Health & Safety Management v15.0

service definition

IS 721821

Blackthorn

Contents

Introduction

Our Health & Safety Management System (HSMS) is an on-premises or cloud-based solution that provides organisations with the tools needed to orchestrate safety processes, identify and better understand their risk landscape, and establish and maintain a culture of safety best-practice across the community or workplace. Under the guises of 'prevent', 'respond', 'educate', our software helps:

a. identify possible causes of injury or illness (hazards), determine the likelihood and seriousness of any harm (the risk), and manage actions to eliminate the hazard or control the risk
b. achieve a focused and coordinated response to actual incidents/near misses
c. centralise and consolidate safety policy, objectives, plans and guidance with update alerts and notifications.

Our software helps organisations achieve 3 imperatives, namely that work activities and premises are safe; staff and the wider organisation are cognisant of and compliant with legislation, regulation and industry specific guidance; and financial risk is managed by reducing exposure to the direct and indirect costs associated with an incident or accident. Aside from ethical, legal and financial reasons, many organisations will feel they have a moral obligation to promote and operate health and safety practices in order to keep employees, students, members, patrons etc. safe and protected from avoidable harm. We believe our software helps in this respect too.

As health and safety practices tend to be sector and discipline specific, we have created a range of solutions covering:

a. Occupational Health Management
b. Industrial/ Environmental Safety Management
c. System Safety Management, and
d. Incident Management.

By integrating our H&S Management tool with our proprietary Risk Management tool, inspection findings can be used to inform and dynamically update underlying risk models, identify missing or failing controls, and inform the scope of future H&S assessments. Our software has the added benefit of automated alerts for notifying management of failing or non-compliant H&S controls, and escalation if non-compliance endures.

With the exception of Incident Management, all of our solutions are *pro-active* in their approach to health and safety, focusing on the avoidance of accidents through the early identification of potential hazards, risks or failing controls. Using either supplied,

tailor-made[1] or self-created forms, H&S audits[2] and inspections[3] can be carried out digitally, allowing the results to be captured centrally and supporting evidence, such as local procedures, photos or independent statements to be uploaded and appended to the assessment. A calendar function makes the planning and scheduling of assessments (a.k.a. audits and inspections) straightforward and the re-allocation of assessments between team members just as easy.

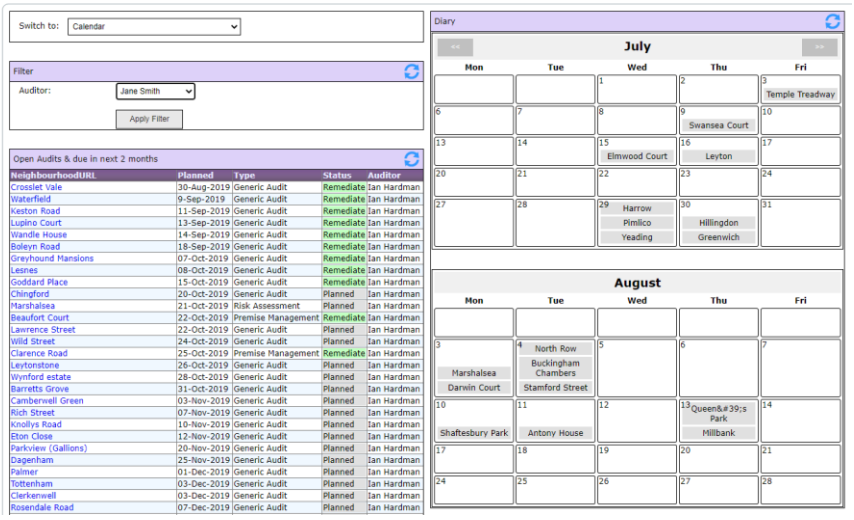

Figure 1: Diary Integration

Powerful workflow and tasking 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 general management oversight. 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.

As an alternative to digital forms (e-Forms), Audit and Inspection checklists can be implemented as surveys. Surveys allow list of questions to be expedited efficiently and with greater autonomy. They also allow assessment reports and remediation action plans to be autogenerated using a library of pre-configured, situational responses. This is particularly powerful in volume, self-assessment situations.

---

[1] Blackthorn supplied form developed for customer to meet a specific audit/inspection requirement.

[2] process of checking that compliance obligations have been meet. This could be compliance with extant policy, processes and procedures, or the existence and successful operation of mitigating controls.

[3] principally focus on hazards in the workplace or premises; the assessment is not necessarily structured, relying more on ad-hoc techniques and experience to flush-out issues.

Completed audits can also be linked to risk models for the determination of control effectiveness.

Incident Management is *reactive* rather than *pro-active* and provides all the resources need to deliver a coordinated and focused response to an accident or incident (near-miss). This includes incident reporting (online portal), triage, emergency response, incident analysis, reviewing and evaluation.

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!

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

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

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

[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.

standard Government networks (PSN, HSCN) or via the Internet with appropriate channel encryption.

