Background Screening Case Management v15.0

service definition

G-Cloud

IS 721821

Blackthorn

Contents

Introduction 2
Service Capability 6
Features and Benefits 15
eGRC Platform 16
Cloud Hosting 17
Service Architecture 17
Resilience 18
Protective Monitoring 18
Business Continuity 19
On-boarding 20
Service Provisioning Time 21
Service De-provisioning Time 21
Service Delivery 22
Off-Boarding 23
Response Times 25
Raising a Support Request 27
Terms & Conditions 28
About Us 29
Contact 29

Introduction

Our Background Screening Case Management (BCM) tool is a cloud-based solution for orchestrating due diligence either pre-employment or prior to granting positions of substantial authority. It is equally suitable for ongoing screening where there is a need for frequent and repeated background checks of employees in high-risk roles.

Across industry there is a growing awareness of the importance of background screening as a means of verifying a person is who they claim to be and ensuring that prospective recruits have the competence and capability to fulfil the role into which they are being hired. Regulatory and compliance drivers are also dictating that businesses invest considerable effort in screening individuals for evidence of past illegal or material misconduct. This is especially true in leadership roles holding power and authority as employers needs assurance that role holders are worthy of such trust.

Despite its intrinsic worth, background screening remains an incredibly complex activity and can throw up numerous challenges due to the many different combinations of check required, and mechanics of a screening process which can give rise to numerous concurrent leads of enquiry. Any, or all, of these leads are susceptible to *dilution* or *loss* in the fog of follow-up communication, leading to delay and inconclusive outcomes.

The Blackthorn Background Screening Case Management system provides a framework for ensuring investigations follow a considered and optimised plan, proportionate and relevant to the role in question. It ensures consistency across checks of a similar type and underpins the *hire* or *promote* decision by capturing the information needed to inform such decisions. It does this while also demonstrating fairness and objectivity in the execution of such judgements. The BCM system frees up time and resources by delegating responsibility for tasks to those best placed to accomplish, and by minimising the administrative burden associated with the collection, organisation and analysis of data, evidence and other inputs to a case. System generated reports further ease the level of administrative overhead.

Our BCM system can be used to assess whether a potential hire is fit for the purpose of employment, whether access to secret data possess significant risk, to inform decisions on the award of potential loans, or any other assessment of an individual's good standing. There are many types of due diligence check that can be conducted, with employers using a mix of those to fulfil a broader background screening requirement. Some more common types of due diligence check are:

- Identity check
- Past employment history
- Criminal record check
- Right to work
- Past employer(s) referencing
- Education and credential verification including career gap period checks.

- Character references
- Financial history check such as credit rating or County Court Judgments
- Media and social media searches.

A pre-employment check might require all of the above due diligence checks in contrast, a BPSS[1] check only requires identity, employment history, criminal records and Right to Work checks. The BCM system establishes the mix of due diligence checks required for a given background screening activity type, treating each check as a mini project requiring careful and considered orchestration to meet the overall screening objective.

As an investigation and assurance tool for regulated industries such as finance, government and aviation, pre-employment checks might include Public Safety Verification checks to screen for terrorist involvement or activity. Regulated industries typically operate under the auspices of strong compliance and ethics programmes and here too the BCM has a role in FCA[2] Level 1 and Level 2 assessment, PCI compliance screening and Sanction Searches used to weed out individuals suspected of illegal activity (denying them leadership positions from where they could continue such activity with impunity). Similarly, the BCM has a role in coordinating activities connected with security vetting staff earmarked for sensitive roles and as a platform for managing and coordinating investigations delivered externally as a third-party service.

The benefits delivered by Background Screening Case Manager include:

- optimised performance with process automation to guide investigators through the multiple stages of screening.
- consistent handling of cases aligned to pre-approved screening strategies.
- real-time reporting of project (case) status to management and investigators
- key information elevated to forefront for improved situational awareness, insight, and decision-making.
- improved candidate engagement and data capture courtesy of online portal
- logical and structured organisation of investigation (case) data with graphical interface for ease of navigation, storage and definition of relationships and dependencies
- time saved freeing up resources to focus on compliance & regulatory matters.
- calendar function to visualise, plan, manage and coordinate investigation activities such as candidate interviews.
- improved awareness of targets, deadlines and the ‘need-for-action’ to progress an investigation.
- flexible reporting including system generated documents and forms.

