Audit Case Management V15.0

service definition

IS 721821

Blackthorn

Contents

Introduction

Our Audit Case Management (ACM) system is an on-premise or cloud-based solution that helps organisations manage their audit and compliance programmes. Support is provided at every stage, from planning, through execution and reporting, to remediation and final close-out. It can be used as part of a compliance programme alongside education, training, and advisory activities to gain assurance that an organisation is aware of, and meeting, its statutory and regulatory responsibilities. As an enabler for internal audit, it can be used to demonstrate that an organisation is 'doing what it proclaims to be doing', and as a means of identifying risk where policy, process or procedure is not being implemented or followed correctly.

Our Audit Case Management platform enables collaboration, allowing audit professionals, stakeholders, and business functions to move through the multiple stages of assessment quickly and easily, and to monitor progress and outcomes as appropriate. It supports the organisation of resources, both people and assets[1], and the creation of processes allowing repeatable patterns of activity (workflow) to be defined and accomplished. Audit checklists can be created and amended. Work activities, whether planned or ad-hoc, can be defined, delegated, monitored, and reported on, giving managers, stakeholders and assessors full visibility of work activities and the status of the wider audit programme. Essentially, everything in one place needed to support an assessment and achieve timely determination.

By integrating ACM with our proprietary Risk Management Tool, audit findings can be used to inform and dynamically update underlying risk models, adjusting for failing or missing controls, changing exposures, etc. They can also inform and shape the scope of future assessments, especially where systematic failures are evident.

ACM integrates assessment processes and activities traditionally carried out using paper, spreadsheets, network file storage and email, and helps eliminate time-consuming administrative tasks such as double-keying, document scanning and manual version control. It improves operational efficiency, eliminating or automating many necessary but time-consuming activities normally peripheral to the main assessment effort. The benefits delivered by ACM include:

- real-time reporting of audit programme status to management / stakeholders
- key information elevated to forefront for improved situational awareness and insight, for example, to allow managers to track progress or auditors to see workloads and priorities
- maintains accountability for audit and follow up actions
- keeps audit activities on track by ensuring follow up actions endure, avoiding dilution or loss in the fog of follow-up communication

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

- calendar function to visualise, plan, manage and coordinate assessment activities
- alerts and notifications for improved awareness of targets, deadlines and the 'need-for-action' to move an audit forward
- system generated assessment reports based on a library of pre-configured, situational responses tied to answer sets (principally for autonomous self-assessment).

ACM caters for a range of audit types including operational, compliance, investigative, IT, management, and procurement. It also can be used for ISO standard based auditing and supplied with pre-existing audit checklists for ISO27001.

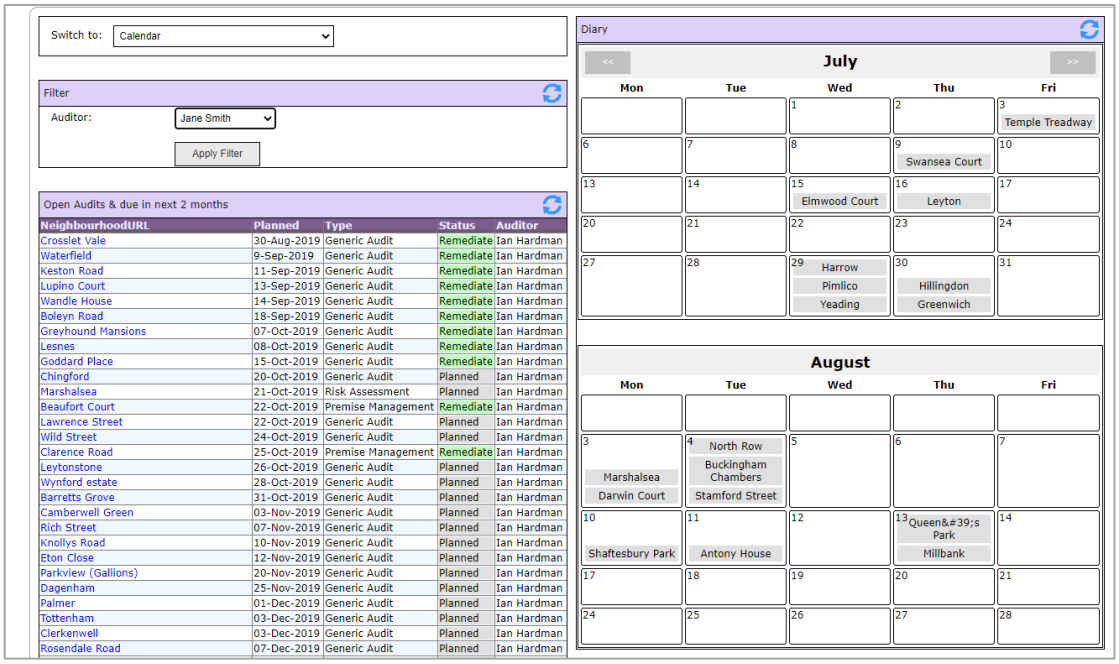


Figure 1: Diary Integration

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!

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

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

Our cloud services[2] 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[3] that meet the accreditation and assurance requirements of data at OFFICIAL (as per the Government's Security Classification), less expensive commercial cloud-hosting, or something in between. Full UK data sovereignty can also be assured no matter which hosting option is chosen. On-premise hosting is also an option. Our services can be accessed over standard Government networks (PSN, HSCN) or via the Internet with appropriate channel encryption.

