

Coroner Case Management v15.0 service definition



Blackthorn

Contents

Introduction	2
Service Capability	4
Features and Benefits	12
eGRC Platform	13
Cloud Hosting	14
Service Architecture	14
Resilience	15
Protective Monitoring	15
Business Continuity	16
On-boarding	17
Service Provisioning Time	18
Service De-provisioning Time	18
Service Delivery	19
Off-Boarding	20
Response Times	22
Raising a Support Request	24
Terms & Conditions	25
About Us	26
Contact	26

Introduction

Our Coroner Case Management (CCM) solution is an on-premises or cloud-based application for coordinating the many facets of an investigation into unnatural or violent death. It enables collaboration allowing bereaved families, healthcare professionals, the police, registrars, pathologists, and other interested parties to directly input information and monitor progress and outcomes as appropriate. It supports the organisation of resources, both people and assets, and creation of processes allowing repeatable patterns of activity (workflow) to be defined and accomplished. Work activities, whether planned or ad-hoc, can be identified, delegated, monitored and reported on, giving the Coroner's Office staff full visibility of the many and varied threads of work and overall status of an investigation as it advances. Essentially, everything in one place needed to support an enquiry and achieve timely determination.

With national policy and guidance advocating larger coronial areas, technology is an important enabler helping ensure the delivery of a consistent and efficient service that meets the needs of a wide and diverse audience. This audience might include bereaved families, Coroner's Office staff, agencies, law enforcement and local and district councils. Technology can also provide a platform and necessary compliance controls for effective corporate and information governance. Blackthorn's Coroner Case Management system addresses these multiple needs by:

- centralising case information, evidence and reports, creating a single, explicit, point of reference
- providing access to context-based information adjusted to individual perspectives and needs i.e. Coroner's Office staff, police, pathologists, jury members etc.
- orchestrating the conduct of investigations, scheduling and allocating activities as pre-conditions and timelines necessitate
- prompting action immediately the conditions for advancement prevail
- automating the generation of forms and reports using supplied templates
- maintaining accountability and audit trail of actions, inputs, and decisions
- maintaining awareness through automated alerts and notifications.

Our case management software drives efficiencies and the achievement of positive outcomes by supporting all aspects of an investigation. This includes data capture, data management, decision making, tasking, tracking, document and form generation and internal/statutory reporting. Powerful workflow ensures effective alignment of operational processes and response strategies; customisable e-Forms simplify data capture; and a searchable, secure database ensures ease of access to case data (where there is authority). Configurable dashboards, with 'drill-down' functionality, ensure important information falls readily to hand, while automatic alerting and user action lists ("My-Tasks") make certain that effort is appropriately channelled, and investigations advance without undue delay. User access control underpins a multi-faceted governance model with the flexibility to ensure that the level of access to

case information is commensurate with the user's needs and authorisation, and that personal information in particular is handled and controlled in line with GDPR legislation.

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 tools and 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 solution and, consequently, the resulting user experience!

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

Our cloud services¹ 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 centres² that meet the accreditation and assurance requirements of data at OFFICIAL level (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.



¹ solutions delivered as an online, subscription service with SaaS modality.

² sovereign data centres meeting the specification of the Baseline Control Set (BSC) and recommendations of the UK Security Policy Framework.

Service Capability

The Blackthorn Croner Case Management system is a holistic solution supporting investigations or enquiries into the causes of death, where the reasons are unclear, or the death happened in detention or custody. It allows information to be quickly and easily assimilated from a wide variety of sources, the information to be analysed, and a determination made as to whether further scrutiny of events and causes of death are warranted. Where further investigation is required, individual actions can be assigned to the different parties contributing to the investigation, and their actions tracked through to successful completion. Support is provided to aid the organisation and conduct of inquests and to fulfil all mandatory reporting requirements.

The incorporation of a Referral portal ensures that external parties associated with a case, including the bereaved, witnesses, care professionals, pathologists etc., can enter or upload information in support of the enquiry, so avoiding the need for double keying, scanning or other nugatory administrative tasks that might otherwise fall to Coroner's Office staff. The portal provides a convenient window through which to view case information such as inquest dates and times or key conclusions, restricting access on the basis of *need-to-know*.