Service Capability

The Blackthorn Health & Safety Management System provides enterprise-level capability for managing safety in the workplace or other locations where people could be exposed to harm. It is a holistic solution that delivers both support for the systematic identification and treatment of hazards as well as tools for managing the attitudes and behaviours of employees and other groups operating under its umbrella. It delivers the tools required for an orchestrated and targeted response to real accidents and incidents, together with support to determine and build (over time) evidence of compliance with regulation, policy and guidance.

Based on a set of core modules, our Health and Safety Management System comes pre-configured with the forms and reports needed to address different operational requirements and national/international standards such as Occupational Health, Industrial Safety, System Safety etc. However, 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. Occupational Health, 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 gestation time between contract award and initial operating capability is measured in weeks rather than months.

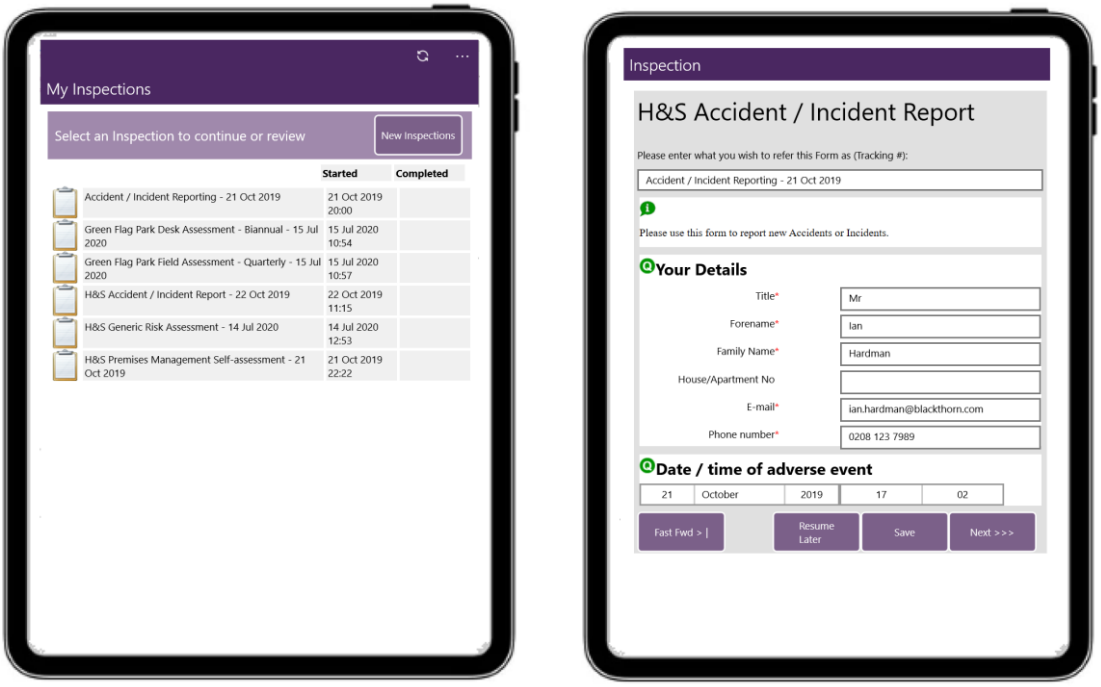

Figure 2: Mobile App

Whilst our H&S Management System can be used in several different contexts e.g. Occupational Health, each variant is underpinned by a set of common modules which include, as standard, functionality allowing users to:

- plan and schedule the annual audit and inspection programme, assigning audit & inspections to individual team members
- perform audits and inspections (on or off-line[6]) using supplied or self-created e-Forms and/or surveys (a.k.a. digital forms)
- create and publish audit and inspection checklists (digital forms) for team use
- create and distribute self-assessment digital forms for community completion
- auto-generated reports with results from self- or facilitated assessments
- upload and apply custody to any file, picture or document associated with an inspection or audit
- determine the likelihood and seriousness of any harm associated with an identified hazard
- identify, assign, and track actions to eliminate hazards or control risks
- review the corporate risk posture (in respect of H&S) based on assessment results and the effectiveness of extant H&S controls
- respond to H&S incidents/accident in a methodical, pre-determined manner, gathering information and evidence from those at the epicentre
- triage reported incidents and assign to an investigating officer
- upload and apply custody to files, pictures and documents relating to an incident
- 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
- use drill-down and hyperlinks (both dashboard attributes) to access the information ‘behind’ the information and gain improved awareness
- create bespoke dashboards using supplied dashboard ‘widgets’; customise supplied dashboards
- generate and pre-populate assessment & management reports using supplied and ‘tailor-made’ report templates (template library)
- add subjective content to auto-generated reports (a.k.a. mail merge)

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

- review and evaluate assessment finding to identity common and systematic failings
- maintain a library of H&S reference materials including regulations, policy, objectives, plans and checklists. Library accessible to H&S team and wider community where authorised
- gain positive confirmation from users (team and wider) of receipt of regulation, policy and objectives updates and amendments.