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

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

Service Capability

The Blackthorn Audit Case Management System provides enterprise-level capability for planning, coordinating, conducting and documenting assessments. It also allows follow-up activities, such as remediation, to be managed and controlled.

Users have full visibility of their audit or compliance projects and the ability to assimilate information from multiple 'point-of-view' for enhanced situational awareness and ultimately, improved decision making. Access to the Audit Case Management System can be extended to business users or wider communities[4] for improved engagement or to facilitate self-assessment. For example, portals created for business use could provide date and time confirmation, status updates, tools to upload/download documents etc.

With our Mobile Audit App[5] (cost option), assessments can be conducted offline and in environments where Wi-Fi network connectivity is poor or non-existent.

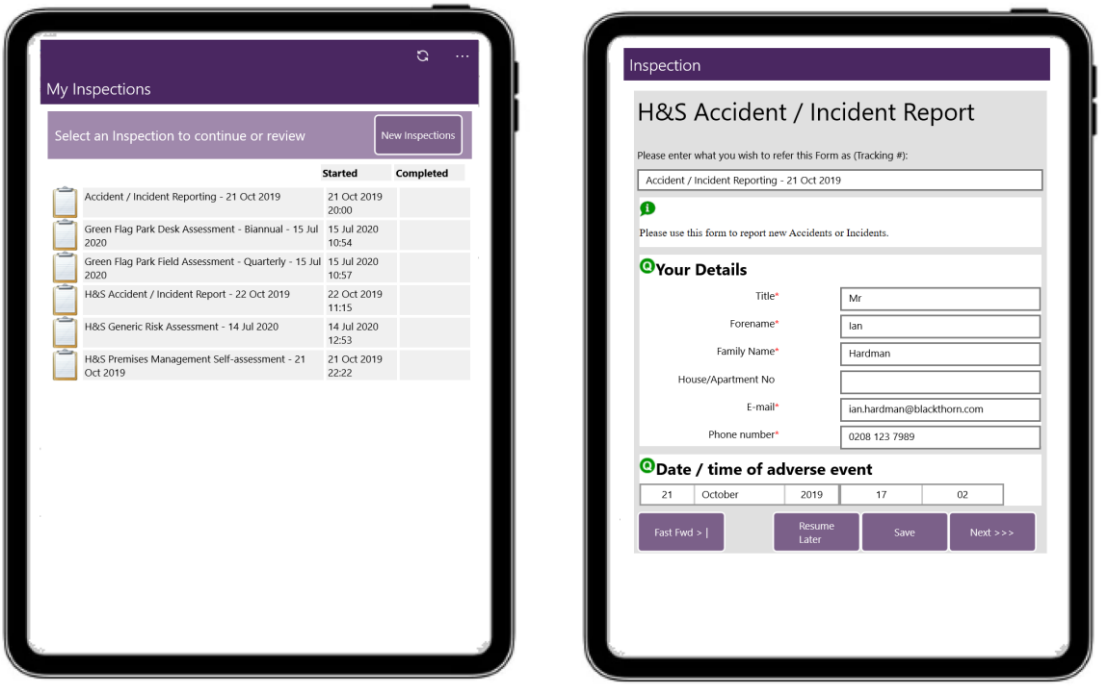


Figure 2: Mobile App

Necessary resources, including templates and information about prior assessments, are downloaded in advance to our Mobile Audit App, and the assessment findings uploaded when permanent access to the central ACM system is re-established.

---

[4] schools, retail sector, restaurants and food preparation organisations and other establishments that might fall within an organisation's sphere of responsibility.

[5] iOS, Android and Windows devices supported.

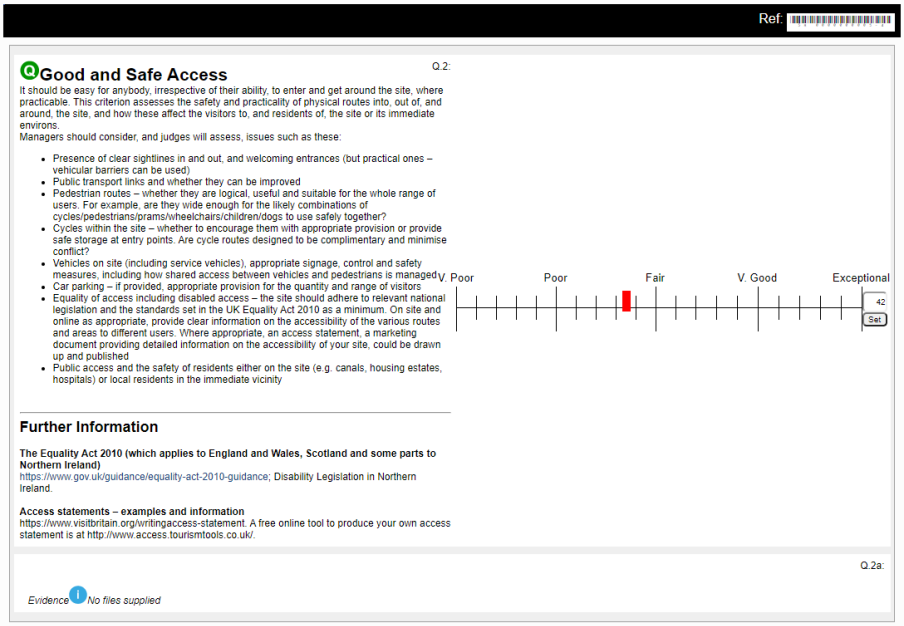


Figure 3: Audit Checklist with data entry slider

Audit and compliance checklists are constructed using a 'surveys' style approach. Assessment questions can be quickly composed, and answers collected in a range of formats such as free-format text boxes, multiple choice or ratings. Questions can be conditional on previous answers or linked to integral risk models. Surveys allow assessment checklists to be expedited efficiently and publication and deployment to be controlled. If audit and/or compliance checklists need to be more tailored and stylised or incorporate schematic diagrams for ease of data collection, digital e-Forms rather than surveys are an option. e-Forms can be either supplied tailor-made or self-created using our built-in e-Forms editor.