Extensive automation and support is provided to assist Coroner's Office staff (at all levels) with investigations, enquires and inquests. A calendar function makes the planning and scheduling of in-house and specialised external activities a straightforward task³, and the re-allocation of work between office staff just as easy. Strategic, operational and analytical dashboards, with drill-down, ensure users have immediate access to the information they require and can track at office, team or individual level the status of referral cases, investigations, staff workload, capacity etc. Powerful *workflow* and *tasking* functions make light the planning and coordination of process activities, while MS-Word templates aid the automatic generation of certificates, investigation reports and other mandatory output. Automated notifications and alerts provide users with early notice of time critical events and pending actions, with escalation to management if delays endure.

The standard operations supported by our Coroner Case Management system include, but are not limited to:

- referral of a death (via portal or conventional 'analogue' channels)
- allocation of case to a Coroner's officer
- no further action – permission by Coroner to issue MCCD
- disposal by way of form 100A ('A' certificate confirming investigation not required)

³ Interfaces with third party calendar functions such as Microsoft Outlook.

- decision on autopsy post-mortem examination and the type of examination i.e. Hospital Pathologist or Home Office, Forensic examination etc.
- decision on non-autopsy post-mortem examination of the deceased e.g. fingerprinting, forensic dentistry, anthropology etc.
- decision regarding toxicology, histology, tissue or organ retention
- decision regarding a second post-mortem examination
- decision regarding CT scanning or other imaging modalities
- disposal by way of form 100B (registrar notification of post-mortem without inquest)
- decision on timing of release of body for funeral
- decision supporting need for investigation
- allocation of case to a Coroner
- decision to discontinue an investigation
- decision to hold an inquest
- decision on use of experts and their engagement
- disclosure to interested persons (via portal or conventional channels)
- summoning of jury members and/or empanelling
- summoning of witnesses
- conclusion of inquest and preparation of Inquisition Report
- notifications, including to the Registrar
- issue of Preventing Future Death Reports
- decision on organ donation
- creation of standard reports/certificates auto completed with information from CCM.

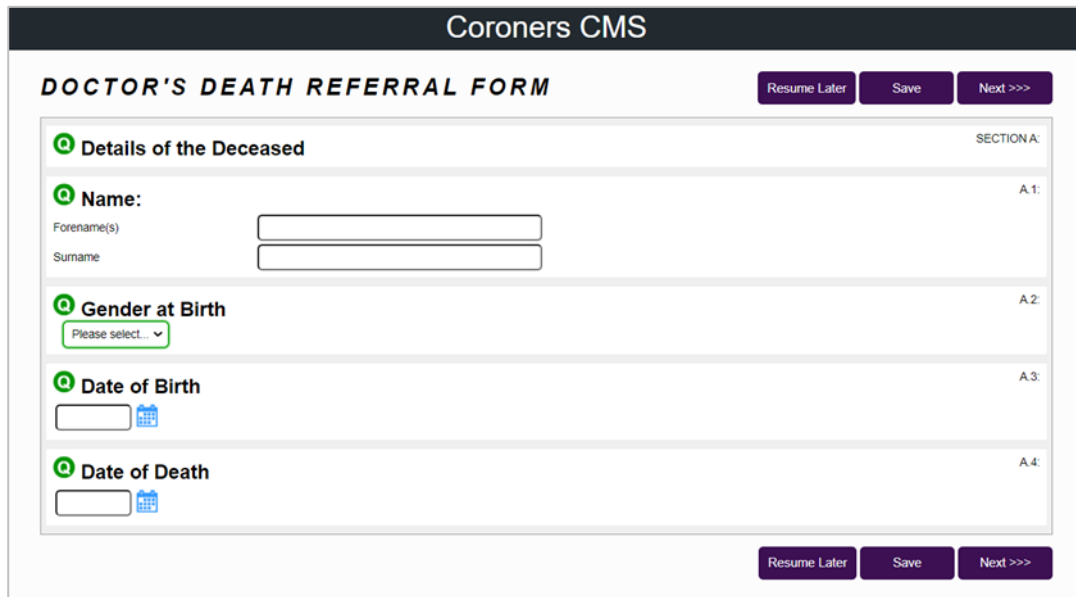
Although offered as a generic solution, our many years of experience of working with public and private sector organisations has taught us that no two Coroner's Offices are likely to have identical requirements and that some tailoring and/or customisation is inevitable. This might be due to the structure of the service and its integration with the City/County Councils or down to the need to integrate with a range of existing third-party systems e.g. finance. In either event, our data configurable software ensures that any additional bespoke coding is kept to a minimum and the gestation time between contract award and initial operating capability is measured in weeks rather than months.

