Incident Response Management
v15.0

service definition

IS 721821

Blackthorn

Contents

Introduction 2
Service Capability 4
Features and Benefits 10
eGRC Platform 11
Cloud Hosting 12
Service Architecture 12
Resilience 13
Protective Monitoring 13
Business Continuity 14
On-boarding 15
Service Provisioning Time 16
Service De-provisioning Time 16
Service Delivery 17
Off-Boarding 18
Response Times 20
Raising a Support Request 22
Terms & Conditions 23
About Us 24
Contact 24

Introduction

Our Incident Response Management (IRM) solution is an on-premises or cloud-based application for handling crisis situations. It helps organisations achieve a focused and coordinated response to major incidents. This solution is particularly suited to security/cyber incident management but can be used in any situation that is threatening and has the potential to cause harm to people or property, disrupt operations, damage reputation or negatively impact the bottom line. Such situations include environmental damage, industrial accidents and confrontational matters.

In a crisis, an organisation's speed-of-response is often critical; a slow response provides greater opportunity for the crisis to intensify or expand its footprint, increasing proportionally the response effort. Experience, forethought, planning, and timely communication are all critical to negating both the threat and impact, and in turn, minimising the inevitable downside. Our Incident Response Management solution ensures:

- delivery of a rapid, proactive response based on pre-defined strategies aligned to incident type
- effective orchestration of strategies
- effective communication between members of the response team and between the response team and third parties i.e. corporate stakeholders, external agencies, authorities, law enforcement, media etc.
- clear accountability in terms of roles and responsibilities
- access to tools for capturing information and ring-fencing information admissible in court
- opportunities to evaluate and optimise the response strategy(ies), raising team familiarity and awareness.

Our software drives efficiencies and the achievement of positive outcomes by supporting all aspects of a response. This includes data capture and analysis, decision making, remediation, and response tracking. Powerful workflow management ensures effective alignment with planned and authorised response strategies, high-fidelity e-Forms simplify data capture, and a searchable, secure database ensures ease of access (whilst preserving case confidentiality). Configurable dashboards and reports, as well as 'drill-down' functionality, ensure that important information falls readily to hand, while automated alerts give users advance notification of critical actions or situations requiring immediate attention. Perhaps most importantly, our IRM solution ensures the right information reaches the right people and when it is needed so they can achieve the optimum response.

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 capabilities and functions to be integrated into one cohesive package. Customers have 'total say' over the look and feel of their solution and consequently, the resulting user experience.

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

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

Our cloud services[1] 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[2] 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.

[1] solutions delivered as an online, subscription service and SaaS modality.

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

Service Capability

Accurately detecting and assessing incidents is challenging because three separate factors come into play:

a. Indicators[3] and precursors[4] come in many forms and with varying levels of detail and fidelity. Some indicators and precursors are clearly signalled and easily detected; others remain obfuscated making them more difficult to discover. Some are reported multiple times by a plethora of automated systems; others by staff, and with the imprecision that accompanies unfamiliar territory.

b. The volume of potential alerts is typically very high – automated sensors can generate thousands of warnings a day, and the number of system-generated alerts can be equally high without selective filtering. Separating standard system events from warnings (likely to indicate an incident), and background noise, is non-trivial.

c. Deep technical knowledge and experience is needed to reliably analyse (security) event related data.

Our purpose-built solution for Incident Response Management (IRM) directly benefits the incident response endeavour by centralising data collection and orchestrating the response through 'playbooks' that establish planned and tested responses to common incident types such as malware, cyber-attack, or a business continuity event such as fire, flood or pandemic. Our Workflow Manager and Ad-hoc Tasking functions can be used to choregraph the playbooks into a sequence of response actions triggered by events or prior actions. Events and decisions can be easily recorded helping with knowledge exchange and communication between members of the Incident Response Team.

Alerts received by the Incident Response Management system can be automatically *triaged* based on predefined rules, but a further manual *triage* can be recorded against alerts as confirmation that they have been correctly assigned as incidents (i.e. events that require follow up action and management). One or more alerts can be used to create an incident, and similarly, a single alert can result in multiple incidents. Reporting can be either be at the alert or incident level.