[1] UK Government Baseline Personnel Security Standard

[2] Financial Conduct Authority

- digital signature capability for approval of documents
- GDPR compliant data handling
- highly scalable with global reach.

Our Background Screening Case Management platform enables collaboration by allowing investigators, candidates and stakeholders (business functions) to move through the multiple stages of screening quickly and easily, and to monitor progress and outcomes as appropriate. It supports the organisation of resources, both people and assets[3], and the creation of processes (repeatable patterns of activity) ensuring that investigations are consistent in both of scope and quality.

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!

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

Our cloud services[4] are delivered on scalable, secure infrastructure with the flexibility to deliver optimum performance at minimum cost. Customers can choose, based on risk appetite, between UK sovereign data centres[5] that meet the accreditation and assurance requirements of data at OFFICIAL (as per the Government's Security Classification), less expensive commercial cloud-hosting, or something in between.

---

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

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

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

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.

Service Capability

The Blackthorn Background Screening Case Management system provides enterprise-level capability for conducting investigations into a person's recent history and independent verification of their education, skills, experience, conduct, and honesty. In doing so, an individual's suitability for hire, promotion, or retention in a leadership role can be established. The system supports the many flavours of background screening from *pre-employment* to *privileged* and *executive*, centralising operations and ensuring efficiency, fairness and consistency no matter the specifics or nature of the screening activity. It imposes discipline and structure on the conduct of investigations, guiding officers through the necessary elements and facets of the checks (e.g. criminal records, Right to Work, security) that together meet the overall screening requirement. It ensures that actions, whether part of the data collection (1st and/or 2nd parties), data analysis, follow-up or preparation of recommendation, are properly managed and controlled. It monitors progress against anticipated timelines, drawing attention to potential slippage and alerting management if lateness endures.

Users have full visibility of their investigation projects and the ability to assimilate information from multiple 'points-of-view' for enhanced situational awareness and ultimately, improved decision making. Candidates, both internal and external, can have online access to the BCM system via temporary user accounts, however access can be further extended to business users and stakeholders, third-parties or other agencies, for improved engagement and/or to facilitate information exchange. For example, if providing a bureau service, government departments (as the customer) might benefit from an online portal providing them with the ability to nominate candidates for review and/or track the progress of screening projects.

A centralised database and Role Based Access Control (RBAC) ensures information is only reachable by those with authority and genuine need, while automatic logging of user and system-initiated actions ensures accountability, acting also as a deterrent against improper behaviour. Data control and logging safeguards the privacy of screening records including Personally Identifiable Information (PII). Data privacy and control is integrated into a Records Management capability that is fully compliant with UK DPA[6] and GDPR[7] requirements.

The BCM system comes pre-configured with the all forms and reports needed to support most types of pre-employment and through-employment screening. A library of standard, tailor-made, and user-defined (i.e. customer built) reports and form templates is provided.

Now, it is not uncommon for a potential hire to have been raised, educated, and worked in several different countries. As a consequence, pre-employment screening has become more complex with related enquires extending overseas. With this in

[6] Data Protection Act, 2018.

[7] General Data Protection Regulation 2016/679, effective May 2018.

mind, the BCM system has been designed to work across time-zones and is supplied with multi-currency and multi-lingual options.

Our recently introduced Mobile App[8] (cost option) allows specific elements of an investigation to 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 activities (e.g. interview reports, follow-up actions, recommendations) uploaded when permanent access to the central BCM 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 HR, Compliance or wider investigations team just as easy. Automated notifications and alerts raise awareness of new and pending actions, up-and-coming targets and critical deadlines. An integrated email handling capability provides a conduit for alerts and meets a wider candidate, investigator, third-party communication need.

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

- assign background screening cases to an investigating officer
- plan and schedule employment screening activities that need to be repeated (annually) to meet compliance obligations
- harvest (online) information from candidate using supplied or self-created (customised) eForms and/or surveys (a.k.a. digital forms)
- harvest (online) due diligence from 3rd-parties (e.g. past employers) using supplied or self-created (customised) eForms and/or surveys (a.k.a. digital forms)
- collect due diligence from candidate or 3rd-party via email
- upload and store files, pictures or documents associated with a screening activity
- review and evaluate candidate information, operational data, due diligence etc., record conclusions and formalise follow-up actions
- track and report on personal, team and office workload
- lay down, in advance, workflows (repeatable patterns of activity) defining the incremental steps to fulfil a given background screening activity types e.g. pre-employment, BPSS, executive
- modify and adapt standard (supplied) workflows to accommodate specific (unique) screening requirements
- work across time-zones with multi-currency and multi-lingual options
- access key information and insight using strategic, operational and analytical dashboards

[8] iOS, Android and Windows devices supported.