The Blackthorn Coroner Case Management solution is based on a technology platform (cloud or on-premises) that incorporates the following features and capabilities:

a) Information Capture

Secure, high-fidelity e-Forms with embedded data validation and consistency checking help to eliminate mundane and error prone data entry. Our e-Forms

are context sensitive, only displaying the fields required for the operation in-hand. Documents, files, audio recordings, photos, 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.)



The screenshot shows the 'Coroners CMS' interface with a 'DOCTOR'S DEATH REFERRAL FORM'. The form is divided into sections, with 'SECTION A: Details of the Deceased' being the first. It contains four main input fields: 'Name' (with sub-fields for Forename(s) and Surname), 'Gender at Birth' (a dropdown menu), 'Date of Birth' (a date picker), and 'Date of Death' (a date picker). Each field is labeled with a green 'Q' icon. To the right of each field is a label: 'A.1:' for Name, 'A.2:' for Gender at Birth, 'A.3:' for Date of Birth, and 'A.4:' for Date of Death. At the top right of the form are buttons for 'Resume Later', 'Save', and 'Next >>>'. At the bottom right are similar buttons.

Figure 1: Death Referral e-Form (example)

b) Referral Portal

Extendable access gives the bereaved, healthcare professionals, the police, the ambulance service, registrars, pathologists, social care organisations, jurors and any other 3rd parties associated with a death/inquest the ability to add or retrieve information as required (access permissions allowing). This reduces administrative pressure on the Coroners' Office and duplication of effort where re-entry or scanning of information would otherwise be required. The referral portal is configurable to the specific needs of different user communities.

c) Records Management

Our 'Records Manager' function provides real-time access to case⁴ data, case documentation and other case attributes such as photos, court transcripts, inquest recordings, pathologist reports etc. uploaded to a case. A graphical interface supports the organisation of this data with subfolders for the classification of different types of case artifact. For example, witness statements can be grouped and appended to the court hearing to which they

⁴ tantamount to a 'folder' used to keep separate the records of individual enquiries and investigations.

pertain. There is no restriction on the file types that can be uploaded to a case.

Logical *associations* can be created between cases and the between records and artifacts across cases. For example, death records can be linked where a single catastrophic event has led to multiple deaths.

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

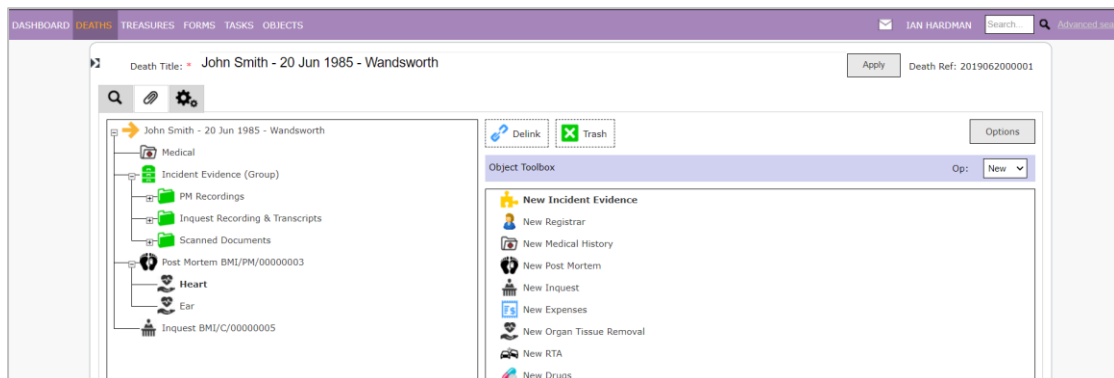


Figure 2: Associations & Filing

d) Case Record ‘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 ACM 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.

