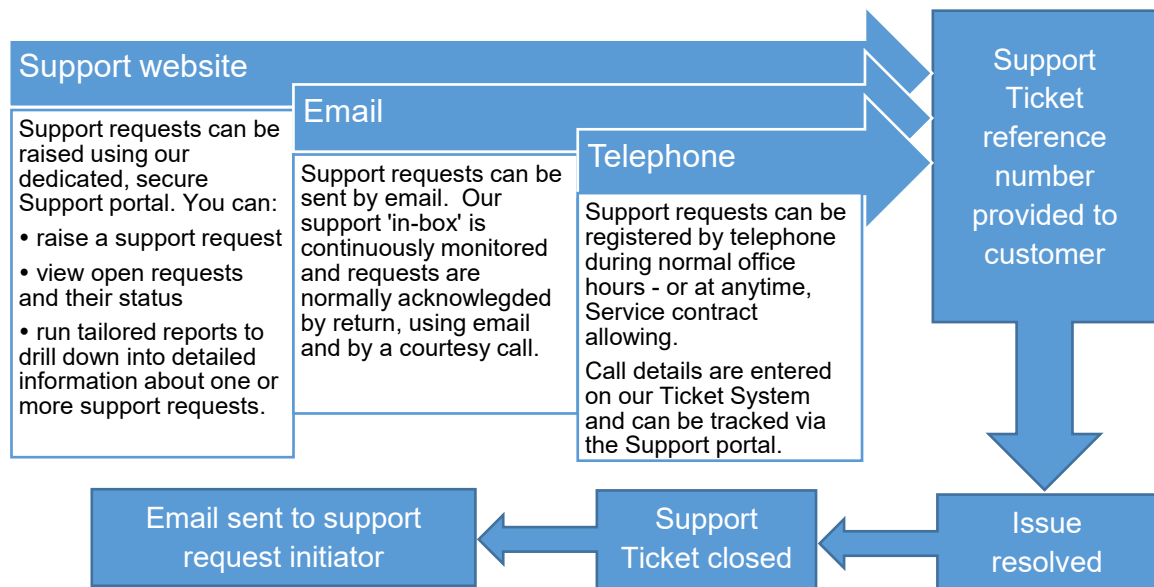


Figure 11: Raising Support Requests

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