A calendar function makes the planning and scheduling of assessments straightforward and the re-allocation of assessments between team members just as easy. Strategic, operational and analytical dashboards, with drill-down, ensure that users have immediate access to the information they require and can track at organisation, team or individual level the status of assessments, remediation tasks, workload, capacity etc. Powerful *workflow* and *tasking* functions make light the planning and coordination of remediation activities, while MS-Word templates aid the automatic generation of assessment reports whether intended for the auditee or wider management oversight. Automated notifications and alerts provide users with notice of failing or non-compliant risk controls, and timely escalation to management if non-compliance endures.

ACM helps mitigate business risk by providing assurance that legislation, regulation and internal policies and protocols are being followed. Our Incident Response Management (IRM) solution is the converse, a solution for orchestrating a coordinated, targeted and spontaneous response to incidents and crisis situations i.e. a reactive rather than pro-active solution. IRM (cost option) ensures that adverse

events are handled in a methodical, pre-determined manner, delivering support to those at the epicentre.

With our Risk Management extension (cost option) you can dynamically recalculate risk based on the effectiveness of controls as determined by audit and inspection. RITA (Risk, Impact and Threat Assessment) is a module that enables asset-based risk models to be constructed using a graphical tree notation ('threat', 'exploitation method', 'intent', 'capability', 'frequency', 'loss', and 'control strength', each 1st order or 2nd order branches of the parent asset). Instead of risk determination being based on a *snap-shot* and subjective measurement, incident data (requires IRM) and audit finding are used to automatically adjust 'frequency' and 'control strength' respectively. By cross-correlating information from incident/accidents and audits, a (near to) real-time picture of operational risk is established.

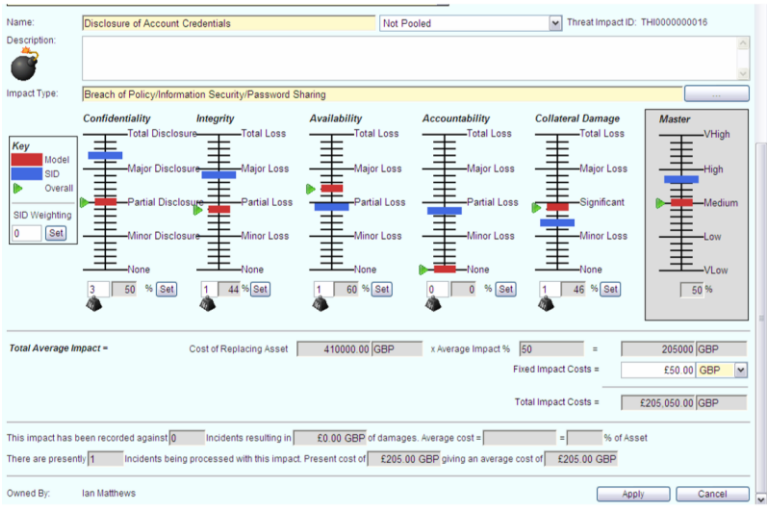


Figure 4: Determination of Risk

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

- plan and schedule the annual audit and inspection programme, assigning work to individual team members
- perform audits and inspections (on or off-line[6]) using self-created surveys or self-created / supplied e-Forms (checklists)
- create and publish surveys (for team use), unpublish superseded surveys
- create and distribute self-assessment surveys for completion by target cohort
- auto-generate reports with results from self- or facilitated assessments
- upload and apply custody to any file, picture or document associated with an assessment

[6] Off-line operation requires purchase of Blackthorn's H&S App which is available for iOS, Android and Windows mobile platforms.

- identify, assign, and track remediation actions to address findings
- review the corporate risk posture based on assessment findings and the effectiveness of extant risk controls
- create notifications and email alerts to raise awareness, prompt action, escalate issues
- gain ‘at-a-glance’ access to key information and insight using strategic, operational and analytical dashboards
- track and report on personal, team and office workloads
- access the information ‘behind’ the information for improved awareness using drill-down and hyperlinks (dashboard attributes)
- create bespoke dashboards using supplied dashboard ‘widgets’; customise supplied dashboards
- auto-complete assessment & management reports using either supplied or ‘tailor-made’ report templates (template library)
- add subjective content to auto-generated reports
- review and evaluate assessment finding to identity common, systematic failings
- maintain an online library of reference materials including regulations, policies, objectives and plans for general education and awareness
- gain positive confirmation from users (team and wider organisation) of receipt of regulation, policy and objectives updates and amendments.

