G-Cloud 15

Service Definition

RiskFlag ISO Accredited Safety Case, Bow Tie and Risk Software

Lot 2b Cloud Software

1. Introduction

Company Overview

RiskFlag is an SME, founded with the goal of improving risk management processes. Two of the founding members are ex-military aviators who all transitioned from flying to safety roles within their service. We apply our knowledge and expertise, along with engineering and aerospace risk management techniques to a broad range of business risk challenges.

We develop specialised software based on our deep understanding of the principles of risk management, including safety case, risk register, bowtie, assessment, assurance, presentation and reporting modules. The software is built with the following three principles in mind:

Accountability | Enhance accountable people's understanding of risk. Present a clear risk picture while engendering the right safety behaviour.

Efficiency | Use technology to do what it is good at, rapidly, giving your team space to do its job better.

Communication | All stakeholders can contribute and collaborate with each other.

RiskFlag is based in Sheffield with team members working remotely around the UK.

We work directly with organisations of all sizes from a range of sectors including housing providers, local councils, Defence, aviation and other high risk industries.

Value Proposition

As part of the new regulatory requirements of the Building Safety Act 2022 (BSA 22), the Building Safety Regulator (BSR) has introduced a safety case regime to oversee the management of building safety risks in Higher-risk Buildings (HRB). This new approach provides greater assurance that risks have been assessed and proportionate steps are in place to manage them on an ongoing basis, ensuring residents are safe in their homes.

Under the new regime, the Principal Accountable Person and Accountable Person(s) are required to assess building safety risks, take all reasonable steps to prevent such risks materialising and limit the impact should an incident occur. To comply with this requirement, a safety case must be produced for each building, with a safety case report provided to the BSR on request.

The safety case must present a coherent argument, supported by appropriate evidence, that the building is safe from the spread of fire and structural failure. RiskFlag's digital safety case is a market leading software solution that facilitates compliance with the regulation. RiskFlag has approximately 65 organisations managing HRB safety cases in the platform, ranging from the largest local authorities and housing associations in England. The safety case software is based on the Military Aviation Authority's endorsed Claim – Argument – Evidence approach and has been tailored to the specific needs of the housing sector including detailed Key Building Information (KBI), assurance frameworks and building related content.

We recognise the challenge of manually writing a report; it is very time consuming and is subject to configuration control and accuracy issues. The embedded word processor which is used to write the body of the report provides a single version of the truth into which all permitted users can input.

With our system, it's possible to rapidly develop safety cases at scale while maintaining a consistent output. This improves efficiencies in safety case management and development, saving the client time and money and not wasting effort in mundane, repetitive tasks that a computer can do in seconds. The structure of the report output is clear and convincing and guides the BSR Assessor through the report in such a way as to significantly limit the time (and associated hourly cost) it takes to review it.

The tool provides the end-user with a high degree of flexibility meaning they can add, remove, and edit the entire structure of the safety case. KBI can also be added as required and connected to various elements of the safety case.

Building risk assessments are carried out using the bowtie and/or risk register modules. The risk register module lets the user conduct a robust Hazard Identification (HAZID) of the HRB, and the assessment module lets the user define the risk using user generated risk matrices. Bowtie barriers can be connected to various elements of the safety case, creating a joined up, coherent risk picture for the Principle Accountable Person to use as a basis for sound risk-based decision making. Resource constrained organisations can therefore prioritise where to allocate time and effort and maximise precious resources.

The Occurrence Reporting module links incident data to barriers and elements of the safety case, providing essential feedback and closing the loop on the risk management process.

In addition to the HRB safety case proposition, the RiskFlag platform can be used for the development and management of an air system's Air System Safety Case (ASSC), as defined by the Military Aviation's Authority's (MAA's) regulation Regulatory Article 1205. The RiskFlag platform follows the guidance provided in the Manual of Air System Safety Cases (MASSC). In addition, the platform can be used by organisations under the MAA's Contractor Flying Approved Organisation Scheme (CFAOS).

What the Service Provides

RiskFlag's comprehensive suite of cloud-based digital risk management tools provide enhanced oversight of risks, be it for HRB or air systems, fostering accountability within the organisation.