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 a 1st order or 2nd order branch of the parent asset). Instead of risk determination being based on a 'snapshot' and subjective measurement, H&S incident data and audit findings 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.

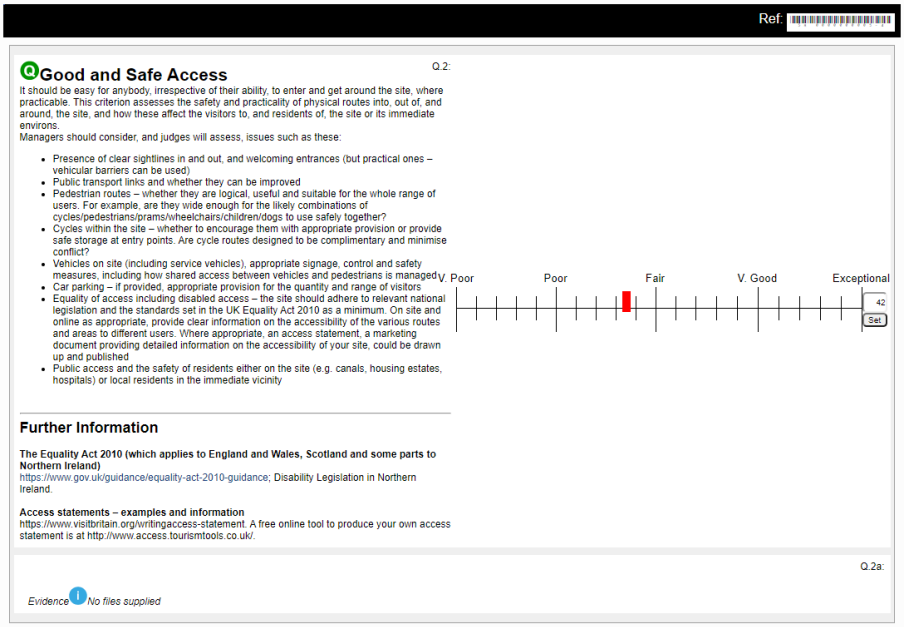

Figure 3: Checklist with data entry slider

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

a) Information capture

High-fidelity e-Forms and inspection questionnaires with embedded data validation and consistency checking help to eliminate mundane and error prone data entry. Our e-Forms are context sensitive, only displaying the fields required for the operation in-hand. Some inspection questions are *conditional* (on earlier answers) constructing navigable, dynamic question sets. Documents, files, audio recordings, photographs, scanned papers etc. can be associated to evidence a response, or later emailed to the system and automatically added to an audit. 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).

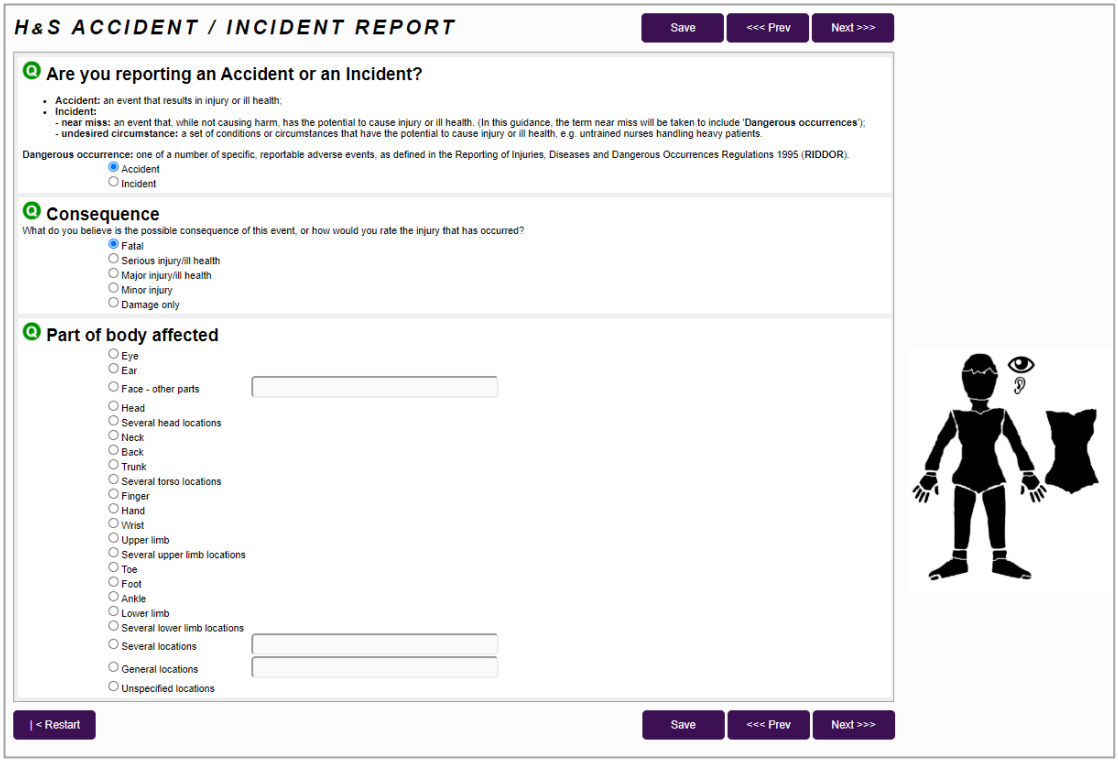

Figure 4: Digital e-Form (example)