- create bespoke dashboards and customise supplied dashboards
- access the information behind the information using drill-down and hyperlinks (dashboards)
- automatically create documents and reports based on standard templates (maintained in library)
- add subjective content to auto-generated documents, forms and reports
- maintain a library of HR employment reference materials including regulations, internal policy, and guidelines
- create notifications and email alerts to raise awareness, prompt action, escalate issues
- interface with third-party system to automate data collection/exchange or triggers associated processes.

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

All variants of our Background Screening 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 and surveys with embedded data validation and consistency checking help to eliminate mundane and error prone data entry. Our eForms are context sensitive, only displaying the fields required for the operation in-hand. Option to make survey questions *conditional* (on earlier answers) and therefore to constructed navigable, dynamic question sets. Documents, files, audio recordings, scanned papers etc. can be emailed to the system and automatically added to a case. Web services allow data transfer (input and output) to other digitally enabled, online systems, again reducing the necessity for manual data entry (see Interoperability below).

Figure 1: Candidate Screening Survey Launch Pad

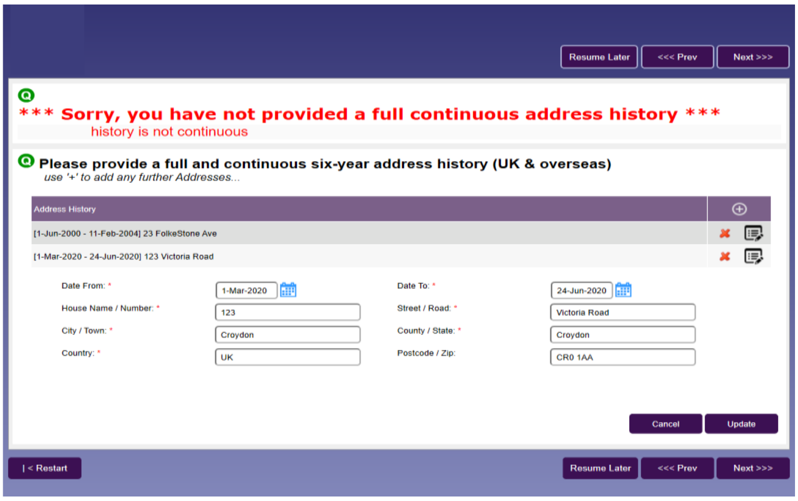

Figure 2: Address History e-Form

b) Records Management

Our 'Records Manager' function provides real-time access to investigation records, including artifacts such as documents, evidence, certificates, statements, photos, recordings etc. associated with a case. 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 subfolder under a case[9]. There is no restriction on the file types that can be uploaded and appended to a case.

[9] tantamount to a 'folder' used to keep separate the records of individual inspections, audits, and incidents.

Logical *associations* can be created between cases and the between records and artifacts across cases. For example, cases created as containers for individual safety incidents could be linked if they share a common cause.

System 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 BCM 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 stakeholders with a snapshot of the status of operations and screening capacity. They provide the investigation officers with fast changing information about their cases, assessments, workload, actionable tasks, overdue activities etc.

