SERVICE DESCRIPTION

Table of Contents

1 Service Overview.

1.1 What is PROVA Risk.

PROVA Risk is a secure, cloud-based SaaS platform that enables organisations to achieve, demonstrate, and maintain compliance with the Terrorism (Protection of Premises) Act (2025) by translating statutory requirements into a structured, defensible, and auditable compliance workflow. The service enables duty holders to:

- complete a Terrorism Reasonably Practicable Test, assessing what is proportionate and defensible for a given site or building in line with the Act.
- develop, implement, and maintain site- and building-level terrorism protection procedures, including evacuation, invacuation, lockdown, and communications arrangements.
- facilitate automated training and exercising cadences for all relevant staff through PROVA Risk's proprietary Learning Management System, including tracking completion of training and exercises.
- store and manage all compliance evidence required to demonstrate that proportionate and defensible steps have been taken under the Act, supporting regulatory assurance, inspection, and audit activity.

The service is designed to support buyers seeking a repeatable, scalable, and low-burden mechanism for meeting statutory counter-terrorism preparedness duties across single or multiple premises.

PROVA Risk supports dutyholders in understanding and operationalising statutory requirements, but it does not provide legal advice and does not replace the Responsible Person's obligation to ensure compliance with applicable law.

1.2 Primary compliance outcome.

The primary outcome of PROVA Risk is to support dutyholders in demonstrating that they have taken reasonably practicable, proportionate, and defensible measures to reduce the risk of harm from terrorist acts, and that those measures are maintained, reviewed, and evidenced over time, in accordance with the Terrorism (Protection of Premises) Act (2025).

The platform is designed to support compliance for premises falling within scope of the Act, including those subject to both standard and enhanced duties, without requiring organisations to interpret legislation independently or develop bespoke compliance frameworks.

1.3 What the service does (in platform terms).

PROVA Risk delivers compliance through four integrated capability areas that align directly with statutory expectations under the Act:

- Terrorism Reasonably Practicable Test (core assessment engine). A structured, guided assessment process that enables dutyholders to determine what mitigation measures and procedures are proportionate for each site or building, taking account of risk, resources, and cost–benefit considerations. Outputs are recorded as a defensible audit trail.
- Implementation of reasonably practicable mitigation measures. The platform enables the practical implementation of outcomes from the Terrorism Reasonably Practicable Test, including:
    - simplified plan builders for evacuation, invacuation, lockdown, and communications procedures.
    - project-management functionality to assign responsibility, track progress, and evidence completion of required mitigation measures.

- Automated training and exercising via Learning Management System. A proprietary Learning Management System that:
    - automatically assigns training and exercise requirements based on site risk profile and duty level.
    - delivers training content including, where appropriate, via personal handheld devices.
    - tracks completion and participation for all relevant staff.

- Evidence retention and ongoing compliance management. A centralised evidence and assurance environment that stores all assessments, plans, training records, exercises, and reviews, enabling organisations to maintain compliance over time and demonstrate continued adherence to the Act.

1.4 How the service simplifies compliance.

PROVA Risk simplifies compliance by operationalising statutory requirements rather than requiring interpretation.

- The Terrorism Reasonably Practicable Test is powered by a dynamic assessment engine that automatically updates in response to changes in risk environment, site characteristics, or legislative and regulatory requirements, ensuring assessments remain current and defensible.
- Outputs from the test directly inform the implementation of proportionate mitigation measures and procedures, supported by structured plan builders and task management tools.
- Training and exercise requirements are automated, ensuring staff preparedness is maintained without reliance on manual scheduling or ad hoc processes.
- All activity is continuously recorded, removing the need for parallel document management or retrospective evidence gathering.

This approach reduces administrative burden while increasing consistency, transparency, and assurance.