Our many years of experience working with law enforcement and other security agencies has taught us that no two organisations are totally alike and whilst their underlying requirements might be the same e.g. ISO27035[5] compliance, some deviation from our established product line is inevitable. This might be required to

---

[3] 'Indicator' is a signal that a security incident might have previously occurred or is occurring.

[4] 'Precursor' is an indication of unusual activity or behavior that often precedes a more sinister security incident.

[5] Information Technology – Security Techniques: Information Security Incident Management

cater for circumstances, individual preferences, or the need to integrate with existing in-house applications and systems. Specific data collection, assessment or reporting needs might also be the catalyst for change. Whatever the reason, our data configurable software ensures that any additional bespoke coding is kept to a minimum and the dwell time between contract award and initial operating capability is measured in weeks rather than months.

The consolidation of activities and information into a single platform has enabled us to deliver a holistic solution to Incident Response Management with the following features and capabilities:

a) Information capture

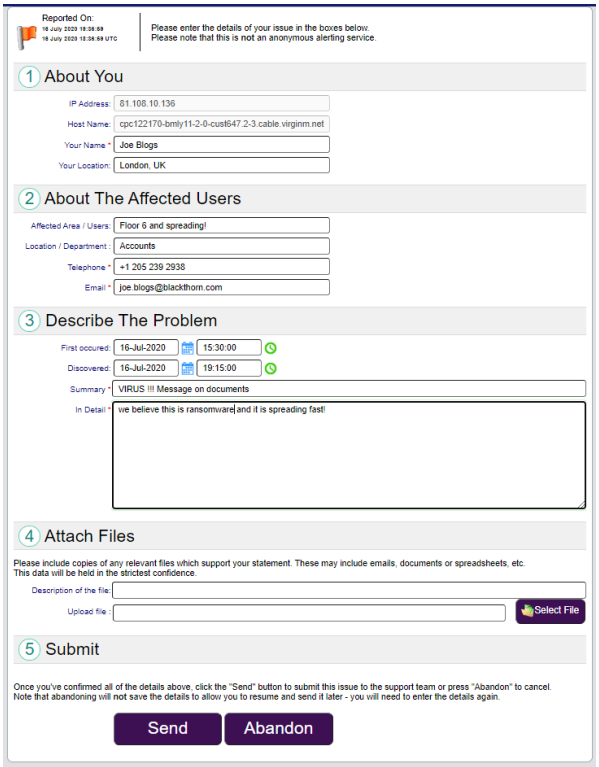

Figure 1: Manual Alerting

High-fidelity e-Forms with embedded data validation and consistency checking help to eliminate mundane and error prone data entry. Our e-Forms are context sensitive, only displaying the fields required for the operation in-hand. All types of files can be captured securely and isolated. Optionally, AV scanning can be disabled on uploaded files to enable capture of example infected files. This includes documents, files, audio recordings, scanned papers etc. which can even be emailed to the system and automatically added to an investigation. Web services allow data transfer (input and output) to other digitally enabled, online systems, such as SIEMs, Reuters News Alerts or similar. Specially designed syslog listeners can interface to multiple devices such as entry system, door logs, firewalls, computer event logs.

b) Records & Evidence Management

Real-time view of information and documentation, including evidential items, relating to an incident. A graphical interface supports the organisation of data and creation of ‘associations’ between data objects such as evidence items

and strategy notes. The relationship of the association can also be defined. Objects can be spanned on workspaces and zoning created.