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. ISO27001 compliance, 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

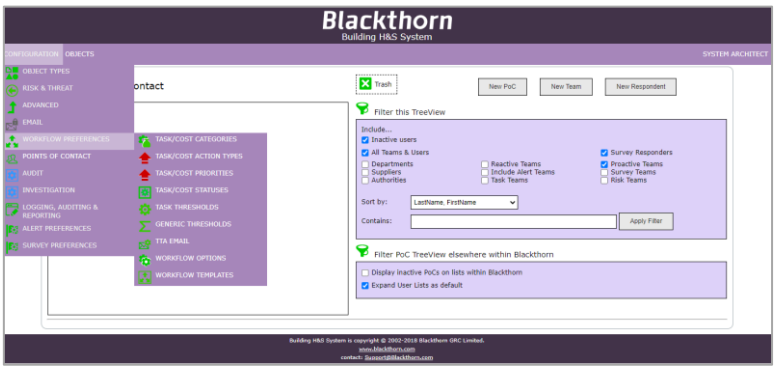


Figure 5: Configuration through GUI interface

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 Audit Case Management System are based on a technology platform (cloud or on-premise) that incorporates the following features and capabilities:

a) Information capture

High-fidelity e-Forms and surveys with embedded data validation and consistency checking help to eliminate mundane and error prone data entry. e-Forms 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).

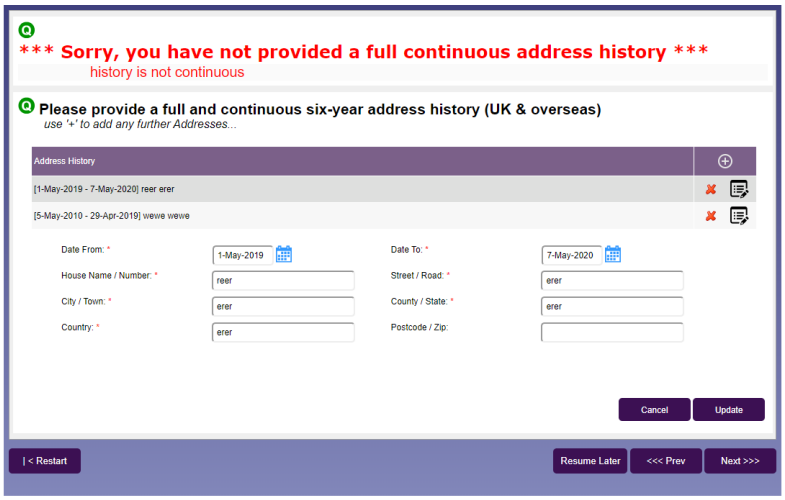


Figure 6: e-Forms

b) Records Management

Our *Records Manager* function provides real-time access to assessment records including plans, checklists, findings, assessee and management reports, remediation plans, remediation task specifications etc. associated with a case[7]. Case records can also hold uploaded artifacts such as documents, evidence, statements, photos, recordings etc. A graphical interface supports the organisation of this data, with subfolders for the

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

classification of different types of case content. For example, statements prepared by subject matter experts could be archived in a dedicated subfolder under a case. There is no restriction on the file types that can be uploaded and appended to a case.

Logical *associations* can be created between cases and the between records and artifacts across cases. For example, cases created as containers for individual annual assessments could be linked if associated with the same business function.

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

c) Search

A Search function employing 'fuzzy logic' allows searches to be conducted with partial or incomplete data. During data entry or file upload, the information presented to the ACM system (including file content) 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 the insight needed to drive decisions. Operational dashboards provide directors, managers, and seniors with a snapshot of the status of operations and key 'control' exposures. They provide assessors and administrators with fast changing information about their cases, assessments, 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. Example dashboards are provided in figures 7 & 8 below.