1.5 Typical users and operating model.

The primary users of PROVA Risk are the Responsible Persons defined under the Terrorism (Protection of Premises) Act (2025). In practice, this includes:

- Local authorities and local councils, acting as duty holders for premises within their estates that fall within scope of the Act (including schools, leisure and recreation facilities, town halls, libraries, and community venues).
- Delegated responsible individuals, such as headteachers or site-specific managers, operating under local authority governance arrangements.
- Central government departments, including the Home Office, where aggregated and anonymised data may be used to understand compliance trends, assurance gaps, and preparedness maturity across sectors, in accordance with data protection law and applicable contractual terms.

The platform supports a hierarchical governance model, allowing responsibility to be delegated to site level while maintaining oversight, assurance, and consistency at organisational or national level.

1.6 Outputs

PROVA Risk produces structured, professional compliance outputs, including:

- site-specific Terrorism Reasonably Practicable Tests, clearly demonstrating what is proportionate and defensible under the Act.

- site- and building-level evacuation, invacuation, lockdown, and communications procedures, aligned to the outcomes of the Reasonably Practicable Test.
- training plans, training records, and completion evidence generated through the Learning Management System.
- exercise plans, scenarios, participation tracking, and outcomes, supporting preparedness validation
- a consolidated evidence base demonstrating ongoing compliance with the Terrorism (Protection of Premises) Act (2025).

All outputs are exportable in standard open formats and suitable for regulatory engagement, inspection, internal governance, and audit.

2 Key Service Features.

2.1 Terrorism Reasonably Practicable Test (RPT).

At the core of PROVA Risk is a Terrorism Reasonably Practicable Test (RPT), designed to operationalise the statutory requirement that public protection procedures are put in place *so far as is reasonably practicable*. The RPT provides a structured, auditable assessment of:

- the nature of the premises, including use, scale, occupancy, accessibility, and contextual risk.
- the resources available to the Responsible Person.
- the cost of mitigation in terms of money, time, and organisational effort.

These factors are balanced in line with established Fire Safety and Health & Safety principles to determine what is proportionate and defensible for each individual site or building. The RPT engine is dynamic, automatically updating assessments where:

- site characteristics change.
- risk context changes.
- statutory or regulatory requirements evolve.

Each completed RPT produces a site-specific, defensible record of what measures and procedures are reasonably practicable under the Act.

2.2 Determination of Appropriate Public Protection Procedures.

The outputs of the Terrorism Reasonably Practicable Test directly determine the appropriate public protection procedures required for each site or building.

For Standard Tier premises, this includes the four statutory procedures:

- Evacuation.
- Invacuation.
- Lockdown.
- Communications.

For Enhanced Tier premises, the same Reasonably Practicable Test applies, with outcomes reflecting increased risk, scale, or complexity where relevant. This ensures that procedures are:

- site-specific, not generic.
- proportionate, not excessive.
- legally defensible, not aspirational.

2.3 Simplified Plan Builders for Procedure Implementation.

PROVA Risk includes simplified, structured plan builders that enable Responsible Persons to implement the procedures identified by the RPT without requiring specialist drafting expertise. Plan builders are provided for:

- Evacuation procedures.
- Invacuation procedures.
- Lockdown procedures.
- Communications procedures.

The plan builders are designed to:

- remove unnecessary or misleading detail.
- support clarity under stress.
- ensure consistency between assessment, procedure, and training.

All procedures are explicitly linked back to the relevant Terrorism Reasonably Practicable Test, maintaining traceability between assessment and implementation.

2.4 Mitigation Delivery and Action Management.

Where the RPT identifies additional measures or actions as reasonably practicable, PROVA Risk provides integrated task and delivery management to ensure implementation is completed and evidenced.

This functionality enables users to:

- assign responsibility for actions.
- track progress and completion.
- record supporting evidence.
- maintain visibility of outstanding requirements.

This ensures that reasonably practicable measures are implemented in practice, not simply identified in principle.

2.5 Automated Training and Exercising (Learning Management System).

PROVA Risk includes a proprietary Learning Management System (LMS) designed to support the training and exercising requirements arising from the Terrorism Reasonably Practicable Test. Key capabilities include:

- automated training and exercise cadences, determined by site risk profile and RPT outcomes.
- delivery of training via personal handheld devices, reducing operational burden.
- role-based assignment of training requirements.
- tracking of completion and participation for both training and exercises.