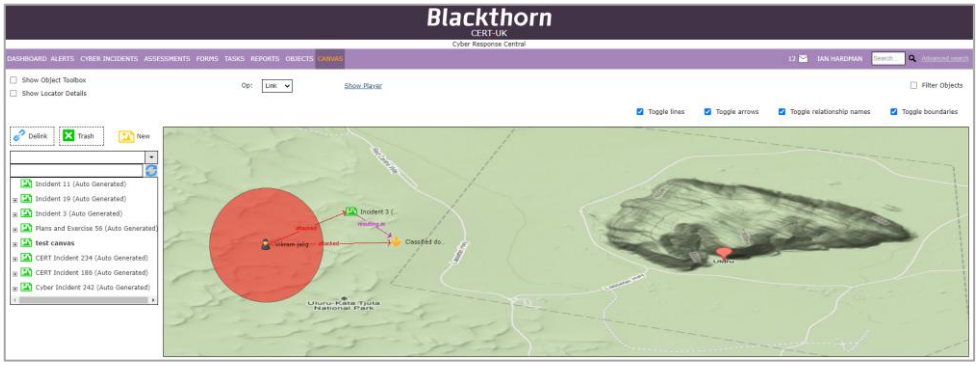

Figure 2: Situation Awareness & Link Types

There is no restriction on the file types that can be uploaded to a case, whether pertaining to evidential data, witness statements, meeting records, inspections, decision points etc. All files are hashed from tampering. The system is able to securely handle sensitive information and restrict access to only those with a genuine 'need-to-know'. A full audit trail is readily available to identify persons who have accessed the information.

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 IRM 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 the insight needed to drive decisions. Operational dashboards provide directors, managers and seniors with a snapshot of the status of operations and recovery. They provide the response team with fast changing information about the incident, response strategy, actionable tasks, overdue activities etc. Analytical dashboards enable a more detailed evaluation of tasks and response planning and give access to underlying details or trends.

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

The IRM system is supplied with a range of standard, pre-configured dashboards which can be individually fine-tuned using filters and personal preferences. Custom dashboards can also be created (permissions allowing) and constructed to meet 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 regulation, policy, internal protocol and guidelines. Document templates can be added to the library of supplied templates allowing standard and bespoke forms and reports to be created digitally and auto completed with relevant incident 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 Incident. 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' that gives the user complete control over the extraction process. This function might be used to facilitate statistical data analysis outside the standard analysis and reporting that is integral to the IRM system. The wizard also provides the ability to navigate around dynamic database content and structures.

g) Tasking & Workflow

Workflow allows repeatable patterns of activity to be defined, organised and accomplished in prearranged order. It is therefore the perfect accompaniment to 'playbooks or other initiatives used to establish and define a response strategy (as a series of tasks) for different types of incident. The IRM system allows Workflows to be defined for a range of outcomes and therefore for deterministic and planned responses to be defined for different crisis types.

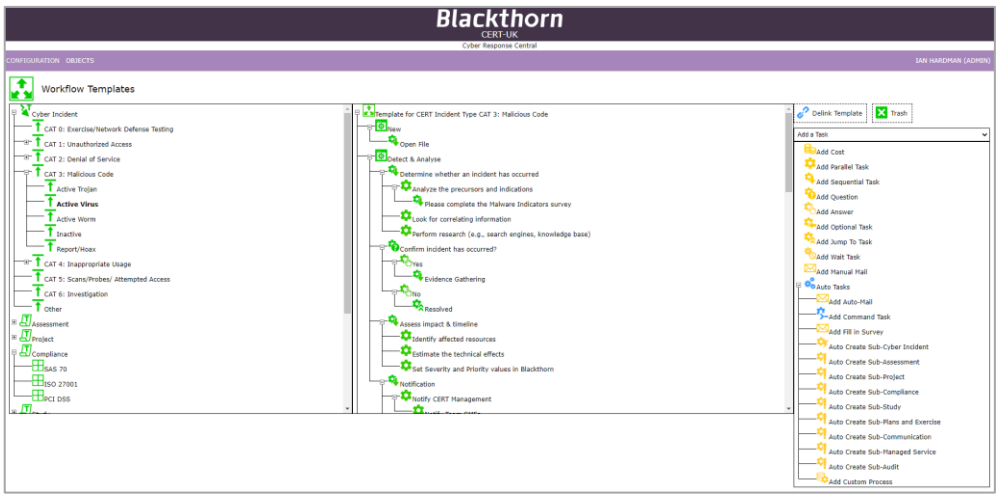

Figure 3: Workflow configuration using drag and drop

Minor deviations to a workflow are allowed to accommodate the specific and unique needs of a developing incident. Incident specific deviations do not affect the master workflow definition.