b) Records Management

Our 'Records Manager' function provides real-time access to inspection, audit, incident, and investigation records, including artifacts such as documents, evidence, statements, photos, recordings etc. associated with a

case[7]. 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. 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 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 ACM system is indexed prior to storage, creating meta-data files that accelerate future searches and look up. The search results remain vigilant of any user access restrictions in force, ensuring the privacy of sensitive information.

d) Dashboards

'At-a-glance' access to key information and insight needed to drive decisions. Operational dashboards provide directors, managers and seniors with a

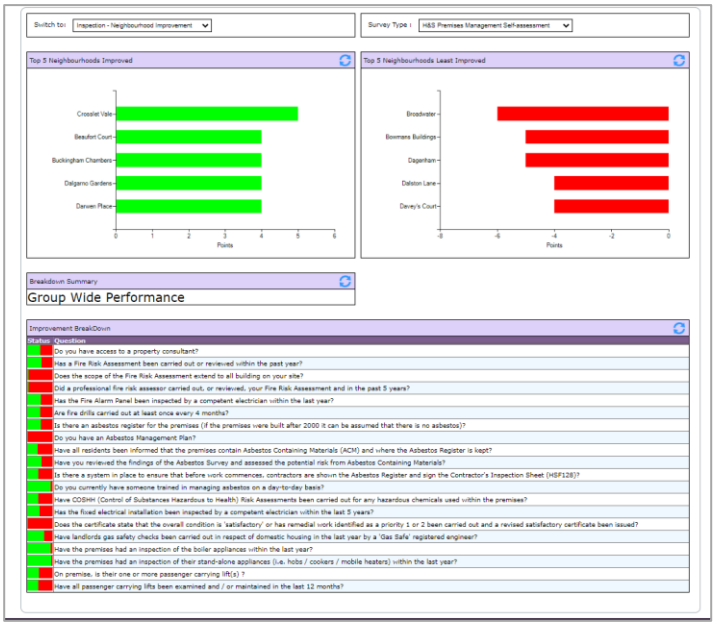

Figure 5: Inspection Summary dashboard

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

snapshot of the status of operations and risk exposure. They provide auditors, assessors and occupational health physicians 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. Sample dashboards are provided in figures 5, 6 & 7.