Training and exercising outputs are automatically linked to the relevant site and procedures, forming part of the statutory evidence base.

2.6 Exercise Planning and Validation.

The platform supports the planning, delivery, and recording of exercises to validate that public protection procedures are workable and understood.
This includes:

- structured exercise planning aligned to RPT outcomes.
- scenario-based exercises appropriate to site context.
- recording of participation, observations, and outcomes.
- linkage of lessons identified back into procedure review.

This enables Responsible Persons to demonstrate that procedures have been tested and reviewed, not simply documented.

2.7 Evidence Retention and Ongoing Compliance.

PROVA Risk provides a centralised environment for storing, managing, and retaining all compliance evidence required under the Act. This includes:

- Terrorism Reasonably Practicable Tests.
- site- and building-level procedures.
- mitigation actions and implementation evidence.
- training and exercise records.
- reviews, updates, and version history.

The platform maintains a continuous, time-stamped audit trail, enabling Responsible Persons to demonstrate sustained compliance during regulatory inspection.

2.8 Governance, Oversight, and Permissions.

The service supports governance models appropriate to public-sector estates, including:

- role-based access controls.
- delegation of responsibility to site-level users.
- central oversight and assurance at organisational level.

This allows local responsibility to sit with site managers (e.g. headteachers or facility leads), while enabling Responsible Persons and regulators to maintain confidence in overall compliance.

2.9 Data Ownership and Portability.

All data remains the property of the customer. PROVA Risk supports:

- export of assessments, procedures, training, and evidence in open formats.
- use of outputs for inspection, assurance, and reporting.
- portability to support exit or service transition.

3 Service Benefits.

3.1 Enables Defensible Compliance with the Terrorism (Protection of Premises) Act (2025).

PROVA Risk supports Responsible Persons in demonstrating that appropriate public protection procedures are in place so far as is reasonably practicable, in line with the statutory duty under the Act.

By structuring compliance around a site-specific Terrorism Reasonably Practicable Test, the platform ensures that decisions are:

- proportionate to the nature of each premises.
- balanced against available resources and cost.
- documented in a way that is legally defensible.

This reduces regulatory risk by ensuring compliance decisions can be clearly explained and evidenced during inspection.

3.2 **Supports Proportionate, Site-Specific Decision Making.**

The service is explicitly designed to avoid one-size-fits-all approaches. Each site or building is assessed individually, ensuring that:

- procedures are appropriate to context and scale.
- resources are allocated where they provide genuine risk reduction.
- smaller or lower-risk premises are not burdened with disproportionate requirements.

This aligns with Protect UK guidance and established Fire Safety and Health & Safety principles.

3.3 **Reduces Administrative and Operational Burden.**

PROVA Risk reduces the administrative burden associated with compliance by:

- replacing ad hoc documents and spreadsheets with a single system of record.
- automating training and exercise scheduling.
- maintaining evidence continuously rather than retrospectively.

This allows Responsible Persons and site leads to focus on delivery rather than documentation.

3.4 **Improves Governance, Oversight, and Accountability.**

The platform supports clear governance structures by:

- assigning responsibility for procedures, actions, training, and exercises.
- enabling oversight across multiple sites or buildings.
- maintaining an auditable trail of decisions and updates.

This supports internal assurance, senior accountability, and confidence at board or elected-member level.

3.5 **Demonstrates Ongoing Compliance Over Time.**

Compliance under the Act is not a one-off activity. PROVA Risk supports ongoing compliance by:

- dynamically updating Terrorism Reasonably Practicable Tests.
- prompting review when risk or site characteristics change.
- ensuring training and exercising remain current.

This helps organisations demonstrate that compliance is maintained, not static.

3.6 Enables Consistent Training and Preparedness.

Through its Learning Management System, PROVA Risk ensures that:

- staff receive training appropriate to their role and site risk.
- training and exercises are delivered consistently across estates.
- completion and participation are recorded automatically.

This supports operational readiness and evidential compliance simultaneously.