With Workflow, work activities (Tasks) in support of a response can be dynamically assigned to members of the Incident Response Team or a wider group. Workflow coordinates the conduct of such work 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.

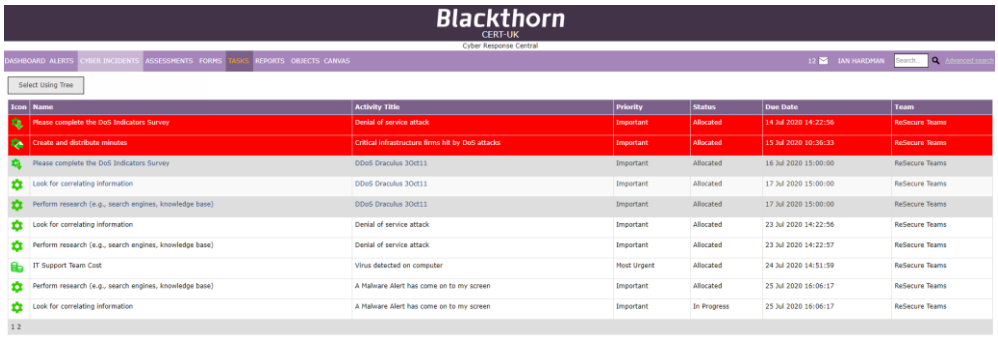

Figure 4: Dashboard: Task status across all activities

While 'Tasking' is integral element of the Workflow function, additional 'Ad-hoc' tasks can be created as part of workflow, or independently, to address the immediate needs of the response effort. Tracking tools provide full visibility of the status of tasks, including child tasks, highlighting lateness and/or overrun.

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

h) Alerting and Notification

Multiple channels are available for alerting and notification. Dashboards provide Incident Response Team members with details of actionable tasks awaiting their individual or collective attention. Email alerts and notifications can be triggered manually or by workflow, raising awareness without the need for the addressee to log-on. Internal messaging is a succinct method of communicating with other IRM 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).

i) 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) ensures 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.

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 you (a.k.a. Data Controller).

k) Remote working

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

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

I) Interoperability

A library of pre-existing web services (Open API compliant and RESTful[6]) 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[7], the vehicle enabling email, is ubiquitous, making it a very open and accessible channel for information exchange.

Features and Benefits

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

[6] RESTful API is an application programming interface (API) that uses HTTP (Hyper-Text Transfer Protocol) to GET, PUT, POST and DELETE data, which is stateless.