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

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

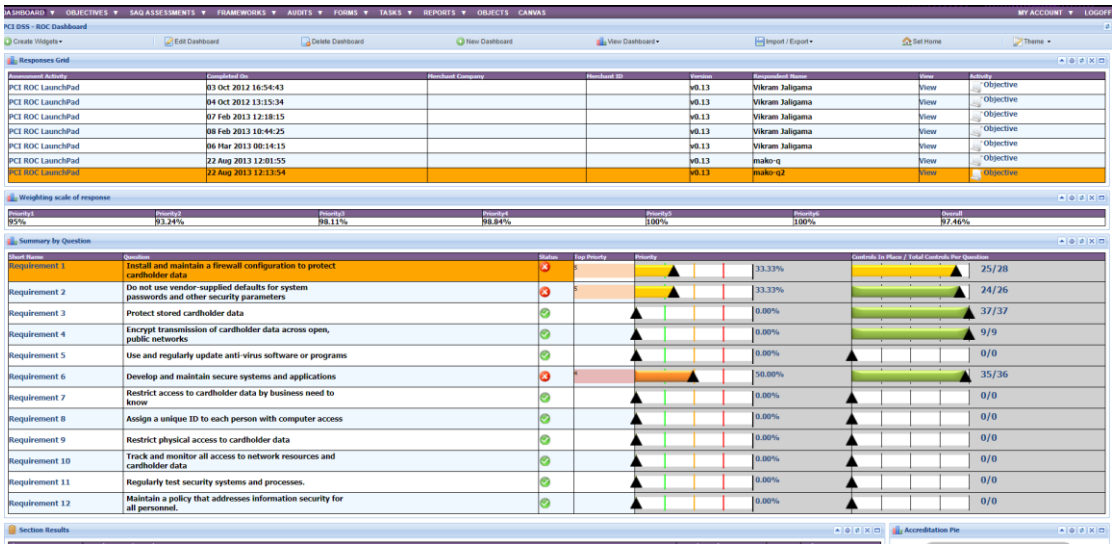
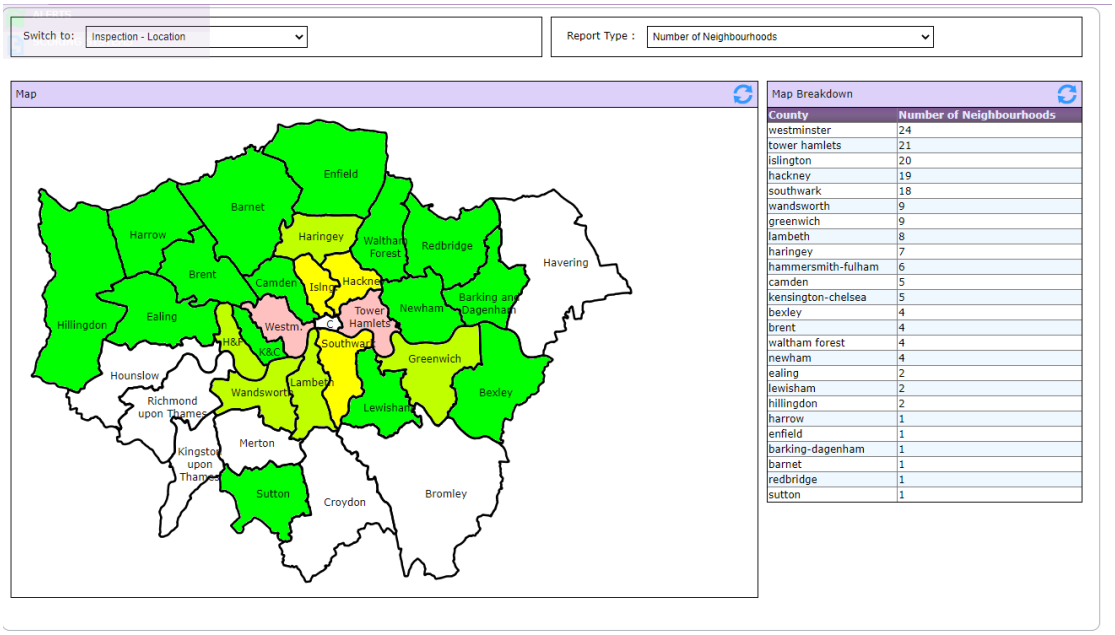


Figure 7: Audit Management dashboard



County	Number of Neighbourhoods
westminster	24
tower hamlets	21
islington	20
hackney	19
southwark	18
wandsworth	9
greenwich	9
lambeth	8
haringey	7
hammersmith-fulham	6
camden	5
kensington-chelsea	5
bexley	4
brent	4
waltham forest	4
newham	4
ealing	2
lewisham	2
hillingdon	2
harrow	1
enfield	1
barking-dagenham	1
barnet	1
redbridge	1
sutton	1

Figure 8: Compliant Neighbourhoods per Borough

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. 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 ACM system. The wizard also provides the ability to navigate around dynamic database content and structures.

g) Tasking & Workflow

Workflow allows a set of actions with a defined outcome to be defined, organised and accomplished in prearranged order. After an assessment, typically there are a number of follow-up activities (tasks) that must be completed within a set timeframe; some of these tasks are related and interdependent and require completion by two or more people, possibly even external departments or agencies. Workflow coordinates the conduct of such tasks, sequencing as appropriate; the work only commencing when conditions allow. Task owners are notified at the appropriate time and reminders issued before, at, and after the 'due date' if the task is late.

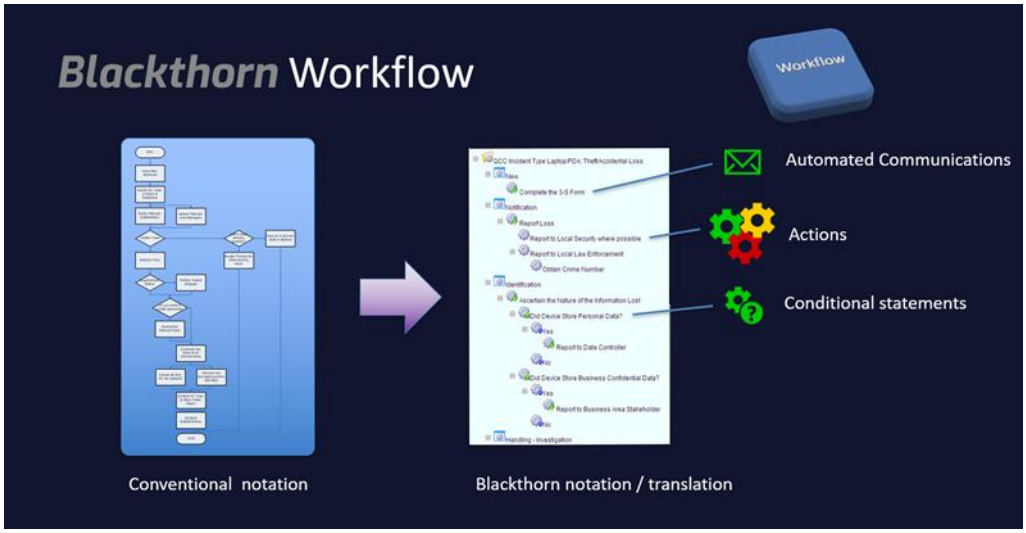


Figure 9: Blackthorn Workflow Notation

Whilst 'Tasking' is integral to the Workflow function, additional 'ad-hoc' tasks can be created as part of workflow, or independently, to address the specific and often unique needs of an assessment case. Work activities and tasks can be dynamically assigned to H&S 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 ACM system. The 'Pool' attribute allows assessments 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 audit teams or between business disciplines i.e. Internal Audit, Compliance, IT security etc. Pools can also be used to silo teams and restrict visibility of assessment cases within a team or department – again, where there is a genuine business reason to do so.