3.7 Provides Inspection-Ready Evidence.

All assessments, procedures, training records, exercises, and reviews are retained in a structured, exportable format. This enables Responsible Persons to:

- respond confidently to regulatory inspection.
- provide evidence to auditors or central government.
- demonstrate due diligence without delay.

3.8 Scales Across Public-Sector Estates.

PROVA Risk is suitable for:

- single-site organisations.
- local authorities managing large and diverse estates.
- central government oversight and trend analysis.

The platform supports consistent standards while respecting site-level differences, enabling scalable compliance without excessive cost or complexity.

4 Technical Overview.

4.1 Service Delivery Model.

PROVA Risk is delivered as a browser-based Software-as-a-Service (SaaS) platform.
The service requires no local installation, specialist hardware, or bespoke client-side software. Users access the platform via a secure web browser over standard internet connections.

This delivery model supports rapid deployment, consistent updates, and scalability across single or multiple sites.

4.2 User Access and Devices.

The service is accessible using modern, standards-compliant web browsers on:

- desktop and laptop computers.
- tablets.
- personal handheld devices (including smartphones).

This enables use by Responsible Persons, site leads, and staff without requiring dedicated devices or on-premise infrastructure.

4.3 Authentication and Access Control.

PROVA Risk includes built-in authentication and role-based access control, enabling organisations to:

- define user roles and permissions.
- restrict access by site, building, or function.
- delegate responsibility while maintaining oversight.

Optional integration with organisational Single Sign-On (SSO) solutions is supported, subject to customer requirements and configuration.

4.4 Multi-Site and Hierarchical Architecture.

The platform is designed to support organisations responsible for multiple premises, including public-sector estates. Technical architecture enables:

- hierarchical organisation structures.
- site- and building-level segregation of data.
- centralised oversight with localised access.

This supports delegation to site-specific Responsible Persons (for example, headteachers or facility managers) while maintaining organisational or authority-level assurance.

4.5 Data Handling and Storage.

All data entered into PROVA Risk is stored securely within the service and logically segregated by customer. Data is structured to support:

- site- and building-level assessments.
- linkage between Terrorism Reasonably Practicable Tests, procedures, training, exercises, and evidence.
- auditability and export in open formats.

Further detail on hosting location and data sovereignty is provided in Section 10.

4.6 Interoperability and Export

The platform supports data export in standard, open formats to enable:

- regulatory inspection and assurance.
- internal reporting and governance.
- service exit and data portability.

PROVA Risk does not require dependency on proprietary third-party software to access or interpret exported data.

4.7 Configuration and Customisation.

The service is configured through:

- organisational structure.
- role and permission settings.
- site and building definitions.

The platform does not rely on bespoke code changes per customer. This ensures consistency, security, and maintainability across the service.

5 Resilience and Backup.

5.1 Hosting Environment and Service Resilience.

PROVA Risk is hosted on Google Cloud Platform (GCP), using resilient, enterprise-grade cloud infrastructure. The hosting environment is designed to support high availability through:

- geographically resilient cloud infrastructure.
- redundancy across critical components.
- managed failover and fault tolerance at platform level.

This architecture supports continuity of service appropriate to a compliance and assurance platform used across public-sector estates.

5.2 Security and Resilience Controls.

PROVA Risk utilises all relevant security and resilience controls available within the Google Cloud environment for the service configuration in use.

This includes, where applicable:

- infrastructure-level redundancy.
- platform-managed security hardening.
- continuous monitoring and threat detection capabilities provided by the hosting environment.
- encryption of data at rest and in transit.

These controls are designed to protect availability, integrity, and confidentiality of customer data and to support service continuity. (Additional detail on security standards and compliance alignment is provided in Section 11.)

5.3 Data Backup and Recovery.

Customer data is subject to automated, regular backups managed within the Google Cloud environment.

Backup arrangements are designed to:

- protect against accidental deletion or corruption.
- support data restoration following service disruption.
- preserve audit trails and compliance records.

Backup frequency and retention are proportionate to the service's function as a planning, training, and assurance platform.