[7] Secure Mail Transfer Protocol

eGRC Platform

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

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

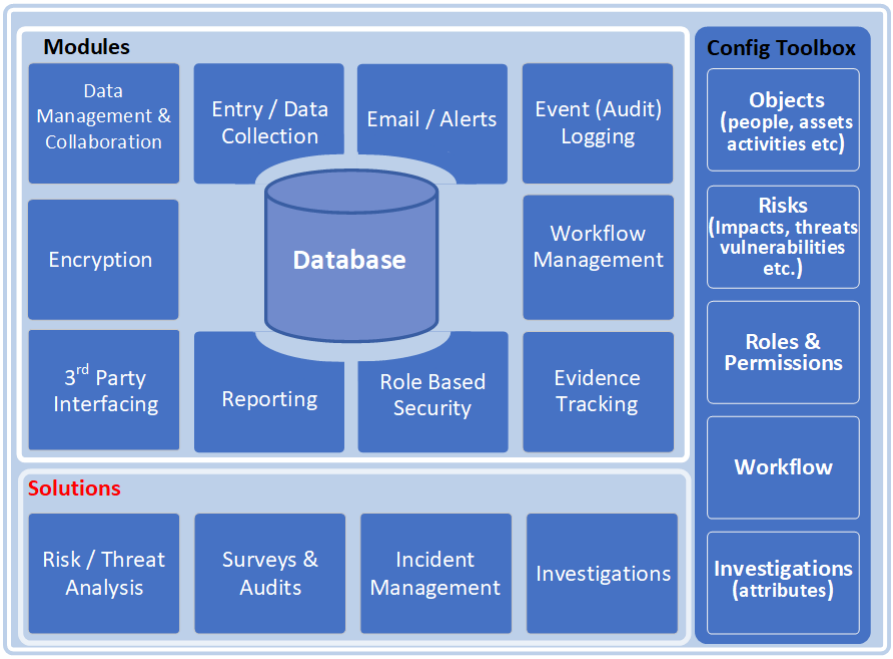

Figure 5 eGRC Platform Architecture

The web technologies employed 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, all of which are regularly refreshed and updated by Microsoft.

Our GUIs employ 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 Incident Response Management solution is available with full database encryption and channel encryption (secure link between the browser and the 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 are planning to store.

We can offer single tenant or multi-tenanted hosting environment suitable for keeping data secure up to IL3/OFFICAL. 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 software availability is better than 99.95% meaning access to reliable and secure data, without compromise.

Service Architecture

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

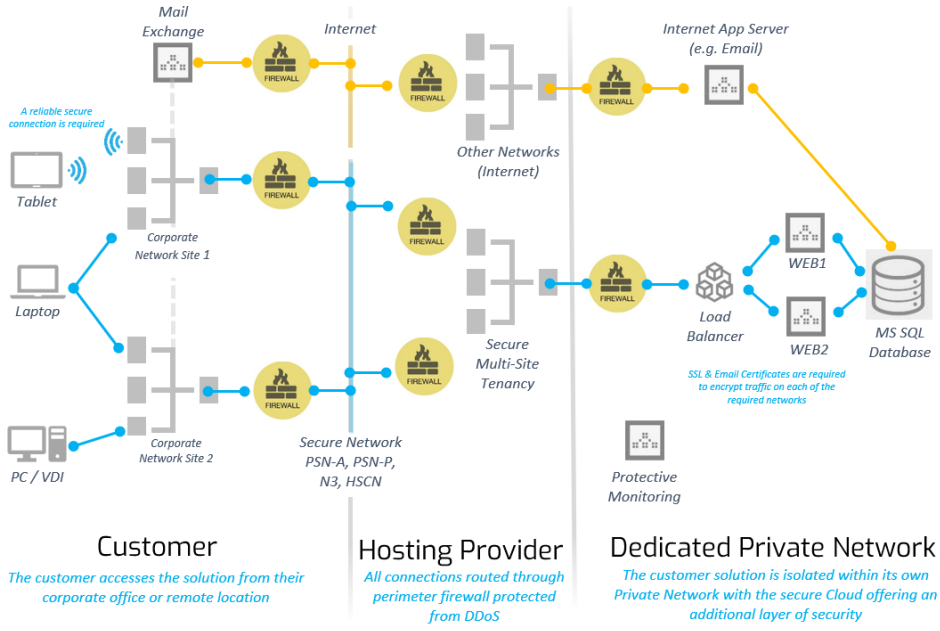

Figure 6: Dual Web Server suitable for hosting Official Sensitive Information

Our standard Government hosting solution (figure 6) 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 extant, secure wide area networks. Duel

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

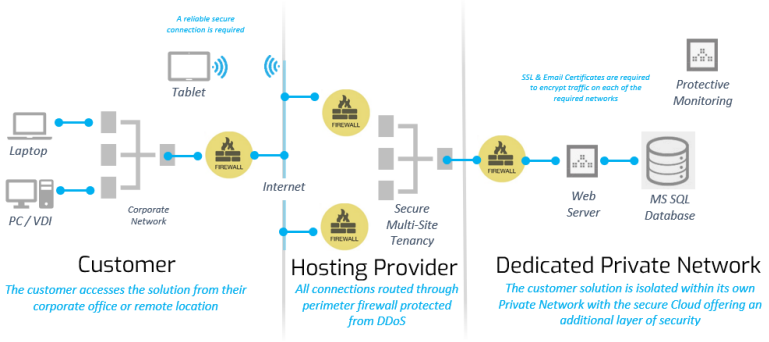

Figure 7: Single Web Server suitable for hosting Commercial Information

Where data security targets are less demanding, we can provide hosting with a commercial hosting provider (Figure 7). The service is accessed over the internet with channel and database encryption as required. Figure 7 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.