Pools also allow new assessment cases to be initially allocated to an 'unassigned' category. Rather than assigning assessments to team members at the start of the calendar or assessment programme, work can be allocated dynamically, closer to the time of execution, taking into account an individual's present workload and capacity. The 'unassigned' category also creates an opportunity for assessors to choose for themselves the assessments they would prefer to progress. 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).

i) Alerting and Notification

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

j) Self-assessment

Standalone report generation drawing responses and commentary from a library of pre-set content stored within the ACM system. By linking responses and commentary to survey answers (deterministic not subjective)[8] assessments can be delivered for self-completion and the assessment report

[8] Booleans, Radio buttons, Drop-downs are all examples of graphical controls that deliver a deterministic outcome to a give question.

auto generated. This feature uses the ACM system's standard report generation capability and library of document templates.

Self-assessment is a suitable option where the focus is more *educational* than compliance/assurance, or the volume of assessments makes 'facilitated' reviews impractical.

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) Compliance and data retention (GDPR)

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

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

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

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

m) Interoperability

A library of pre-existing web services (Open API compliant and RESTful[9]) are available for standard interfacing needs. OLEDB services are available allowing direct interaction with our data storage medium. Additionally, data can be exchanged digitally via email - both inbound and outbound. This has many advantages as SMTP[10], the vehicle enabling email, is ubiquitous, making it a very open and accessible channel for information exchange.

Features and Benefits

Features	Benefits
•Centralised management and handling of 'case' information •Context sensitive eForm for data collection •Graphical tools to construct and organise case data and evidence •Role based security for secure partitioning of information •Workflow management for process automation •Evidence tracking •Automatic creation of papers and files for court (option) •Case accountability follows the advancement of the case and is dynamically allocated •User configuarble 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.

[9] 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.

[10] Secure Mail Transfer Protocol.

eGRC Platform

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

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

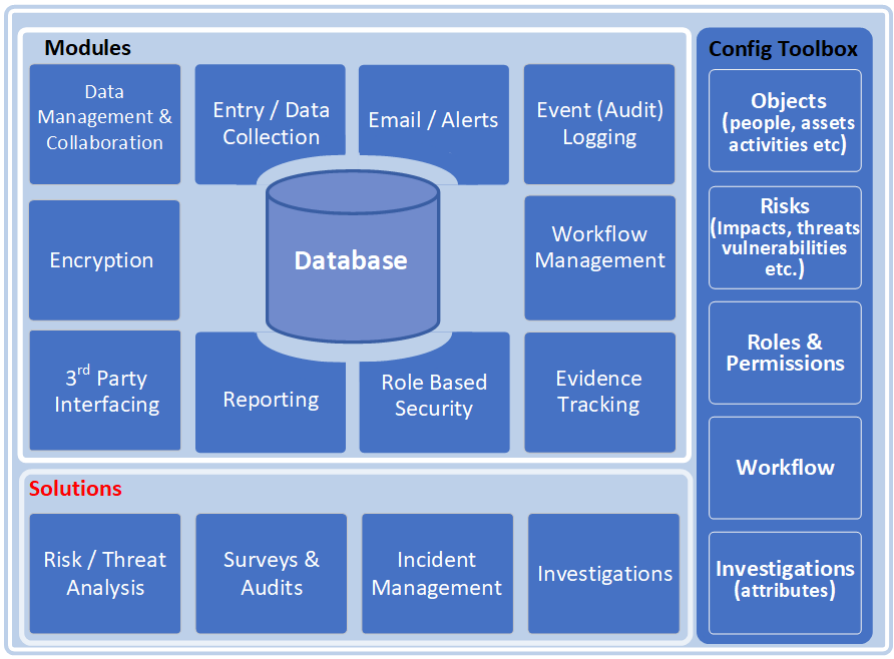


Figure 10: eGRC Platform Architecture

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 Audit Case Management solution is available with full database encryption, as well as channel encryption (secure link between browser and cloud infrastructure). We have established relationships with several hosting providers and can offer different hosting options based on risk appetite, budget, and the sensitivity of the data you need to store.