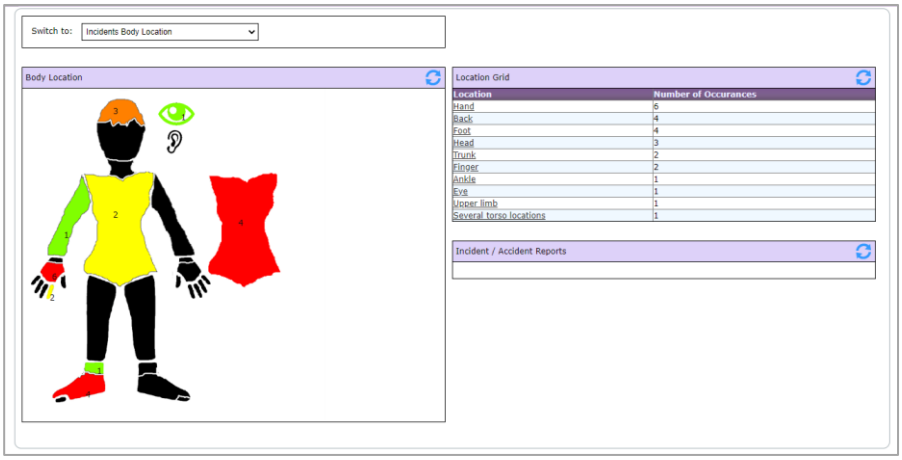

Figure 6: Incident Body Location form

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

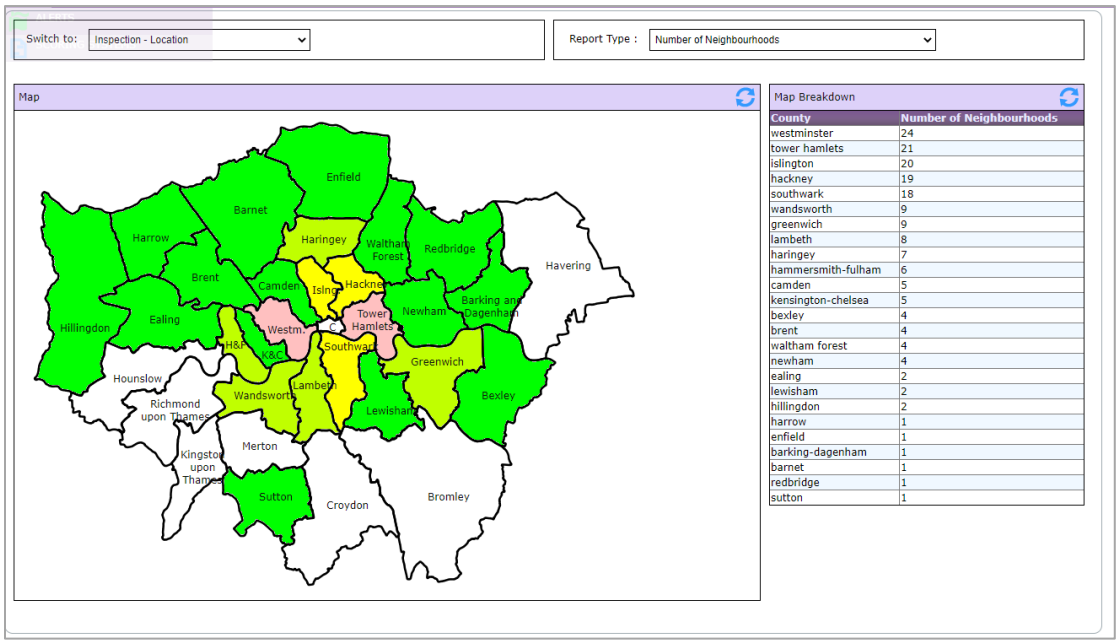

Figure 7: Compliance per borough dashboard

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

e) Forms and Reports

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 HSMS 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.

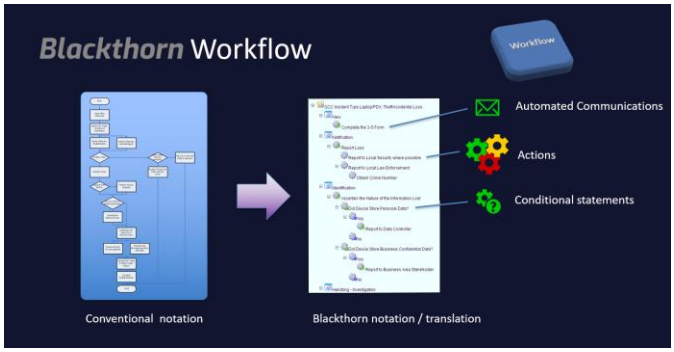

Figure 8: Workflow notation

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

Whilst 'Tasking' is integral to the Workflow function, additional 'ad-hoc' tasks can be created as part of workflow, or independently, to address the specific and often unique needs of a 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.

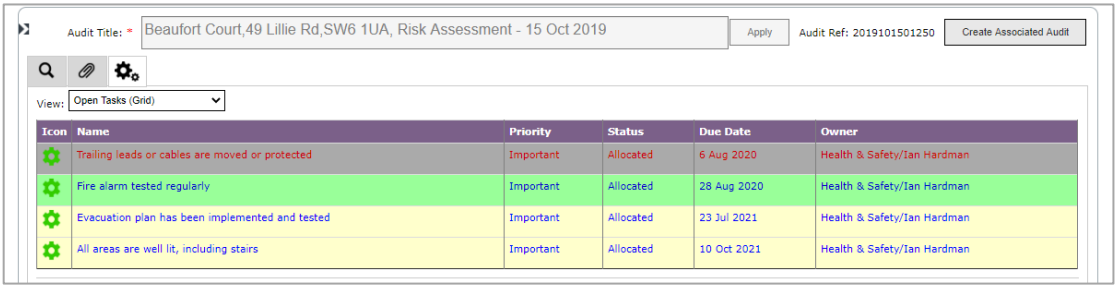

Figure 9: Task dashboard

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

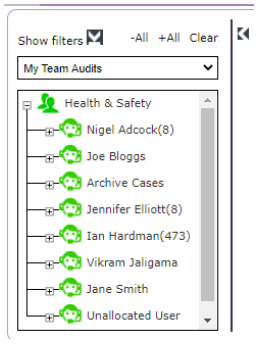

Figure 10: Work Allocation

Case records have a number of attributes that are used solely by the HSMS. 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 H&S teams or different H&S disciplines (i.e. Occupational Health, Industrial H&S etc.) where the HSMS platform 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 case relates to an externally reported safety incident and until triaged will be without a formal owner (investigating officer). Unassigned cases can be triaged by a Team Leader, Manager or duty officer, and manually assigned to the Case Officer best placed to assist. Where the allocation is based on case workload, an individual's workload can

be reviewed via dedicated ‘My-Task’ screens or a dashboard (see Dashboards above).

i) Alerting and Notification

Multiple channels are available for alerting and notification. Dashboards provide assessors, case officers, physicians 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 users, and whilst requiring the recipient to have a HSMS 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.