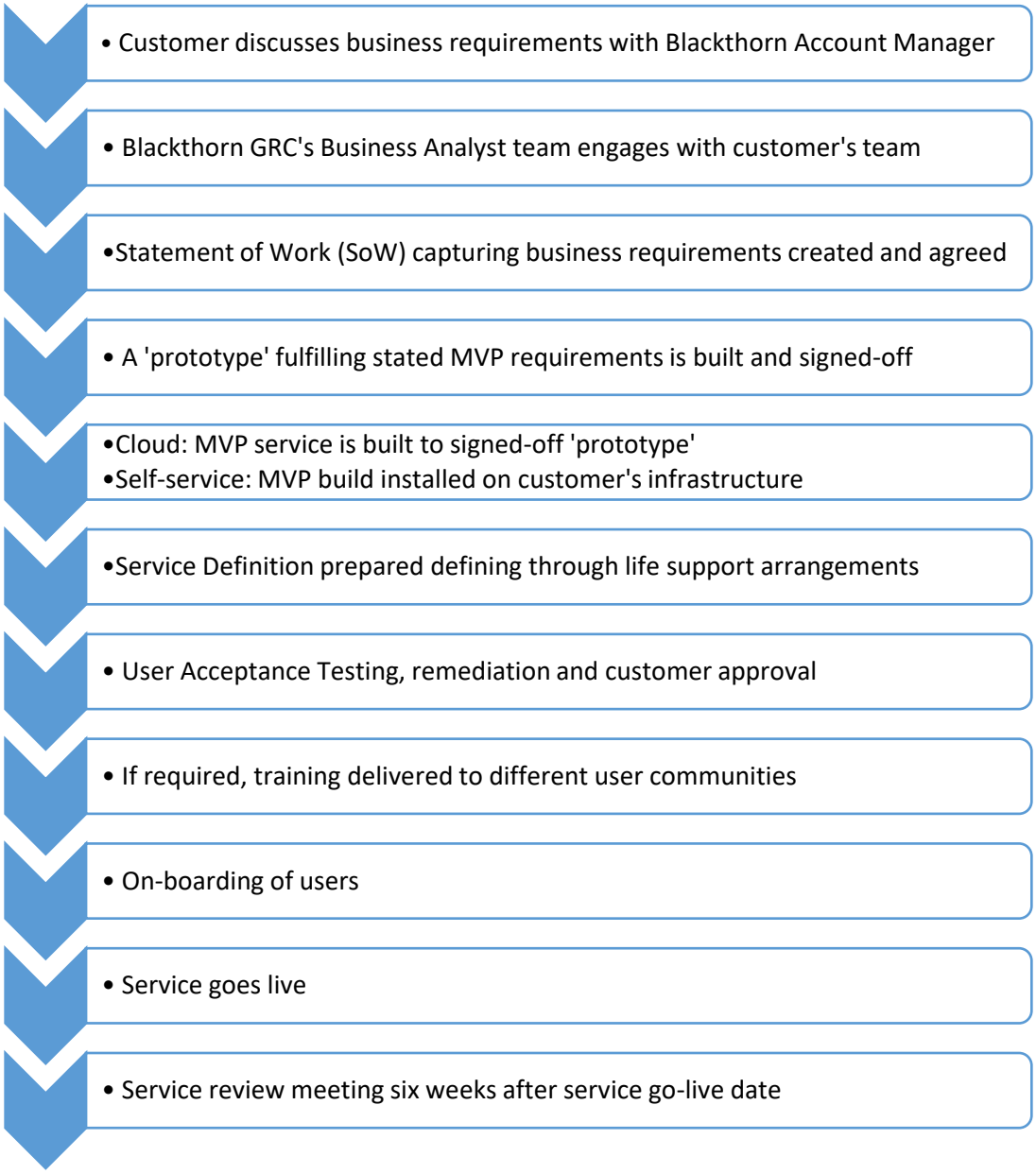

Figure 8: On-boarding stages

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

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

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

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

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

Service Provisioning Time

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

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

Service De-provisioning Time

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

Service Delivery

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

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

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

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

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

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

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

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

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

- Change Management
- Service Desk response SLAs
- reporting frequency
- meeting schedules.