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

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

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

Service Architecture

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

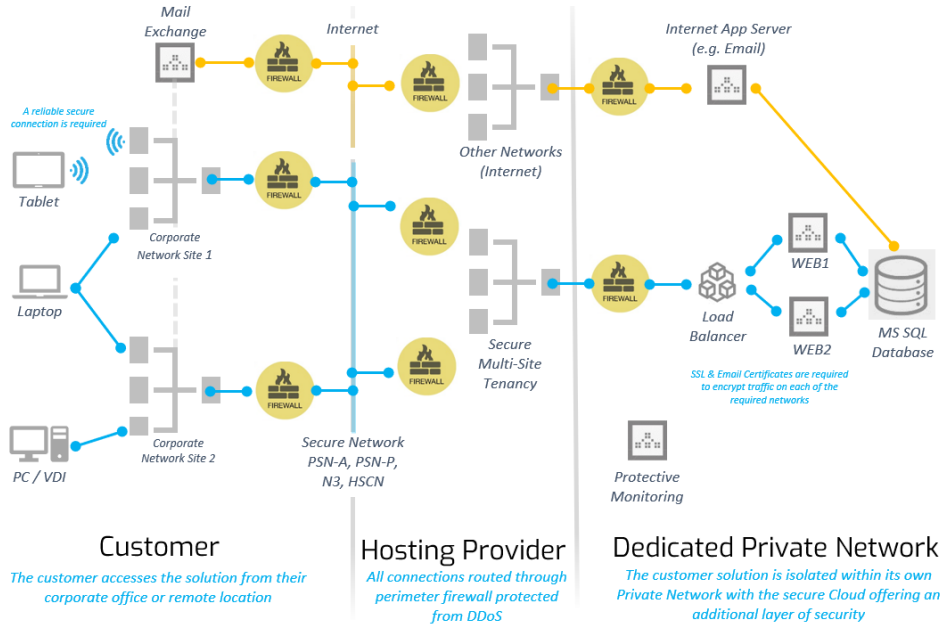


Figure 11: Dual Web Server suitable for hosting Official Sensitive Information

Our standard Government hosting solution (figure 11) 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-connection requirements. An air-gapped connection to an internet facing application service provides options for email over internet (GDS

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

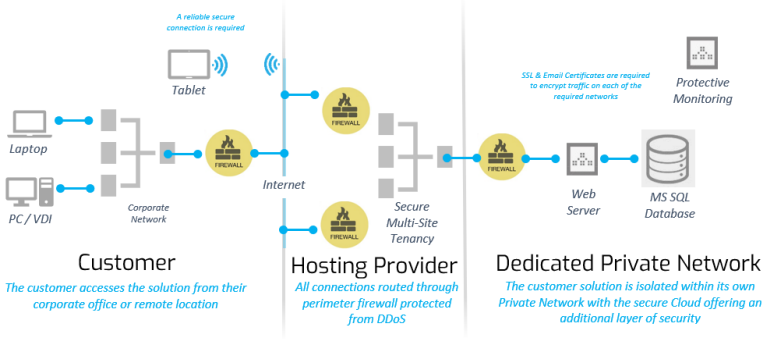


Figure 12: Single Web Server suitable for hosting Commercial Information

Where data security targets are less demanding, we can provide hosting with a commercial hosting provider (figure 12). The service is accessed over the internet with channel and database encryption as required. Figure 12 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.