As your service provider, Blackthorn has in place established processes for handling FOI and SAR requests where prior authorisation has been given by the 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[8]) 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[9], the vehicle enabling email, is ubiquitous, making it a very open and accessible channel for information exchange.

Features and Benefits

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

[8] 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.

[9] 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

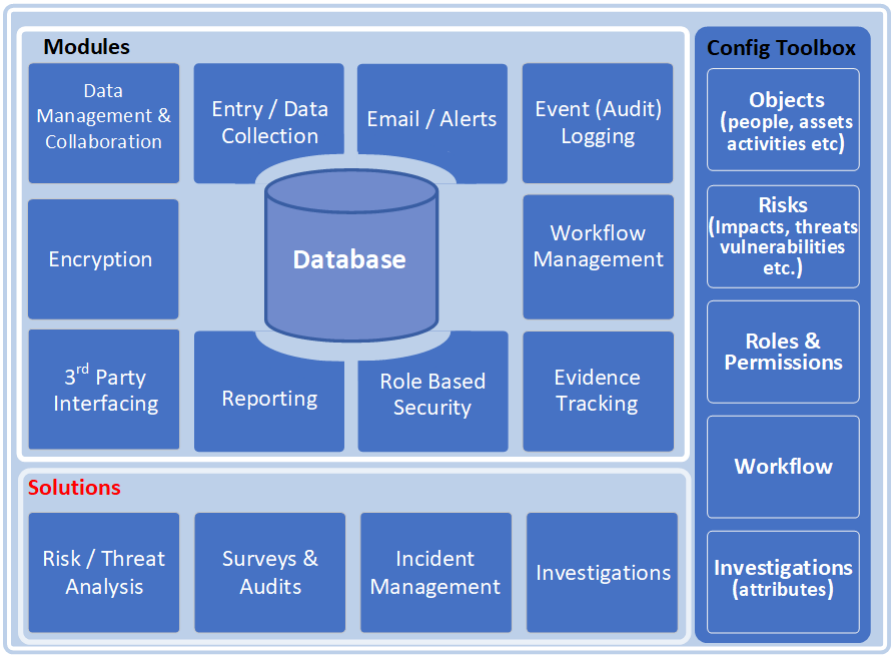

Figure 11: eGRC Platform Architecture

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 H&S 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.

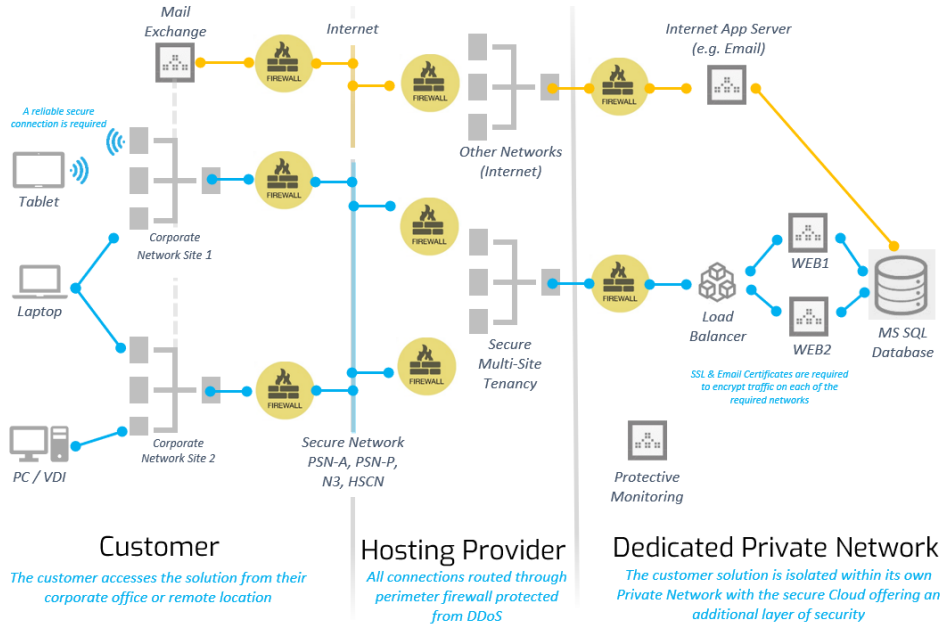

Figure 12: Dual Web Server suitable for hosting Official Sensitive Information

Our standard Government hosting solution (figure 12) leverages data centres meeting the accreditation and assurance requirements of data at OFFICIAL. They are reached via secure corporate and wide area networks (e.g. PSN, HSCN) and meet all Government code-of-connection requirements. An air-gapped connection to an internet facing application service provides options for email over internet (GDS