5.4 Business Continuity and Disaster Recovery.

PROVA Risk maintains business continuity and disaster recovery arrangements aligned with the capabilities of the Google Cloud hosting environment.

These arrangements are intended to:

- restore service availability following disruptive events.
- maintain integrity of Terrorism Reasonably Practicable Tests, procedures, training records, and evidence.
- minimise prolonged loss of access.

Continuity and recovery processes are reviewed periodically to ensure continued suitability.

5.5 Planned Maintenance.

Planned maintenance activities are managed to minimise impact on users. Where possible, maintenance is conducted outside standard UK business hours and communicated in advance when user impact is anticipated.

6 Onboarding and Offboarding.

6.1 Onboarding Approach.

PROVA Risk is designed to be adopted incrementally and without disruption to existing organisational operations.

Onboarding does not follow a fixed “implementation project” model. Instead, organisations can begin using the platform as soon as their account is provisioned, configuring sites, buildings, and users progressively as information becomes available.

This approach supports both:

- organisations bringing a small number of premises into scope initially, and
- larger public-sector bodies onboarding estates over time.

There is no requirement to complete all configuration before the platform delivers value.

6.2 Initial Configuration.

Initial setup focuses on establishing the governance structure required under the Terrorism (Protection of Premises) Act (2025).

This typically involves:

- defining the organisational hierarchy (authority, department, or estate level).
- registering sites and buildings that fall within scope.
- assigning Responsible Persons and delegated site-level users.
- enabling the Terrorism Reasonably Practicable Test framework.

All configuration is completed through standard administrative interfaces within the platform.

6.3 User Enablement and Adoption.

PROVA Risk is designed to be usable by non-specialists. User enablement is supported through:

- contextual in-platform guidance.
- short instructional video content.
- written support documentation.

For organisations with complex estates or governance arrangements, onboarding support can be provided to assist with structure, permissions, and early adoption, without creating dependency on ongoing consultancy.

6.4 Operational Use Following Onboarding.

Once onboarded, organisations can immediately begin:

- completing Terrorism Reasonably Practicable Tests.
- developing site- and building-level terrorism protection procedures.
- assigning training and exercise requirements.
- building a compliance evidence base.

There is no requirement for staged go-live milestones or parallel systems.

6.5 Offboarding and Contract Exit.

PROVA Risk supports orderly and transparent offboarding at the end of a contract or upon earlier termination.

Before exit, customers can export all data held within the platform, including:

- Terrorism Reasonably Practicable Tests.
- site- and building-level procedures.
- training and exercise records.
- associated compliance evidence.

Data exports are provided in open, non-proprietary formats suitable for long-term retention or transition to alternative systems, and available for 30 business days after contract end date.

6.6 Data Deletion and Assurance on Exit.

Following confirmation that data export has been completed, customer data is securely deleted from the platform in line with contractual obligations and data protection requirements.

Deletion activities are logged to support audit and assurance requirements.

No exit fees apply in relation to data export or data deletion.

7 Service Constraints.

PROVA Risk is a compliance enablement and assurance platform. It is designed to support Responsible Persons in meeting their duties under the Terrorism (Protection of Premises) Act (2025) by providing structured assessments, procedures, training, exercising, and evidence management.

As such, the service operates within the following defined constraints.

7.1 Scope of Responsibility.

PROVA Risk supports compliance activities but does not replace the statutory responsibilities of the Responsible Person. The platform:

- enables the application of the Terrorism Reasonably Practicable Test.

- supports the development and maintenance of public protection procedures.
- provides tools to train staff, exercise plans, and retain evidence.

However, responsibility for determining final compliance decisions, implementing physical or organisational measures, and responding to incidents remains with the Responsible Person.

7.2 No Live Operational or Emergency Response Capability.

The service does not provide real-time operational functionality. Specifically, PROVA Risk does not:

- monitor live threats or incidents.
- integrate with emergency services command-and-control systems.
- issue live emergency alerts to the public.
- replace local emergency response arrangements.

Its role is to ensure that procedures, training, and evidence are in place before an incident, and that preparedness can be demonstrated after.