Designed with modularity in mind, the safety case application seamlessly integrates with other RiskFlag modules, such as risk register, bowtie and assessment. The software streamlines the handling of safety cases and risk information. Its user-friendly interface ensures a straightforward onboarding and training process, minimising the challenges of team turnover.

Furthermore, RiskFlag experts are available at an extra hourly rate to assist in defining the safety case methodology and providing remote expert support.

Users can effortlessly export high-quality, company-branded Safety Case reports from the system at any moment and view the dashboard for an overview of the status of the safety case. A HRB Safety Case Report can be exported for the BSR at a press of a button; a zip folder of all the evidence can also be downloaded with a single button press, with all the files automatically renamed in the required BSR format.

Bowties can be created within the system or imported from BowTieXP. Metadata can be added to each bowtie element to create a full risk picture and controls connected to the safety case.

An organisation's risk matrix can be developed in the platform and a risk registered developed, such as a HAZID.

Occurrence data can be connected to the bowtie to validate barrier effectiveness and inform risk-based decision making.

Social Value

RiskFlag supports social value activities including, kickstart of economic growth initiatives, initiatives that break down barriers to opportunity for graduates trying to find their first role in the workforce, and green initiatives, to help Britain become a clean energy superpower.

We have opened an IT hub in Sheffield and employ graduates from their courses, ensuring that we pay above the National Living Wage. We also provide training courses to advance their careers. This ensures that hi-tech roles remain in the area.

We are sponsoring a software developer with his university thesis on the subject of AI in risk management. We are an equal opportunities employer – 2 of our 7 staff are veterans and one of the senior leaders is female.

To support Britain becoming a clean energy superpower, we have chosen to work with a start-up that is making renewable powered aviation a reality, for a reduced fee.

We invest in the health and well-being of the RiskFlag team. We provide employees with more than the statutory minimum paid leave allowance. We have provided our team with an office in Sheffield which has leisure facilities, to ensure that they have a choice of working from home or in the office. We check in with staff via various channels (in-person, virtual meetings, telephone calls, messaging) every day. We therefore understand their workload and can solve problems before they escalate.

It is the responsibility of RiskFlag’s Commercial Director to define the social value budget for the coming year. It is a minimum of 2% of the forecast software revenue. Each social value activity is defined using SMART objectives and tracked via the RiskFlag accounting package.

Overview of the G-Cloud Service

The software assists organisations in complying with the portion of the Building Safety Act 22 that demands an active safety case be in place for all High-Risk buildings.

The software is accessible from any device with a web-browser. It has an embedded word processor for the production of high-quality reports, eradicating version control issues and facilitating collaborative input. The report can be customised with templates and branding and exported at the click of mouse.

Document links from the report take the reader directly to the evidence location or speak to us about API options for seamless data linking. Photos, screen shots and documents can also be stored directly within the RiskFlag system if required.

Users can create custom safety case templates to drive consistency through the organisation. Templates also connect to Key Building Information and reports.

We know that organisations with large property portfolios need to scale their output, and this can be done swiftly and accurately using the safety case clone feature. Carry across user defined elements (such as claims, arguments, evidence, users, scores, documentation, delivery plans) from one safety case to another.

With the purchase of a RiskFlag licence, the safety case module can be connected within the platform to the bowtie, risk register, assessment, reporting, compliance and presentation modules. The user can define the structure of each module to their requirements, develop their own Hazard Risk Matrix, for example. Having these modules in the same eco-system allows the user to have a clear understanding of risk and reduces workload when developing and managing a safety case.

The management dashboard can be configured to provide various views, including an overview of the status of the safety case, of tasks still to be completed or overdue and evidence that requires attention. The in-built workflow and notification system allows allocation and management of tasks within the application.

The safety case can be audited for activity and changes made, an essential part of a robust Safety Management System.

We have worked closely with Lewisham Council, an early adopter with the Building Safety Regulator to continuously improve the product. This has been based on regular feedback from the Building Safety team at Lewisham. This has now been extended to our 65+ HRB clients.