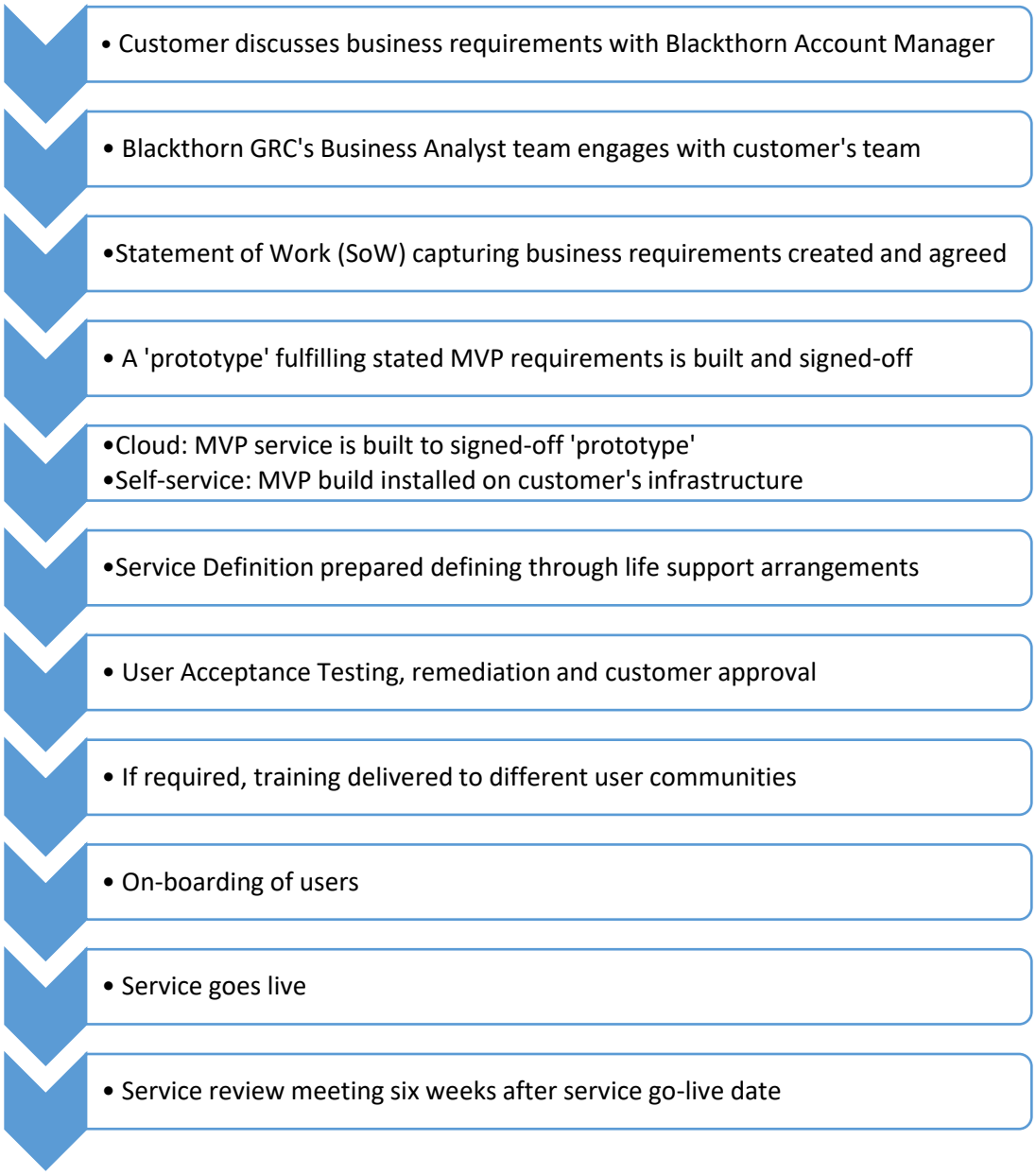


Figure 13: On-boarding stages

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 13 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.

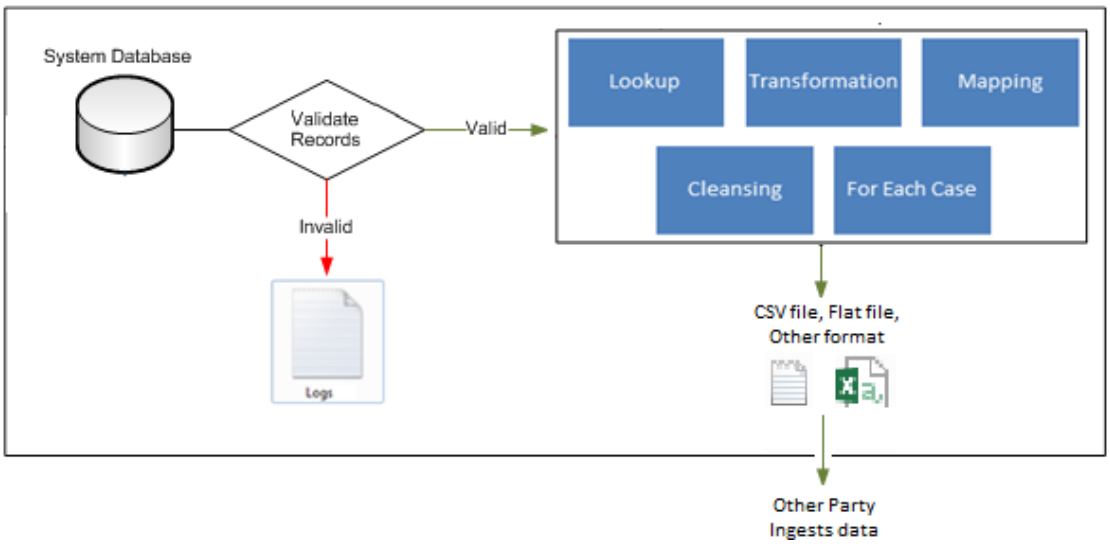


Figure 14: Data migration process

The data migrating process could involve:

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

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

Figure 14 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

	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.	and return service to full operational state. 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 15.

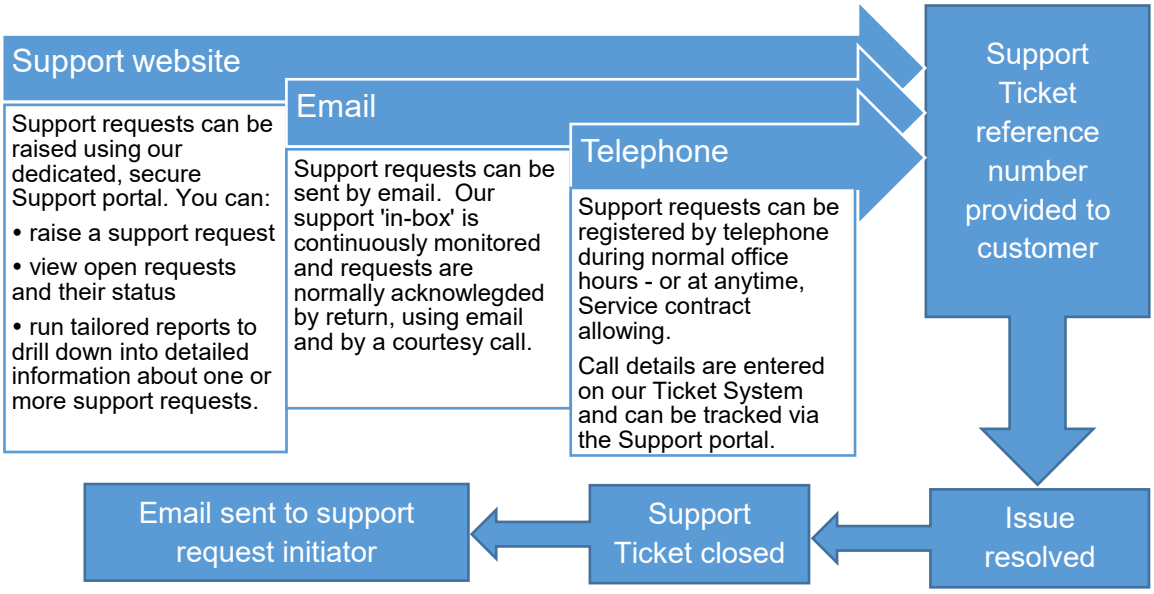


Figure 15: Raising Support Requests

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