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

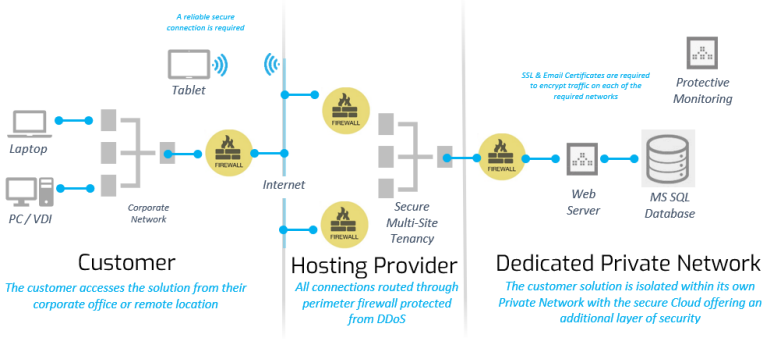

Figure 13: Single Web Server suitable for hosting Commercial Information

Where data security targets are less demanding, we can provide hosting with a commercial hosting provider (figure 13). The service is accessed over the internet with channel and database encryption as required. Figure 13 shows a single webserver, but again, this infrastructure is scalable both in terms of machine capacity and performance and the number of virtualised machine instances used to host our web-Application software.

Resilience

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

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

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

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

Protective Monitoring

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

Business Continuity

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

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

On-boarding

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

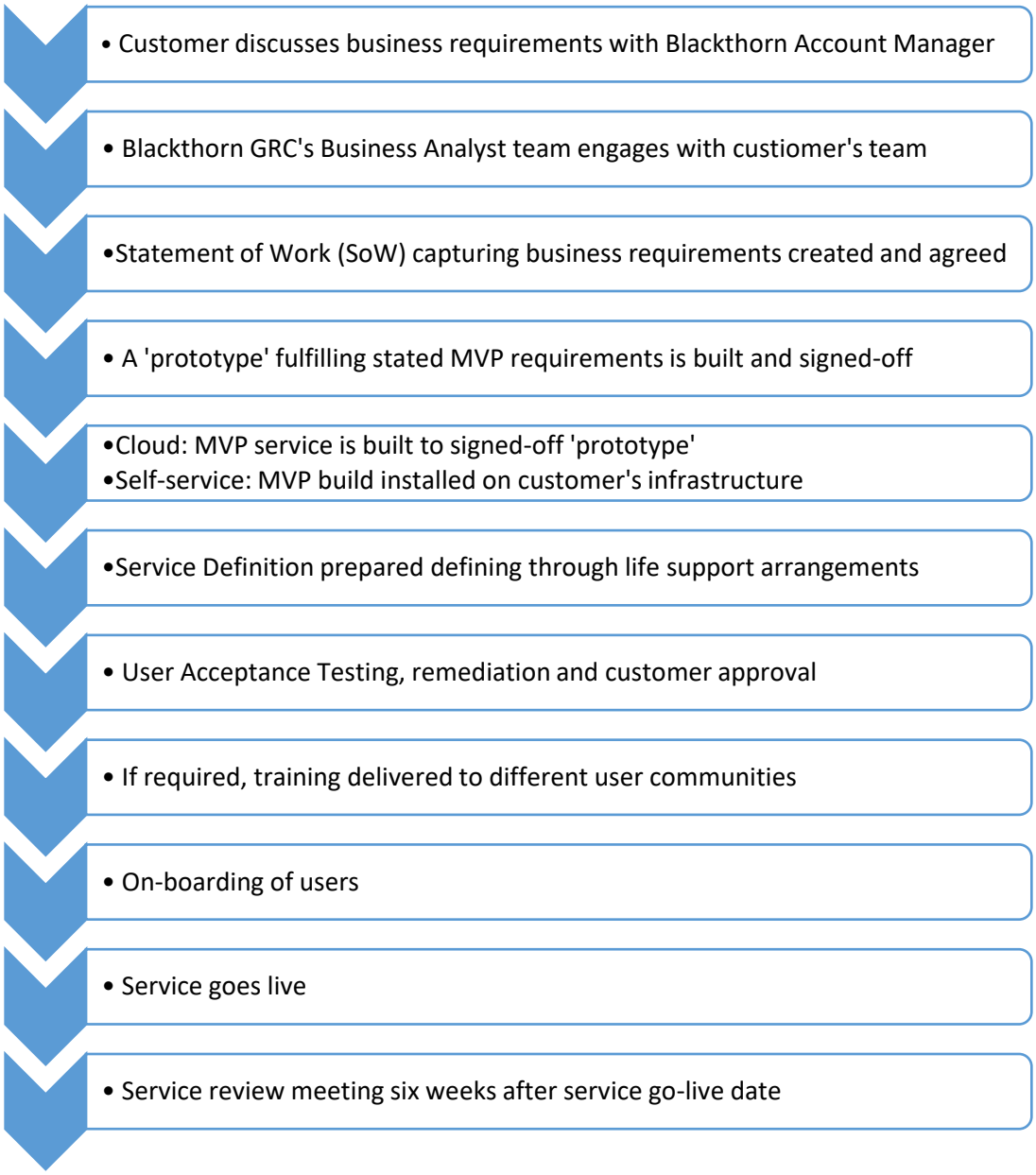

Figure 14: On-boarding stages

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 14 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.