The Search function allows cases to be located by ‘name of deceased’ or other names linked to a case, such as aliases, family members, staff or agencies. Any attribute (data field) of a case can be used, or multiple attributes for a more targeted search.

e) Dashboards

‘At-a-glance’ access to key information and the insight needed to drive decisions. Operational dashboards provide managers and seniors with a snapshot of the status of operations and performance of the service. They provide case officers 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.

Filtering by case attribute, for example Case Officer, reported date, case status, age, cause of death, allows the ‘window’ onto case data to be narrowed and better focused. Filters can also be used for analytical reporting

and detailed trend analysis. Here, disposal, ethnicity, gender, postcode, cause of death etc. might be appropriate qualifiers.

All dashboards benefit from drill-down functionality and embedded hyperlinks providing access to successive tiers of information or the ability to navigate to other dashboards, case records, or CCM screens.

The CCM system is supplied with a range of standard, pre-configured dashboards which can be individually fine-tuned using filters and personal preferences. Custom dashboards can also be created (permissions allowing) and constructed to meet specific, individual needs. A graphical interface and a range of standard widgets (standard dashboard components) is available for this purpose. Custom dashboards can be configured for personal (i.e. private) use or published to benefit the wider team.

f) Forms and Reports

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

g) Data Extraction

Data export (in either .xlsx or .csv file formats) is supported by a 'wizard' giving the user 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 CCM system. The wizard also provides the ability to navigate around dynamic database structures and content.

h) Tasking & Workflow

Workflow allows a set of actions with a defined outcome to be defined, organised and accomplished in prearranged order. In the course of an investigation there are a multitude of 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, 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.

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 unique needs of an individual case. Work activities and tasks can be

dynamically assigned to Coroner's Office staff or a wider group. Tracking tools provide full 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.

i) Case Allocation

Case records have a number of attributes that are used solely by the CCM system. The 'Pool' attribute allows cases to be segregated into sub-groups, each sub-group being visible to a specific user community. The most obvious benefit of pools is the ability to establish Chinese walls between Coroner's

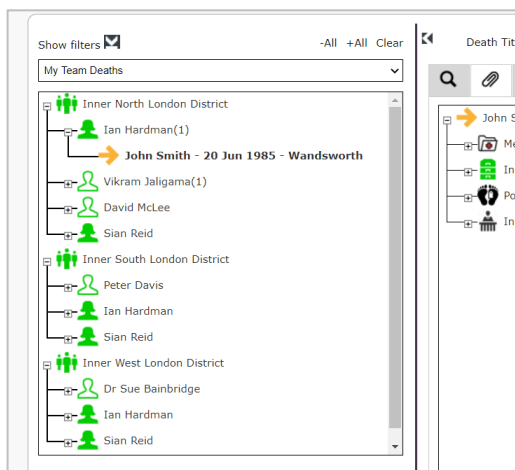


Figure 3: Workload

Office jurisdictions where there are two or more jurisdictions within a given area. Pools can also be used to silo teams and restrict visibility of cases within an office – again, where there is a genuine business reason to do so. Conversely, Pools can be used to extend access by giving users access to more than one sub-group. This might be appropriate where a Coroner Office needs access to one or more cases belonging to an adjacent district.

Pools also allow new cases to be initially allocated to an 'unassigned' category. This is especially useful if created by an external agency via the Referral Portal. Unassigned cases can be triaged by an authorised member of Coroner's Office staff and manually assigned to the Case Officer best placed to assist. Where the allocation is based on case workload, an individual's workload can be reviewed via dedicated 'My-Task' screens or a dashboard (see Dashboards above).

j) Alerting and Notification

Multiple channels are available for alerting and notification. Dashboards provide Case Officers with details of actionable tasks awaiting attention. The task list can be case centric or list actionable tasks from all cases assigned to the officer. Email alerts and notifications can be triggered manually or by workflow, raising awareness without the need to log-on. This is particularly helpful if the recipient is an infrequent user or external agency or service without a CCM account.