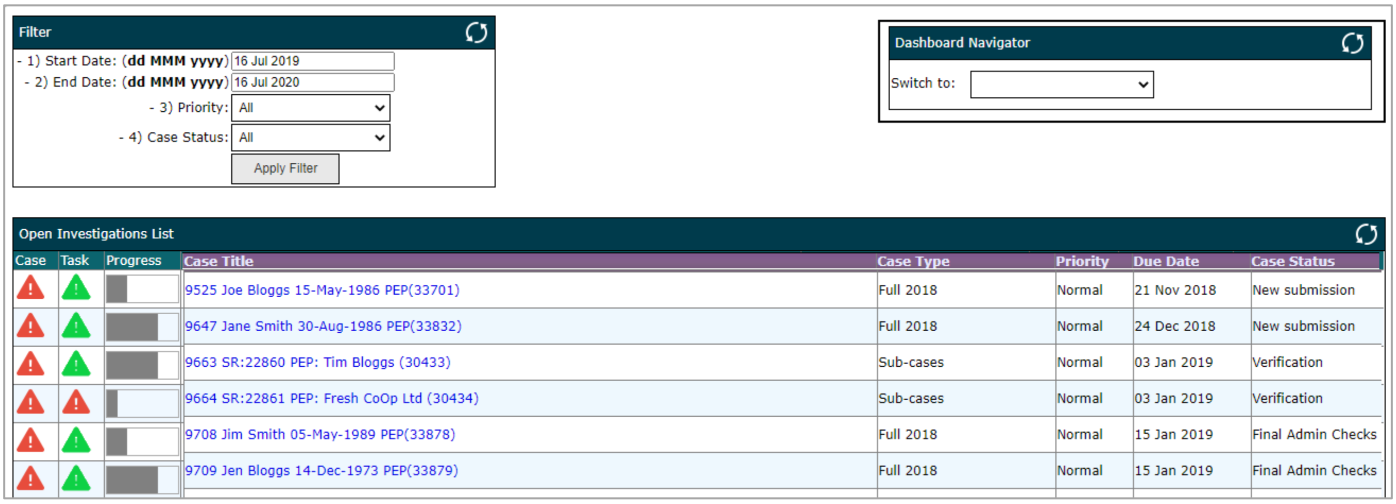

Figure 3: Case Status Dashboard

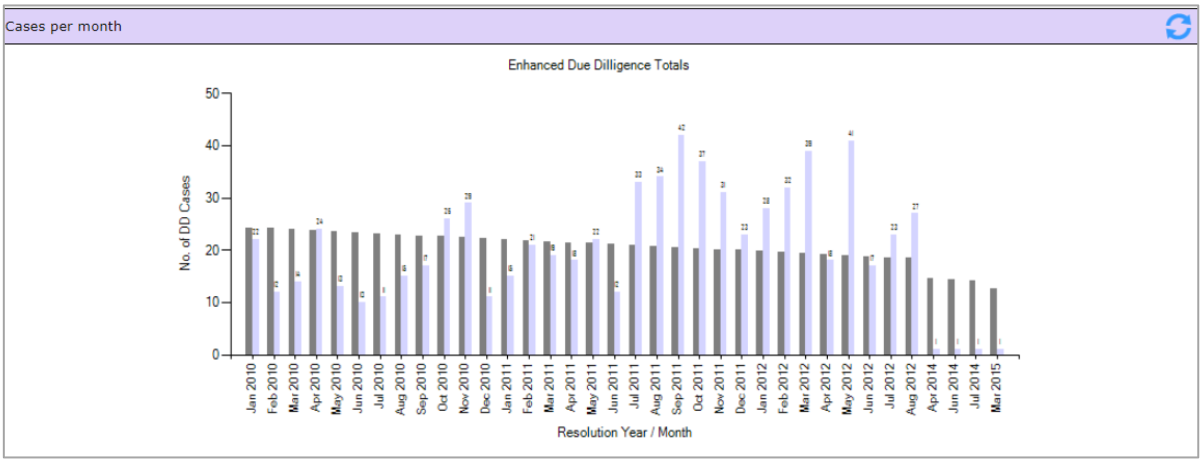

Figure 4: Case Volumes by month

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 figures 3 and 4 above.

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

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

e) Forms and Reports

Tool support 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.

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 BCM 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. In the course of an inspection, audit, incident or investigation 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.