The key benefits they have experienced using the tool are:

- Provides Principle Accountable People with a very clear picture of the building risks for which they are accountable.
- Provides an auditable trail of accountability.
- Supports compliance with the Building Safety Act 2022
- It assists in the creation and management of the golden thread.
- Workflow management drives accountability
- Creates an auditable activity log of all interaction with the safety case.

- Manages evidence in a structured, rapidly accessible and efficient way, leading to significant time and cost savings when creating subsequent safety cases.
- Instantly creates safety case reports linked to valid evidence.
- Promotes safety case thinking within the organisation with minimal training requirements.

In addition to the HRB safety case offering, RiskFlag also offers ASSC support to Ministry of Defence (MoD) clients and CFOAS support to contractors supporting MoD.

Associated Services

Software maintenance and upgrades are part of the basic package.

Remote and on-site support services can also be provided for additional cost.

For an optional additional cost, an API is available, allowing advanced users to interact with the RiskFlag system via other applications. RiskFlag can also be configured to extract data from other systems using suitable APIs; this is a bespoke service requiring developer time.

Only static content can be uploaded (no videos).

Technical support is provided as part of the subscription cost. Other professional support services are on a case-by case basis IAW the pricing document. These include:

- Virtual software training – product manager
- Onsite risk management training – consultant
- Onsite Bow Tie or HAZID workshop – consultant
- Virtual safety case review - consultant
- API development – engineer
- Custom software developments - engineer

2. Data Protection

Information Assurance

RiskFlag is Cyber Essentials+ approved and is accredited to ISO9001, and ISO27001 standards.

The RiskFlag GDPR policy is a critical component of our data protection framework. Our policy is clear, concise and written in language such that employees can easily read and understand it and is available upon request. We regularly train our staff in data protection and communicate the policy to ensure its successful implementation and compliance.

One of the benefits of being a Micro organisation is that we know all our employees well and this personal relationship helps to ensure everyone adheres to company policy.

For new employees we clearly communicate all company policies and procedures during onboarding and periodically throughout their tenure.

All PDFs will meet WCAG 2.2 AA accessibility standards. The software application has achieved a 76% accessibility score, and we are working towards full WCAG 2.2 AA compliance.

We also conduct regular training sessions to educate employees about policies, particularly those related to compliance, safety, and ethics, using various formats, such as in-person training, online modules, and workshops to accommodate different learning styles.

We require employees to acknowledge that they have read and understood the policies on an annual basis via an email confirmation.

We periodically review and update policies to keep them current with changing laws, regulations, and industry standards.

Data Back-Up and Restoration

Automated auditing of the software stack provides fast notification of any threat, vulnerability or exploitation. Scanning tooling is built into the containerisation technology, and software dependency auditing tools are also implemented. All vulnerability issues are investigated and triaged, with the most severe given top priority.

Data is backed up daily on a different site to the main server.

The disaster recovery plan would see the service transferred to secondary nominated VPS provider via tested method with expected turnaround time of less than 2 hours.

Malware protection is dealt with via multiple layers of security:

- We do not allow malware to gain a foothold within the system, or any systems that connect to it, by ensuring:

  - Well configured firewalls on servers and offices
  - Development using secure laptops only.
  - Strong passwords required for everything.
  - MFA required for all administrative actions.
  - Rate limiting & lockout is in place.

- We ensure that if there is potential for a breach, the CTO / CISO are notified immediately.
- Software supply chain dependencies automatically scanned on a daily basis.
- All login attempts are emailed out for review immediately

Business continuity statement/plan

We have a Business Continuity document that describes our disaster recovery plan. The policy is disseminated throughout the organisation and available to all on the shared site. The policy is reviewed annually and updated if required and is available upon request.

Alongside the BCP is the risk register – this is reviewed every 6 months and mitigations are checked for validity and effectiveness. New risks are added to the register as they become apparent. To identify risks, we have a rigorous HAZID process that incorporates feedback from clients, feedback from staff, reporting and information from risk assessment workshops.