Key information about critical dates and actions can also be disseminated via the Referral Portal. For example, jurors can be notified of court dates or witnesses about statement submission cut-off dates.

k) Collaboration and Accountability

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 to an 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.

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) Remote working

As case records are centralised, online access to the web server is required to coordinate and manage investigations. Where this access is over the internet, security policies can be set allowing case officers to work remotely away from recognised office locations. If access to the hosting environment is over a secure network such as the PSN, RLI or HSCN, users able to access the Coroner's Office network remotely (i.e. via a VPN bridge) will be able to access the CCM service via the same route.

Our iOS, Android and Windows Apps allow certain case management functions to be conducted off-line; the App and Webserver synchronising once network access is re-established.

n) e-Signatures

The authenticity of documents and emails can be assured using digital certificates to verify that an object has not been intentionally or unintentionally modified since signing. This feature, together with strong database security, ensures that exported information is trustworthy and also admissible in court.

Integration with DocuSign® provides an alternative method of proving the provenance of documents and a means of enabling 3rd- parties to attest to the authenticity of content uploaded to the system.

o) Interoperability

A library of pre-existing web services (Open API compliant and RESTful⁵) are available for standard interfacing needs. OLEDB services are available allowing direct interaction with our data storage service. Additionally, data can be exchanged digitally via email - both inbound and outbound. This has many advantages as SMTP⁶, the vehicle enabling email, is ubiquitous, making it a very open and accessible channel for information exchange.

⁵ 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.

⁶ Secure Mail Transfer Protocol

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.

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. Investigation Case Management. 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.

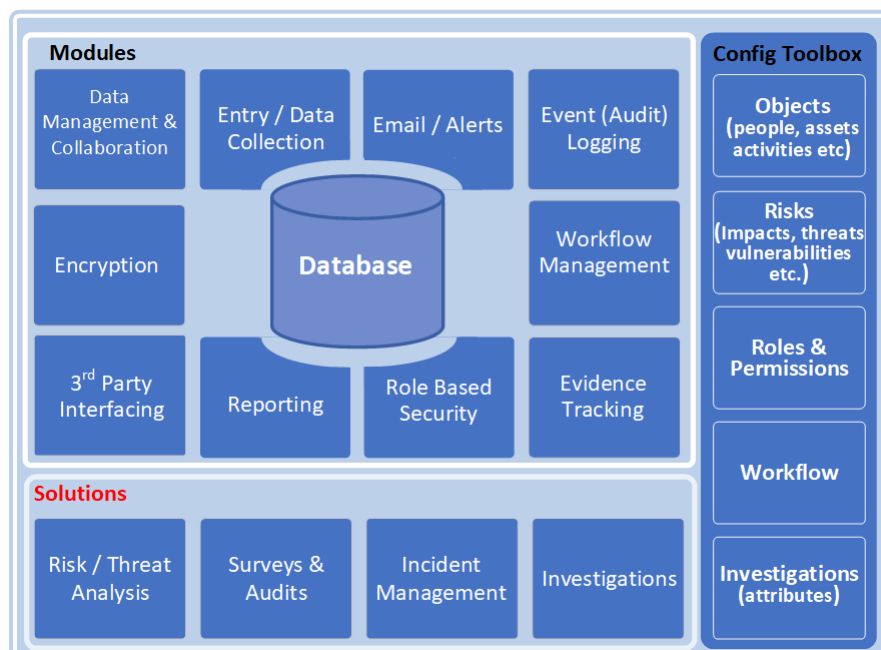


Figure 4: eGRC Platform Architecture

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 Internet Explorer IE9 and IE11 (IE8 if there is a genuine necessity), Firefox and Chrome. 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 Coroner 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 to only you, and any other parties you so authorise.