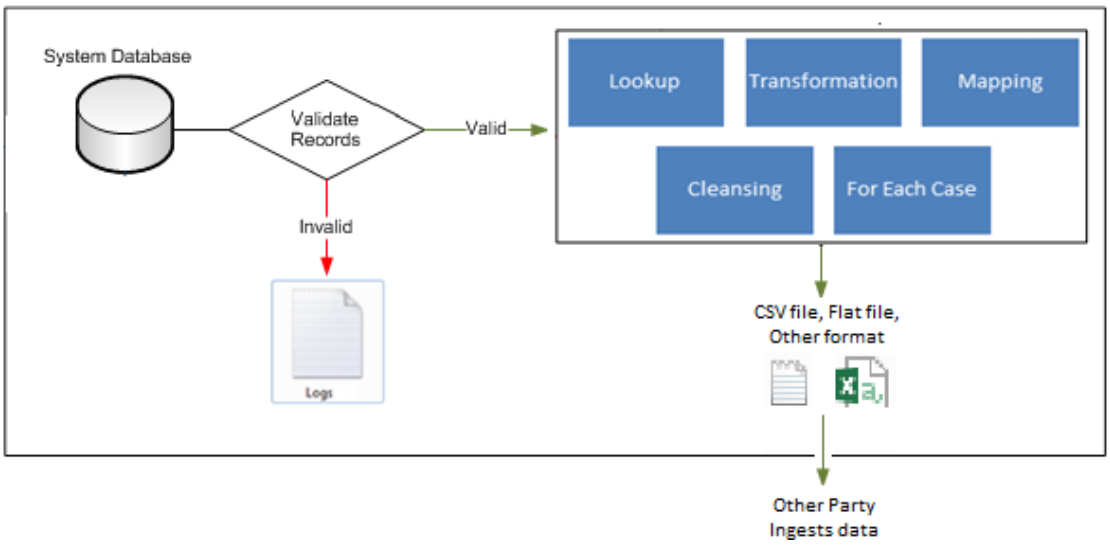

Figure 15: Data migration process

The data migrating process could involve:

a. extracting all textual data to a ‘flat’ or .csv file of agreed format, the file acting as the interface between the two systems, or
b. 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 15 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 16.

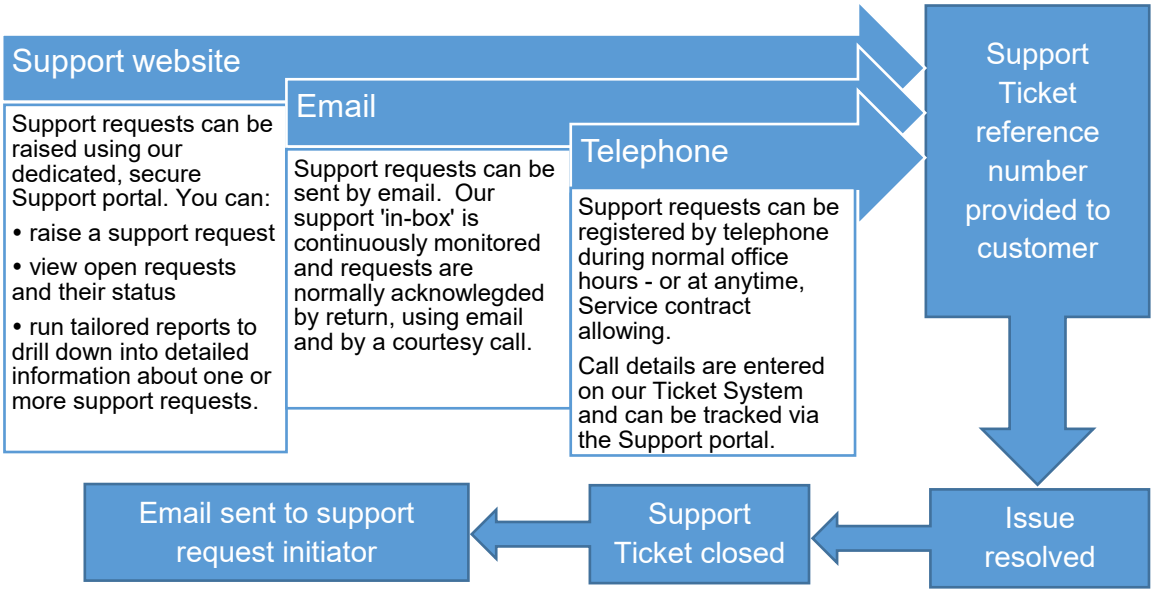

Figure 16: Raising Support Requests

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