Remediation Tasks

Task Name	ManageTask	Task Owner	Task Created date	Associated Investigation	Status	Task Due Date
Booth and air to be tested		Nigel Adcock	18 Oct 2019	1261 Accident / Incident Reporting - 16 Oct 2019 (Jones)		21 Oct 2019
Training PPE		Jane Smith	18 Oct 2019	1261 Accident / Incident Reporting - 16 Oct 2019 (Jones)		16 Jul 2020
Supervision/monitoring		Joe Bloggs	18 Oct 2019	1261 Accident / Incident Reporting - 16 Oct 2019 (Jones)		25 Oct 2020
Partner appointed to review		Nigel Adcock	18 Oct 2019	1261 Accident / Incident Reporting - 16 Oct 2019 (Jones)		27 Oct 2021
Rearrange and Rebuild certain areas of scaffolding		Nigel Adcock	21 Oct 2019	1263 Accident / Incident Reporting - 18 Oct 2019 (Jones)		16 Jul 2020
Replace hooks, block or fitting that is rusted, cracked, or damaged		Vikram Jaligama	21 Oct 2019	1263 Accident / Incident Reporting - 18 Oct 2019 (Jones)		21 Nov 2019
Ensure all workers have site inductions		Jane Smith	21 Oct 2019	1263 Accident / Incident Reporting - 18 Oct 2019 (Jones)		28 Oct 2019
Replace interlock switch with tongue type switch		Joe Bloggs	21 Oct 2019	1249 Accident / Incident Reporting - 9 Oct 2019 (Adcock)		18 Oct 2019
Rearrange machine to allow access to window		Jane Smith	21 Oct 2019	1249 Accident / Incident Reporting - 9 Oct 2019 (Adcock)		18 Oct 2019
Service Lift		Vikram Jaligama	22 Oct 2019	1292 H&S Accident / Incident Report - 22 Oct 2019 (Hardman)		22 Oct 2019
Risk Assessment			22 Oct 2019	1292 H&S Accident / Incident Report - 22 Oct 2019 (Hardman)		24 Oct 2019

Figure 5: Tasks Status Dashboard

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 a case. Work activities and tasks can be dynamically assigned to HR / Compliance staff or a wider group. Tracking tools provide fully visibility of the status of tasks, including child tasks, highlighting lateness and/or overrun.

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

h) Case Allocation

Case records have a number of attributes that are used solely by the BCM 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 different Background Screening teams, different offices or locations or different disciplines (i.e. HR, Compliance etc.) where the BCM system is servicing the needs of more than one department. Pools can also be used to silo teams and restrict visibility of cases within a team or department – again, where there is a genuine business reason to do so.

Pools also allow new cases to be initially allocated to an ‘unassigned’ category. This is especially useful if the request for background screening is generated externally, possibly by an affiliate or international office, and until triaged (reviewed) will be without a formal owner (investigating officer).

i) Alerting and Notification

Multiple channels are available for alerting and notification. Dashboards provide investigating officers 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 users, and whilst requiring the recipient to have a BCM account, does offer the advantage of keeping the content of the communication within the confines of the system (avoid possibility of any data leakage or creep).

j) 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.

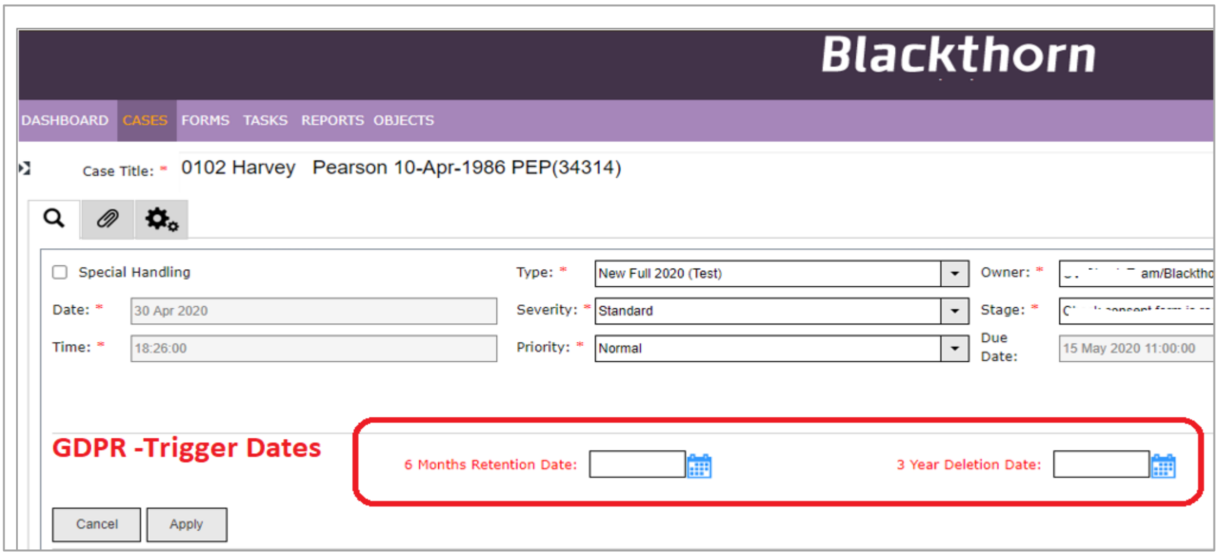

Figure 6: Setting data deletion trigger dates

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).

k) 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.

l) Interoperability

A library of pre-existing web services (Open API compliant and RESTful[10]) 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

[10] 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.

many advantages as SMTP[11], the vehicle enabling email, is ubiquitous, making it a very open and accessible channel for information exchange.