Privacy by Design

Our proactive approach to security is deeply ingrained in every aspect of our service to ensure the utmost protection of user data and compliance with privacy regulations. By combining the proactive measures listed below we aim to provide a secure and compliant environment for our users, demonstrating our commitment to data protection and privacy in accordance with GDPR standards.

- Data Encryption. We employ robust encryption protocols to safeguard sensitive information at all stages of data transmission and storage. This encryption ensures that unauthorised parties cannot access or intercept any data exchanged within our system.
- Regular Security Audits and Assessments. Our security measures undergo frequent assessments and audits by independent third-party experts. This proactive approach helps us identify potential vulnerabilities and address them promptly, ensuring that our security protocols are continually strengthened.
- Access Controls and Authentication. We implement strict access controls and multi-factor authentication mechanisms to ensure that only authorised persons can access sensitive data. This reduces the risk of unauthorised access and enhances overall account security.
- Data Minimization. Our service adheres to the principle of data minimisation, meaning we only collect and retain the data necessary for the intended purpose. This reduces the risk associated with unnecessary data exposure and ensures compliance with GDPR principles.

- Privacy by Design. Our platform is designed with privacy in mind from the ground up. We integrate privacy features into our service architecture, ensuring that user data is protected by default rather than as an afterthought.
- GDPR Compliance Features. We have incorporated specific features within our service to facilitate GDPR compliance. This includes functionalities such as data access and deletion requests, allowing users to manage their personal information in accordance with GDPR requirements.
- Incident Response Plan. In the unlikely event of a security incident, we have a well-defined incident response plan in place. This enables us to respond promptly, mitigate the impact, and communicate transparently with affected parties.

3. Using the service

Ordering and Invoicing

The process for ordering is managed on a case-by case basis. The initial request is sent by email to Info@riskflag.com.

This is followed by a demonstration of the software.

Clients have the option of conducting a 5-day free assessment, in which the following success criteria will be reviewed and assessed using a survey at the end of the period (criteria may be amended on a client-by-client basis):

- User engagement with the digital safety case - Speed with which an individual can be up and running on the system with minimal training.
- Time saved in management of the live safety case – a subjective assessment to be made by the building safety managers.
- Ease of interaction with linked evidence.
- Speed and simplicity of report creation.
- Auditability of the safety case.
- Speed and accuracy of roll out of all safety cases compared to using Word or Excel.
- Other specific success criteria for the assessment.

Once satisfied the tool meets the needs of the organisation, we will discuss additional requirements such as professional services or module add-ons.

Following the free assessment and prior to onboarding all users, we require the emails of all users. The account manager will set up all users on the system and arrange a time for a 90-minute onboarding session.

Availability of Trial Service

Software assessments are available on a case-by-case basis, with defined assessment criteria, for a maximum of five working days.

On-Boarding, Off-Boarding, Service Migration, Scope etc.

RiskFlag has a robust Customer onboarding process, which includes the signing of NDAs where appropriate and Software as a Service (SaaS) and Services Agreements. Prior to agreeing a SaaS or Services agreement, the RiskFlag account manager agrees a Software Service Request to include scope, deadlines, budget and unique requirements. The Service Request document is used to clearly and accurately capture and agree the customer's requirements.

We use an automated tool for managing our customer onboarding process, in which we create, track, automate, and complete tasks to streamline processes and improve efficiency.

Customer requirements are scoped and agreed with the customer and RiskFlag Subject Matter Experts (SME) prior to the definition of a Service Request that:

- Defines the Customer requirements.

- Defines the RiskFlag solution.
- Defines the RiskFlag deliverables, with Key Performance Indicators where required (KPI).
- Defines the RiskFlag assumptions.
- Defines any contract milestones, which includes a review at agreed stages within the contract.

The Service Request document is presented to the Customer for agreement. At the review (ideally conducted face-to-face) RiskFlag SME review the status of contract with the customer to ensure customer satisfaction, bench-marked against the agreed deliverables, KPIs and customer requirements.

Onboarding of all users starts with a free 90 minute kick of meeting.

A free follow-up meeting of up to 90 minutes is then held with the system administrators.