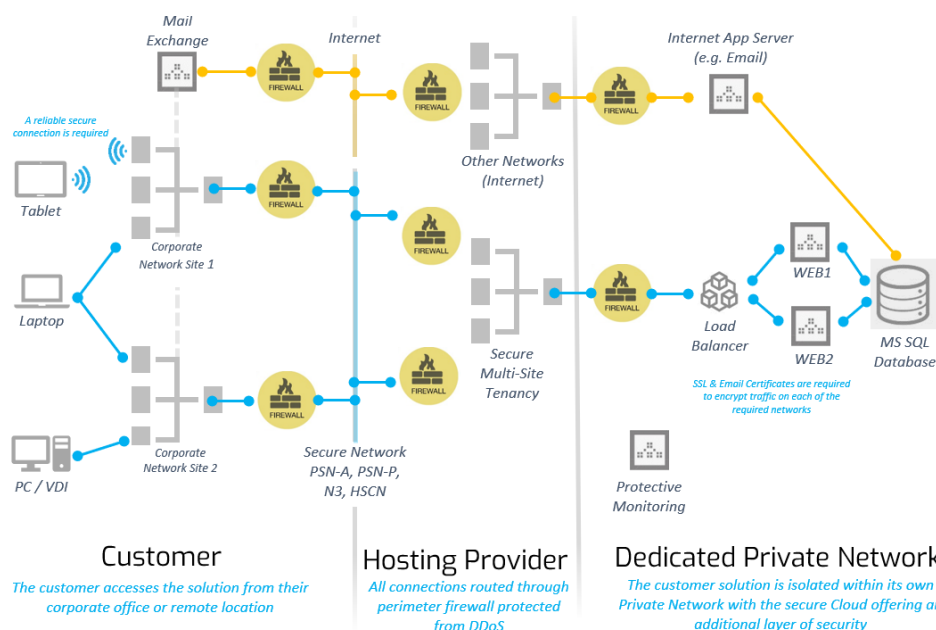


Figure 5: Dual Web Server suitable for hosting Official Sensitive Information

Our standard Government hosting solution (figure 5) 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, N3) and meet all Government code-of-conduct requirements. An air-gapped connection to an internet facing Application Service provides options for email over internet (GDS preference), reducing the demand on the extant, secure wide area networks. Dual

webservers behind a load balancer provide the capacity to handle large volumes of HTTPS traffic but this configuration is obviously scalable, both up and down.

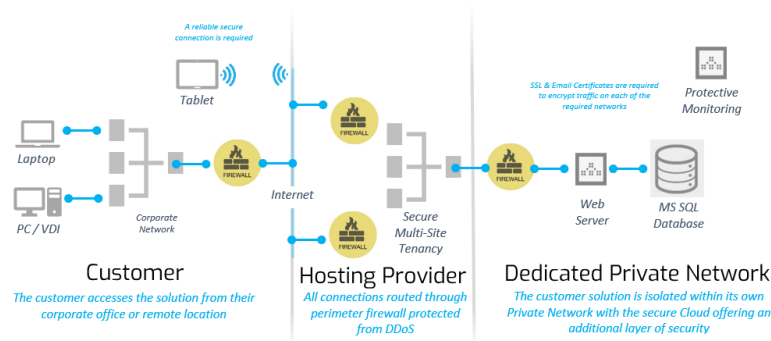


Figure 6: Single Web Server suitable for hosting Commercial Information

Where data security targets are less demanding, we can provide hosting with a commercial hosting provider (figure 6). The service is accessed over the internet with channel and database encryption as required. Figure 6 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 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.