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

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

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

Off-Boarding

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

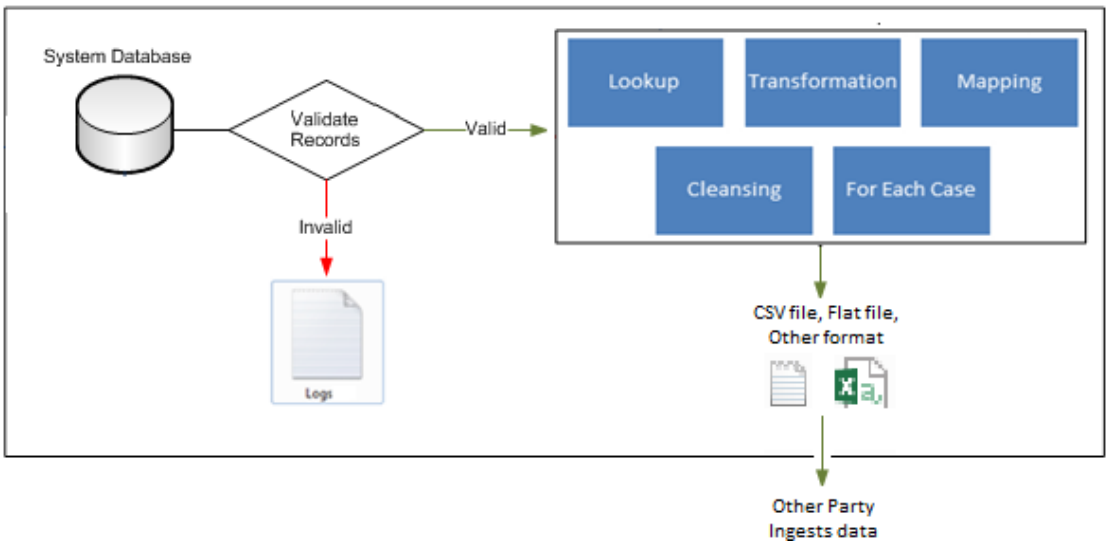

Figure 9: Data migration process

The data migrating process could involve:

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

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

Figure 9 illustrates the process at high level.

Response Times

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

Priority	Description	Initial Response	Resolution
P1 **Major Business Impact**	Product/service defect has a substantial effect on business operations with no available work-around. Results in complete loss of service for end-users, immediately impacting the clients of end-users. An error or failure where: • User(s) unable to access service • Necessary work unable to proceed • No immediate work-around available.	RT: < 2 hours Acknowledgement of receipt of Support Request and supply of Case Reference No. If there is an obvious and tenable workaround, this will be proposed as a short-term fix to enable necessary work to continue. If 'work-around' acceptable, priority level of support request might be reduced to P2 (only with customer's approval).	RT: Initial Response + < 8 hours Restoration of service to its previous operational state giving access to all normal 'end-user' services. Caveats: a) Recovery involving fail-over to secondary data centre – 24 hrs RTO b) Recovery action that addresses symptoms rather than cause (i.e. work-around) might require follow-up investigation, analysis, and remediation. This work will be carried out under the auspices of separate Remediation Plan and progressed as a P2 incident c) Assistance will be provided with networking issues between data centre and end-users but RT does not apply.
P2 **Significant Business Impact**	Business operations impacted with a significant reduction in performance or capacity (processing or bandwidth). Business operations able to continue but if defect not resolved there will be	RT: < 6 hours Acknowledgment of receipt of Support Request and supply of Case Reference No. Supply of initial diagnosis. If there is an obvious and tenable work-around that	RT: Initial Response + < 5 working days Supply of work-around to as temporary means of recovering business operations. Supply of interim release (or scheduled maintenance release) to remediate issue and return service to full operational state.