7.3 Dependence on Accurate User Input.

The outputs of the Terrorism Reasonably Practicable Test and related procedures are dependent on the information entered by users. Responsible Persons and delegated site leads are expected to:

- accurately describe site characteristics and use.
- keep site and building information up to date.
- review assessments when circumstances change.

The platform supports prompts and review cycles, but it does not independently verify site conditions.

7.4 Internet Connectivity and Browser Access.

As a cloud-based SaaS platform, PROVA Risk requires:

- a standard internet connection.
- access via a modern, standards-compliant web browser.

The service does not support offline operation. Users must have connectivity to access, update, or export information.

7.5 Configuration Rather Than Bespoke Development.

PROVA Risk is configured through organisational structures, roles, sites, and buildings.

The service does not typically include:

- bespoke feature development for individual customers.
- custom code deployments per organisation.

This approach ensures consistency, security, and maintainability across the platform, in line with public-sector SaaS best practice.

8 Service Targets, Levels and Support.

8.1 Service targets.

Service availability, availability of support, support channels, response times, incident management and recovery objectives, are outlined below. These describe the intended operating level of the service and should be read alongside the Call-Off Contract.

8.2 Service availability.

- Target monthly service availability: 99.5% during UK business hours (08:00–18:00, Monday–Friday, excluding UK public holidays).
- Overall target monthly service availability (24x7): 99.5%.
- Planned maintenance windows:
    - Scheduled, where possible, outside UK business hours.
    - Customers notified at least 5 working days in advance where maintenance may cause noticeable disruption.
- Exclusions: downtime due to customer networks, third-party connectivity, or force majeure is not counted against availability targets.

8.3 Availability of Support.

PROVA Risk provides continuous, 24/7 access to user support, recognising that Responsible Persons and site leads may need assistance outside standard business hours, including during exercises, inspections, or urgent compliance activity. Support is available through multiple channels to suit different user needs and urgency levels.

8.4 Support Channels.

Support is provided through the following mechanisms:

- 24/7 helpline, providing direct access to support assistance.
- AI-powered chatbot, available at all times within the platform to support common queries, navigation, and guidance on platform use.
- Online support portal, allowing users to raise and track support requests electronically.

This multi-channel approach ensures users can access assistance in a way that is proportionate to the issue they are experiencing.

8.5 Support response times

For incidents and support requests raised via the defined support channels:

- P1 - Critical (service unavailable or severely degraded for all users). Target initial response: within 2 hours, 24x7.
- P2 - High (major functionality impaired, significant impact on critical users). Target initial response: within 4 hours during UK business hours.
- P3 - Medium (degraded functionality, workarounds available). Target initial response: by next business day.
- P4 - Low (how-to questions, minor issues, enhancement requests). Target initial response: within 2 business days.

8.6 Incident Management.

Incidents and support requests are logged and managed through a structured support process. This includes:

- triage and prioritisation.
- investigation and resolution.
- communication with the reporting user where appropriate.

Security-related matters are escalated in line with internal incident management procedures.

8.7 Recovery objectives.

- Recovery Time Objective (RTO): For platform-wide outages: target restoration of service within 4 hours of incident classification as P1, subject to the nature of the incident.
- Recovery Point Objective (RPO): Target maximum data loss of 1 hour for transactional data under normal operations.

8.8 In-Platform Guidance and Assisted Use.

PROVA Risk places strong emphasis on guided use within the platform itself, reducing reliance on external documentation or reactive support. The service includes an extensive library of in-platform help content, comprising:

- screen-recorded instructional videos embedded directly within relevant workflows.
- guided walkthroughs delivered by the platform's instructional avatar, Capt Chris, providing consistent and accessible explanations of key tasks and compliance concepts.
- short, task-specific videos aligned to individual steps within the Terrorism Reasonably Practicable Test, plan builders, training, and evidence workflows.

In addition, the majority of platform pages include contextual tooltips and inline guidance, providing:

- immediate explanations of terminology and concepts.
- clarification of why specific information is required.
- additional detail where legislative or procedural context may be helpful.