Features and Benefits

Features	Benefits
• Built on core modules • Easily extendable and customisable • Intuitive, clear user interface • User configured reports and dashboards: information you need at your fingertips • Drill-down; detail accessible but not at expense of clarity • Workflow to ensure methodical and repeatable execution • Build automated PDF and Emails • Tools for assigning, managing and reporting on requests • Sophisticated role based access control to ensure secure partitioning of information	• Easy identification of workload of requests across the organisation • Optimised time management with workflow, task assignment and user alerting • Build PDF reports to HR automatically • Send status update emails to department to ensure they kept informed • Full audit trail; users fully accountable for their actions • Segregation of case information ensuring personal information is only reviewed by appropriate personnel • Special handling for highly sensitive employees • Secure storage of data with channel encryption on remote links • Clean, intuitive user interface reducing any training requirements • Wide range of supported platforms e.g. tablet, laptop, desktop

[11] 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. Health and Safety Assessments, Skills and Competencies Survey 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

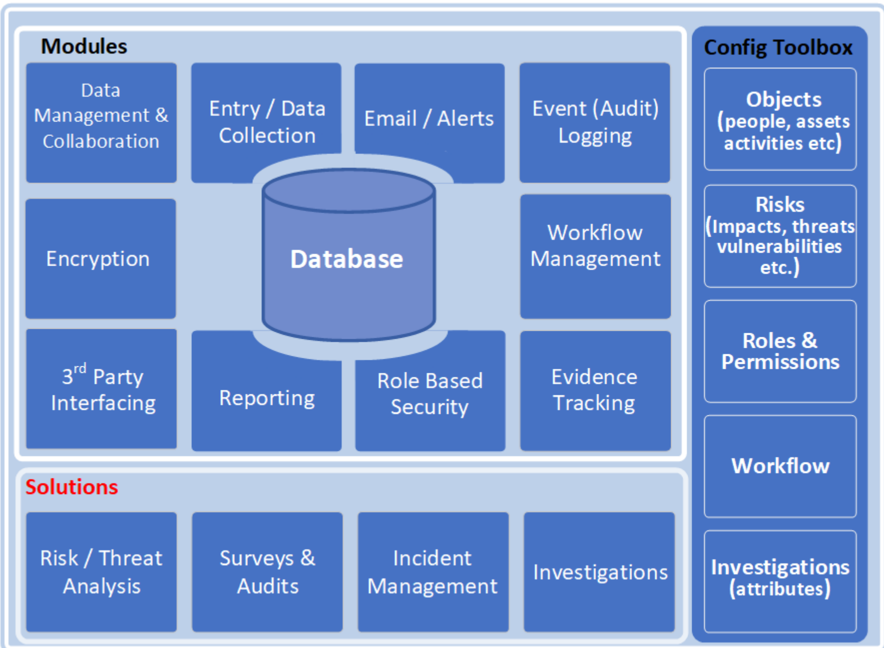

Figure 7: eGRC Platform Architecture

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

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

Cloud Hosting

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

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

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

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

Service Architecture

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

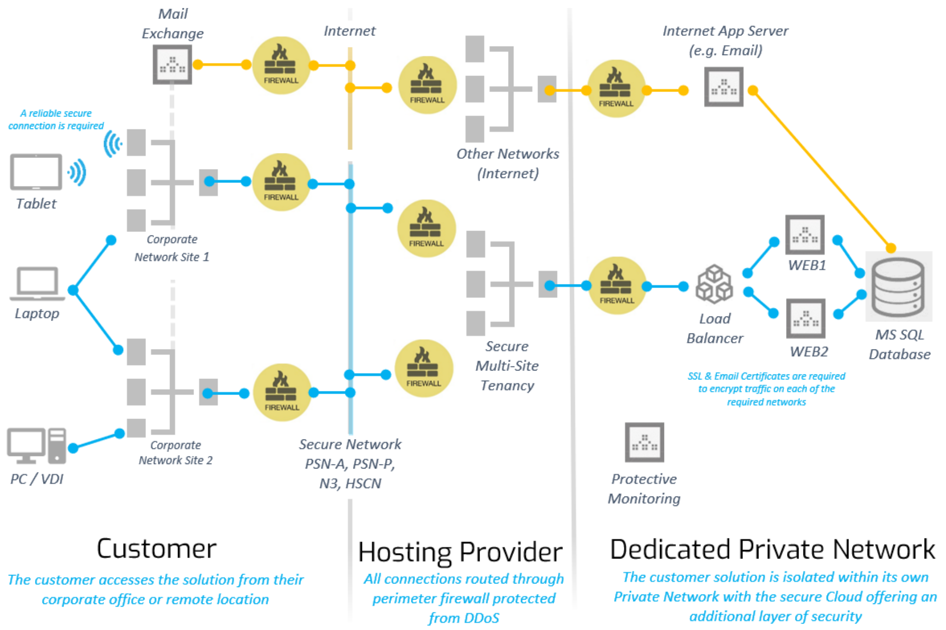

Figure 8: Dual Web Server suitable for hosting Official Sensitive Information

Our standard Government hosting solution (figure 8) leverages data centres meeting the accreditation and assurance requirements of data at OFFICIAL. They are reached via secure corporate and wide area networks (e.g. PSN, HSCN) and meet all Government code-of-connection requirements. An air-gapped connection to an internet facing application service provides options for email over internet (GDS preference), reducing the demand on the Government's wide area networks. Duel webservers behind a load balancer provide the capacity to handle large quantities of HTTPS traffic but this configuration is obviously scalable, both up and down.