Additional onboarding sessions are available, these are charged as per our pricing document.

Professional services such as guidance on how to create a safety case or build a safety management system are defined in the pricing document.

Training

- Initial on-boarding includes training on the key features.
- Follow-up 90-minute sessions can be used for training, these are charged as per our pricing document.
- Online "how-to" videos
- In-application help and guidance
- Guidance documentation
- Additional paid for training is available, as defined in the Pricing Document

Implementation Plan

A detailed implementation plan can be provided to the buyer on request.

Service Management

- Maintenance window is outside normal weekday working hours.
- Customisation by written agreement on a case-by-case basis
- Feature deprecation is a 6-month process.
- There are no ITSM procedures / standards in use.

At RiskFlag we have a defined process to manage customer requirements, deliver on agreed timescales and manage expectations. The process is as follows:

Capture Customer Requirements:

- We start by collecting all relevant information from the customer. This may include written requests, phone conversations, emails, or forms. All data is

captured and stored in our CRM software. Our teams are trained to check that the requirements are specific, clear, and documented.

Record and Document:

- We create a comprehensive record of the customer's requirements in the form of a Service Request. The Service Request includes all relevant details such as scope, deadlines, budget, and any additional requirements.

Review and Validation:

- We review the customer's requirements with the relevant teams and stakeholders to ensure they are feasible and well-understood. At this point we will clarify any ambiguities or discrepancies.

Planning and Scheduling:

- We develop a detailed plan for how the requirements will be met. This plan includes a timeline, resource allocation, and task assignments which are managed through our Process software and CRM. We ensure that the schedule aligns with the customer's expectations and agreed-upon timescales.

Resource Allocation:

- We allocate the necessary resources, including and Account Manager at this point, to meet the customer's requirements and ensure that the team responsible for the project is fully briefed and equipped to manage their responsibilities.

Service Constraints

- Maintenance window is outside normal weekday working hours (1800 – 0600 UK time). Users will be notified of any planned maintenance.
- Customisation by written agreement on a case-by-case basis
- Feature deprecation is a 6-month process

Service Levels

RiskFlag uses commercially reasonable endeavours to make the Services available 24 hours a day, seven days a week, except for:

(a) Planned maintenance carried out during the maintenance window of 1800hrs to 0600hrs UK time; and

(b) Unscheduled maintenance performed outside Normal Business Hours, provided that the Supplier has used reasonable endeavours to give the Customer at least 6 Normal Business Hours' notice in advance.

We aim to respond to customer queries, complaints and feedback within the agreed timeframe, which is based on the following:

- The specifics of the customer
- The expectations of our customer based on what our competitors do.
- Our own internal goals for response time.

- What channel the enquiry is on

For technical issues, our standard response times are detailed below:

Critical
- Complete loss of service or a critical functionality, impacting all users.
- Acknowledgment; 2 hours.
- Resolution or workaround; 1 working day.

High
- Major functionality is impacted, affecting a significant number of users.
- Acknowledgment; 4 hours.
- Resolution or workaround; 2 working days.

Medium
- Noncritical functionality is impacted, affecting a limited number of users.
- Acknowledgment; 3 days.
- Resolution or workaround; 1 working week.

Low
- Minor issues that do not significantly impact functionality.
- Acknowledgment; 4 working days.
- Resolution or workaround; proportionate timeframe.

We have an integrated customer communications platform in place to manage customer relationships within our applications. The software itself supports us in evaluating our customer interaction by channel, busiest time and trending topics and create reports, highlighting areas of success and areas for improvement.

Outage and Maintenance Management

The risk of technical issues causing delays is mitigated via:

- Outage avoidance:
  - stringent validation and testing are employed throughout the development process.
  - pre deployment validation
  - staggered rollout
- Service performance planning.
  - continuously monitor system load to identify any performance issues before they become noticeable to end users.
  - caching strategies to reduce load on the systems.
  - review capacity planning strategy on a regular basis.
- Measure downtime.
  - system health is continually monitored with logs going back a minimum of 30 days.
  - log and analyse cause, duration, and impact of any downtime.