	medium to longer term consequences. Possible 'workarounds' are labour intensive affecting performance and productivity but offer an acceptable short-term solution. An error or failure where: • Users still able to access service • Performance reduced • No Workaround available.	provides a stop-gap solution, this will be proposed. Agree plan that addresses cause and provides permanent fix.	Plan any further software releases necessary for permanent fault correction.
P3 **Minor Business Impact**	Non-essential business function is unavailable causing a degree of inconvenience but without any significant impact on operations. An isolated error or issue where: • Users still able to access service • Loss of some specific capability • No loss of system performance • Workaround is available.	RT: < 2 working days Response as for P2 incidents.	RT: Initial Response + < 10 working days Response as for P2 incidents.
P4 **No Discernible Business Impact**	All other types of issue including: • 'How-to' questions • Supply of documentation • Cosmetic changes to GUI, dashboards or reports.	RT: Best Endeavours Acknowledgment of receipt of Support Request and supply of Case Reference No. (if matter cannot be immediately resolved). Agree nature and timeframe for resolution of issue.	RT: Best Endeavours Deliver outlined solution within agreed timeframe.

Table 1: Blackthorn standard SLA for support

Raising a Support Request

There are several routes to raising a support ticket with Blackthorn's Help Desk. These include telephone, email and via Blackthorn's support portal – see Figure 10.

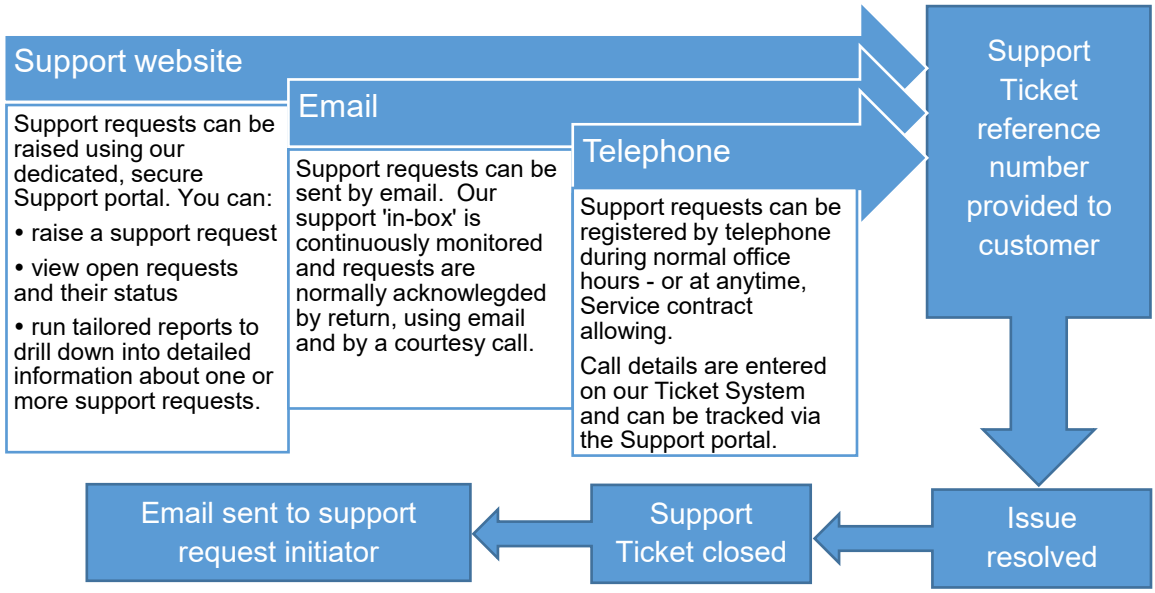

Figure 10: Raising Support Requests

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