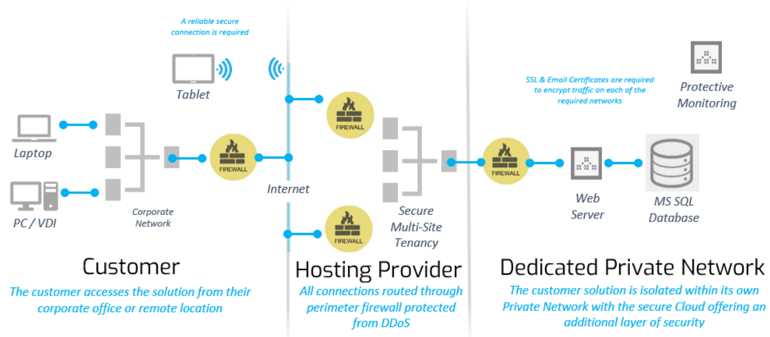

Figure 9: Single Web Server suitable for hosting Commercial Information

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

Resilience

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

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

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

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

Protective Monitoring

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

- Customer discusses business requirements with Blackthorn Account Manager
- Blackthorn GRC's Business Analyst team engages with custiomer's team
- Statement of Work (SoW) capturing business requirements created and agreed
- A 'prototype' fulfilling stated MVP requirements is built and signed-off
- Cloud: MVP service is built to signed-off 'prototype'
- Self-service: MVP build installed on customer's infrastructure
- Service Definition prepared defining through life support arrangements
- User Acceptance Testing, remediation and customer approval
- If required, training delivered to different user communities
- On-boarding of users
- Service goes live
- Service review meeting six weeks after service go-live date

Figure 10: On-boarding stages

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

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

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

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

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

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

Service Provisioning Time

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

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

Service De-provisioning Time

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

Service Delivery

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

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

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

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

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

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

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

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

a. contact points
b. escalation processes
c. support arrangements
    - Incident Management
    - Problem Management
    - Change Management
d. Service Desk response SLAs

e. reporting frequency
f. meeting schedules.