    - implement preventative measures based on the analysis forming continual feedback loop
- preparedness for ad-hoc service needs
    - we maintain flexible infrastructure that can be easily scaled.
    - we employ rapid deployment techniques to quickly update systems and infrastructure as and when required.
    - we have a robust disaster recovery plan.

Financial Recompense Model for not Meeting Service Levels

We do not offer service credits for not meeting service levels.

4. Provision of the service

Customer Responsibilities

In relation to the Authorised Users, the Customer undertakes that:

- the maximum number of Authorised Users that it authorises to access and use the Services and the Documentation shall not exceed the number of User Subscriptions it has purchased from time to time which at the Effective Date is as set out in Schedule 1.
- it will not allow or suffer any User Subscription to be used by more than one individual Authorised User unless it has been reassigned in its entirety to another individual Authorised User, in which case the prior Authorised User shall no longer have any right to access or use the Services and/or Documentation.
- each Authorised User shall keep a secure and confidential password for their use of the Services and Documentation, in accordance with the Customer's own internal IT security protocols.
- it shall maintain a written, up to date list of current Authorised Users and provide such list to the Supplier within 5 Business Days of the Supplier's written request at any time or times.
- it shall permit the Supplier or the Supplier's designated auditor to audit the Services in order to establish the name and password of each Authorised User and the Customer's data processing facilities to audit compliance with this agreement. Each such audit may be conducted no more than once per quarter, at the Supplier's expense, and this right shall be exercised with reasonable prior notice, in such a manner as not to substantially interfere with the Customer's normal conduct of business.
- if any of the audits referred to in 2.2(e) reveal that any password has been provided to any individual who is not an Authorised User, then without prejudice to the Supplier's other rights, the Customer shall promptly disable such passwords and the Supplier shall not issue any new passwords to any such individual; and
- if any of the audits referred to in 2.2(e) reveal that the Customer has underpaid Subscription Fees to the Supplier, then without prejudice to the Supplier's other rights, the Customer shall pay to the Supplier an amount equal to such underpayment as calculated in accordance with the prices set out in 1 of Schedule 1 within 10 Business Days of the date of the relevant audit.

The Customer shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the Services and/or the Documentation and, in the event of any such unauthorised access or use, promptly notify the Supplier.

Technical Requirements and Client-Side Requirements

The client requires a web-browser.

The client requires a web enabled device (PC, laptop, tablet, mobile phone). The user experience is designed for PC/laptop and may be degraded when viewed on a tablet or phone.

Outcomes/Deliverables

Live building safety case through the life of the building

Bowtie diagram exports

Building Safety case report

Development life cycle of the solution

We have adopted the Agile methodology for software development in our projects.

Identify Problems/Needs:

During the initial phase, we engage with stakeholders to gather requirements and understand their needs. This involves conducting interviews, surveys, and analysis to comprehensively capture the problem statement and user expectations.

Plan:

We break down the project into manageable units or 'sprints', typically lasting 2-4 weeks. Each sprint begins with a planning meeting where the team selects tasks from the product backlog, which is a prioritised list of work to be done.

Design:

The design phase in each sprint involves creating prototypes or wireframes, which are then reviewed with stakeholders. This iterative design process allows for regular feedback and adjustments early in the development cycle.

Build:

The development team works on the tasks defined for the sprint. The focus is on creating a potentially shippable product increment by the end of each sprint. Continuous integration is practiced to merge changes regularly and detect issues early.

Test:

Testing is integrated throughout the sprint. This includes automated unit tests, integration tests, and manual testing to ensure the quality and functionality of the software. Feedback from testing is used to make immediate improvements.

Deploy:

At the end of each sprint, the new increment of the software is reviewed and can be deployed to a production environment. This frequent deployment cycle allows stakeholders to start using the latest version quickly and provide real-world feedback.

Maintain:

Post-deployment, we focus on maintaining and updating the software. This involves monitoring performance, fixing bugs, and continuously refining the product based on user feedback and changing requirements.

Review and Adapt:

After each sprint, we conduct a retrospective meeting to reflect on what worked well and what could be improved. Insights gained from these meetings are used to refine our processes and practices in subsequent sprints.