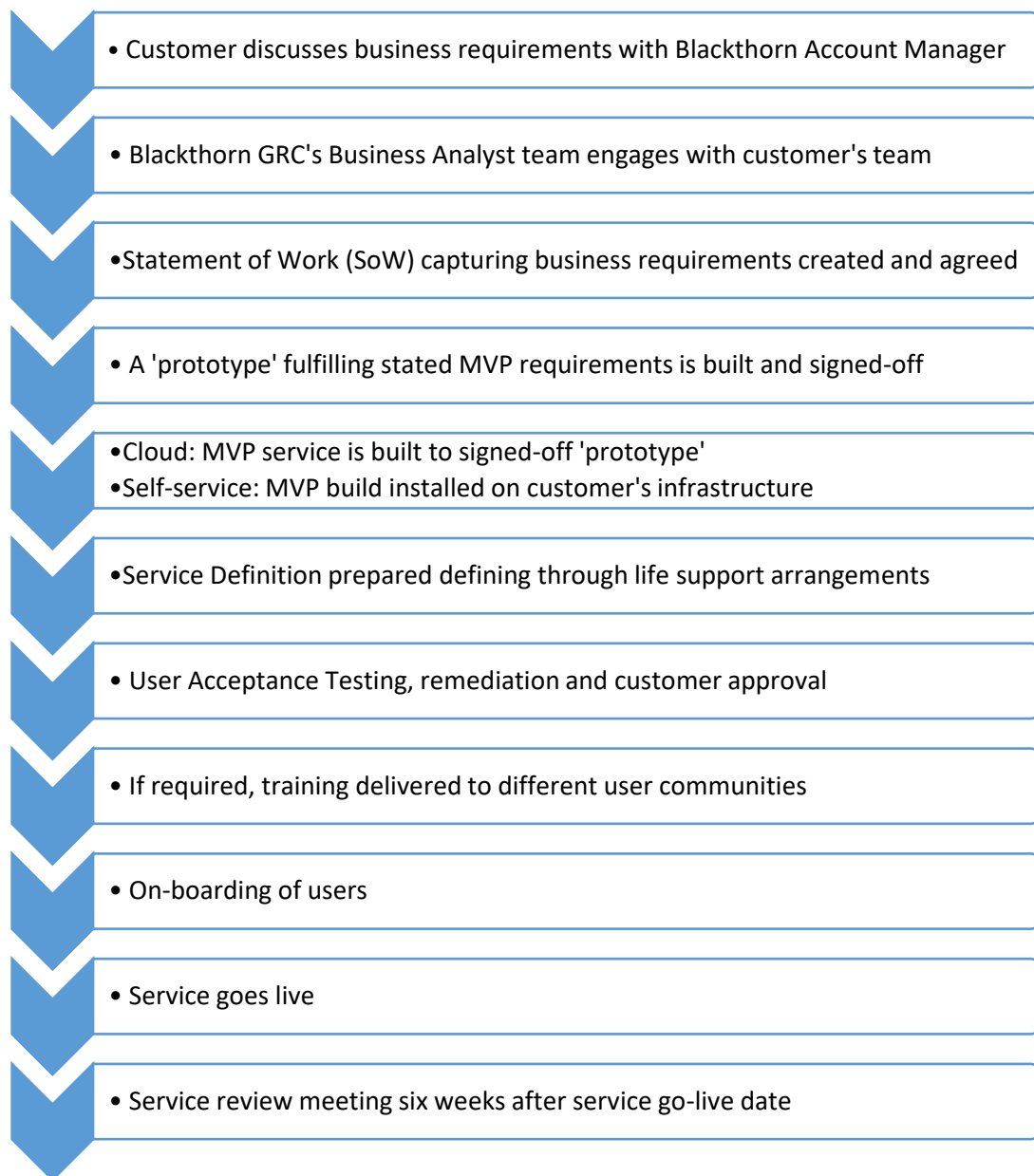


Figure 7: On-boarding stages

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 7 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:

- contact points
- escalation processes
- support arrangements:
 - Incident Management
 - Problem Management
 - Change Management

- Service Desk response SLAs
- reporting frequency
- 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.