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

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

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

Off-Boarding

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

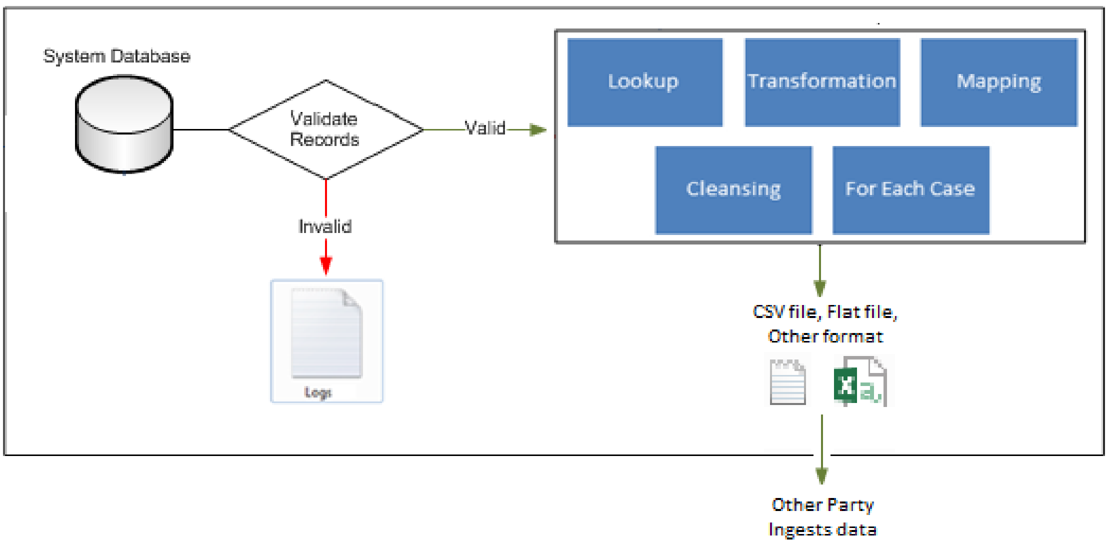

Figure 11: Data migration process

The data migrating process could involve:

Blackthorn

g. extracting all textual data to a ‘flat’ or .csv file of agreed format, the file acting as the interface between the two systems, or
h. writing bespoke scripts and processes to manage the migration and to commute data (including non-textual items such as photos) direct from the old to new system.

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

Figure 11 illustrates the process at high level.

Response Times

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

Priority	Description	Initial Response	Resolution
P1 **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 12.

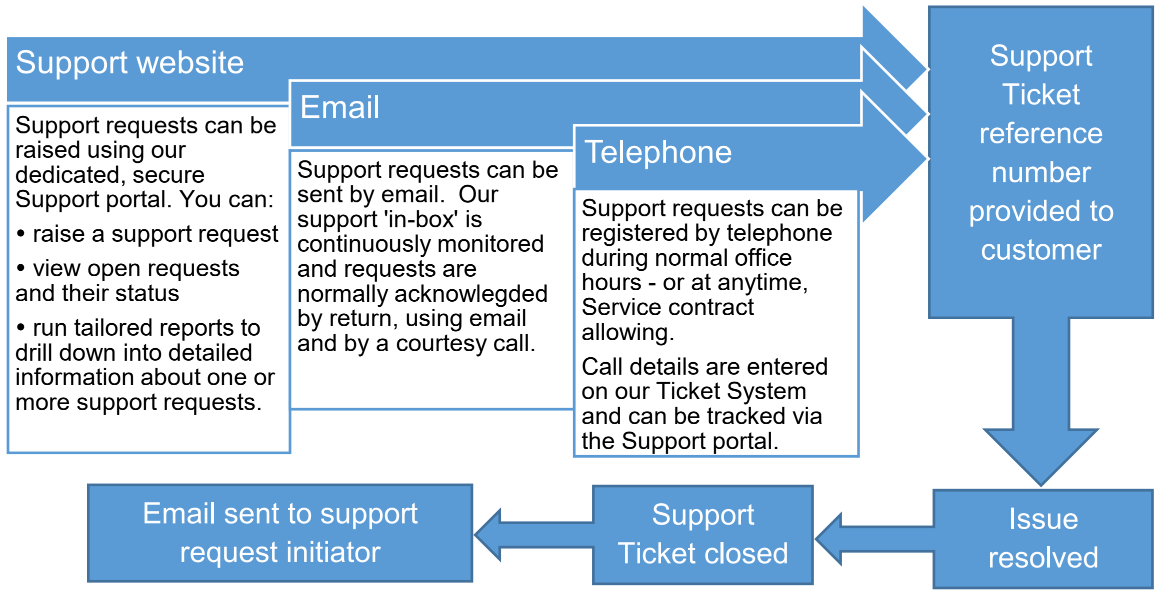

Figure 12: Raising Support Requests

Terms & Conditions

See our standard Terms and Conditions document.

About Us

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

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

Contact

Email: g-cloud@blackthorn.com

Telephone: +44 (0) 208 123 7989