By employing Agile, we maintain a high degree of flexibility and responsiveness to change, ensuring that the final product aligns closely with user needs and expectations. This methodology fosters collaboration, adaptability, and continuous improvement in our software development process.

After-sales Account Management

Execution:

- We implement the plan and execute the tasks according to the agreed-upon schedule. A series of contract monitoring milestone meetings, regular customer check-ins via the Account Manager and ad-hoc contact allows us to keep a close eye on progress and address any issues that may arise in a timely manner.

Quality Assurance:

- We maintain a rigorous quality assurance process that ensures the delivered product meets the customer's requirements and expectations.

Communication:

- It is vital for everyone at RiskFlag to maintain open and transparent communication with the customer throughout the process. We provide regular updates on progress, notify them of any changes or delays, and address any concerns promptly.

Monitoring and Control:

- Our teams continuously monitor the project's progress against the schedule and adjust as necessary to ensure that it stays on track.

Delivery:

- The delivery phase sees the RiskFlag product being provided to the customer within the agreed timescales. We ensure that all necessary documentation, training, and support as specified in the requirements is provided to the highest standard.

Customer Feedback and Evaluation:

- We seek feedback from the customer on the delivered product and use this feedback to evaluate the process, feed into our KPIs and make improvements for future projects.

Termination Process

Contracts are paid for annually in advance. Our standard terms and conditions make clear that the software and associated IP is owned by RiskFlag, but clients are the identified owner of any data they choose to store in the system and RiskFlag will return any stored data to the client in a mutually agreeable format (e.g. .zip file) on contract termination. Buyers can give 90 days notice for any reason for termination.

5. Our experience

Case Studies

1.Lewisham Council

RiskFlag has been working with Lewisham Council on the development of their HRB Safety Cases since early 2023.

The problem

The team at Lewisham had identified the following problems:

- Accountable people do not always give due consideration to the conclusions within the safety case.
- There is no mechanism for managing the safety case on an ongoing basis.
- It is difficult to hold people to account using a Microsoft word document.
- Embedding evidence within Word creates a very large document, which appears not to be tolerated by the HSE.
- People cannot actively interact with the safety case.
- It is impossible to know who has interacted with the safety case and when.
- The manual creation of safety cases is very time consuming and inefficient.
- Non-experts were overwhelmed by the apparent complexity of the safety case when presented in Word.

How RiskFlag solved the problem

After 9 months of using the software, the Building Safety team at Lewisham have cited the following benefits and improvements in the way they write and manage safety cases:

- Provides Accountable Persons with a clear picture of the building risks for which they are accountable.
- Provides an audit trail of safety case interaction.
- Workflows drive interaction and accountability.
- Evidence is managed in a structured, accessible and efficient way, leading to significant time and cost savings compared to how we were doing it before.
- Promotes a positive safety culture within the organisation.
- Safey cases can be scaled rapidly, meaning we are far more efficient and can use our time more effectively.

2.Combat Aviation, Ministry of Defence

RiskFlag was engaged to write the Air System Safety Case (ASSC) strategy report and then the ASSC acquisition basis report.

Our team of experts used their extensive knowledge of safety cases to write compliant strategy and acquisition basis reports.

Engaged via QinetiQ through the EDP, they said: “RiskFlag's innovative digital tools and expertise make them our go-to business for safety case solutions" QinetiQ.

“RiskFlag's work on the Air System Safety Case Strategy has been of a high standard, securing buy-in from the MoD’s approval authorities. I trust RiskFlag to deliver on-time and their expertise and support has contributed to the overall likelihood of success of the programme." MOD

The strategy report was scrutinised by the Military Aviation Authority and found to meet the requirements of the regulation.

Clients

Example clients include:

babcock™	Southwark Council	Lewisham
Camden	TOWER HAMLETS	Hackney
Lambeth	Hyde	the guinness partnership
L&Q	Berkeley Group	Sanctuary
VERTICAL	beaufort	Nova Systems

Contact Details

Mark Keeble

mkeeble@riskflag.com

07979604749