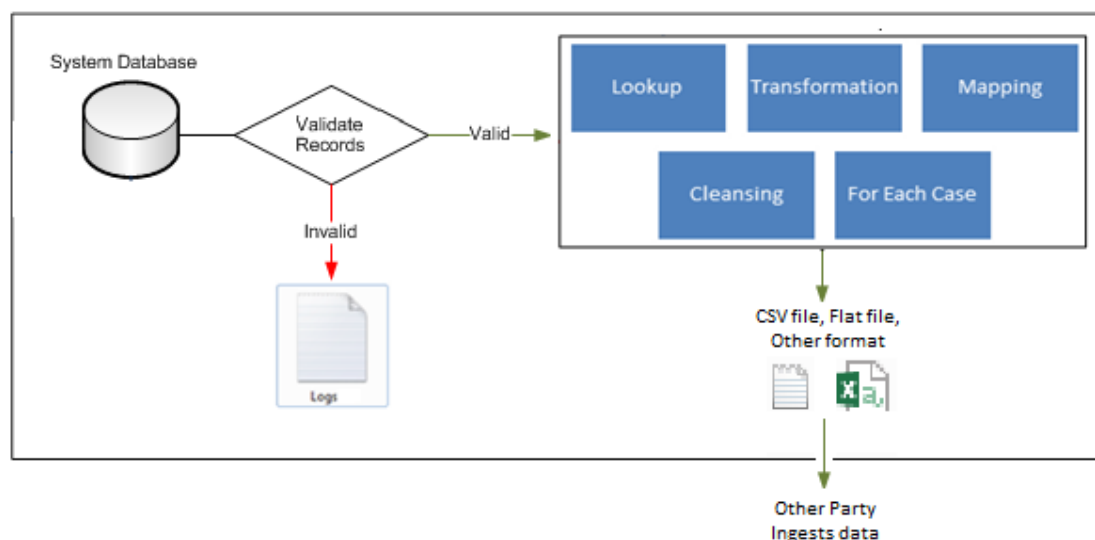


Figure 8: Data migration process

The data migrating process could involve:

- extracting all textual data to a 'flat' or .csv file of agreed format, the file acting as the interface between the two systems, or
- 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 8 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	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	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.

	medium to longer term consequences. 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.	provides a stop-gap solution, this will be proposed. 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 9.

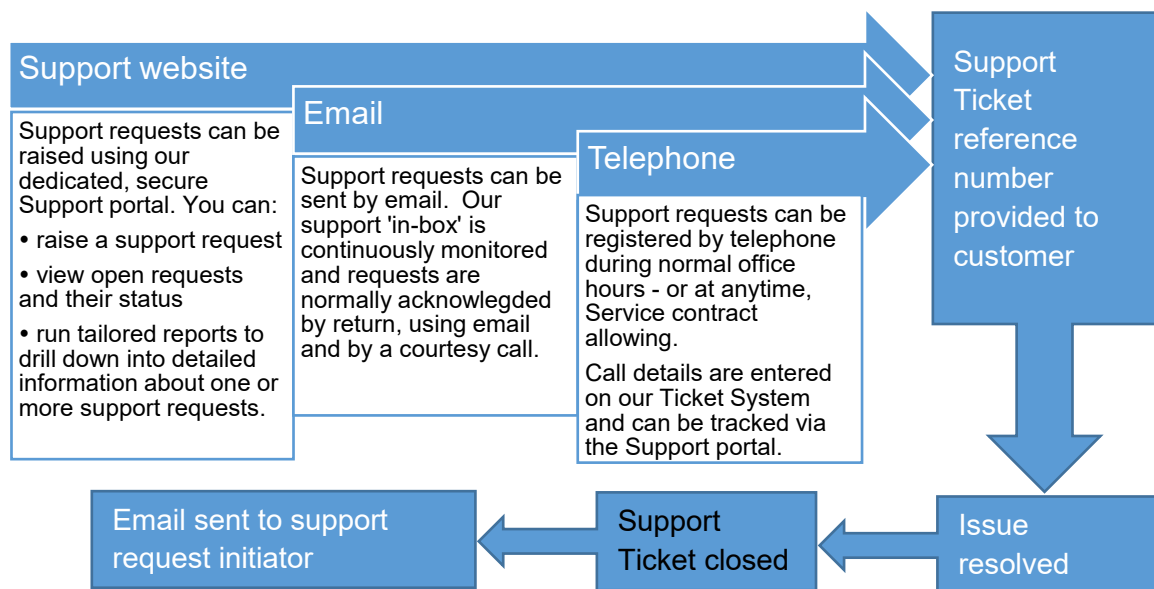


Figure 9: Raising Support Requests

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