This approach ensures users can access the right level of guidance at the point of need, supporting correct and consistent use of the platform while reducing the need for external training or support intervention.

8.9 Service Improvement.

Support interactions and user feedback are reviewed to identify recurring issues, usability improvements, and emerging requirements linked to changes in legislation or guidance.

Where appropriate, insights from support activity inform platform updates and enhancements.

9 Maintenance and Updates.

PROVA Risk is maintained as a continuously evolving SaaS platform to ensure ongoing alignment with the Terrorism (Protection of Premises) Act (2025), Protect UK guidance, and related public-sector assurance expectations.

Updates are delivered in a controlled and managed manner, without disrupting customer use or compromising compliance records.

9.1 Update Approach.

The platform follows a managed release model, under which improvements and changes are introduced through planned updates rather than ad hoc modification.

Updates may include:

- usability improvements.
- performance enhancements.
- refinement of workflows linked to the Terrorism Reasonably Practicable Test.
- updates required to reflect changes in legislation, statutory guidance, or regulatory interpretation.

This approach ensures that the platform remains current while maintaining stability.

9.2 Protection of Customer Configuration and Data.

Platform updates are designed to preserve:

- existing Terrorism Reasonably Practicable Tests.
- site- and building-level procedures.
- training and exercise records.
- evidence and audit trails.

Customer configuration, data, and historical records are not overwritten or lost as part of routine maintenance or updates.

9.3 Communication of Changes.

Where updates introduce changes that may affect how users interact with the platform, information is provided in advance or alongside the update. This may include:

- release notes.
- in-platform notifications.
- updated guidance or support materials.

This ensures users understand what has changed and why.

9.4 Planned Maintenance.

From time to time, planned maintenance may be required to support updates or infrastructure improvements.

Such maintenance is managed to minimise disruption and, where possible, scheduled outside standard UK business hours.

9.5 Continuous Alignment with Legislative and Regulatory Change.

PROVA Risk is maintained with the intention of reflecting developments in:

- the Terrorism (Protection of Premises) Act (2025).

- Protect UK guidance.
- related public-sector assurance and inspection expectations.

Where changes in the legislative or regulatory environment affect compliance requirements, the platform is updated to support continued defensibility and proportionality. Updates required to reflect changes in legislation, statutory guidance, or regulatory interpretation are implemented within a reasonable timeframe following their publication.

9.6 Dynamic Risk Environment Updates.

PROVA Risk is designed to reflect that the risk environment relevant to the Terrorism (Protection of Premises) Act (2025) is not static.

The platform's Terrorism Reasonably Practicable Test engine is capable of updating assessments in response to material changes in the wider threat environment, including changes to the UK national terrorism threat level or other relevant risk indicators.

Where such a change is assessed as having a potential impact on site-level risk profiles:

- Terrorism Reasonably Practicable Tests are automatically re-evaluated for affected sites and buildings.
- associated risk scores and proportionality assessments are updated within the platform.
- any resulting changes to reasonably practicable risk mitigation measures or procedures are identified.
- Users are informed where updated assessments indicate that additional or enhanced measures may now be reasonably practicable, allowing Responsible Persons to review, implement, and evidence any required changes.

This ensures that compliance is maintained over time and remains aligned to the prevailing risk context, without requiring manual re-assessment in response to external threat-level changes.

10 Data Hosting and Sovereignty.

PROVA Risk is hosted in a UK regional data centre on Google Cloud Platform (GCP), providing UK-based primary storage and processing for customer data. All customer production data entered into the platform is stored, processed, and backed up in UK data centres under the control of PROVA Risk and its sub-processors, except where otherwise agreed in writing with the Customer. This approach is intended to support UK public-sector requirements for data residency, sovereignty, and regulatory assurance.

10.1 Data Location.

Customer production data is held within Google Cloud data centres located in the United Kingdom. No customer production data is routinely processed or stored outside the UK. Limited access to, or processing of, customer data from outside the UK may occur for specific and controlled purposes, for example:

- use of support, monitoring, or ancillary services (such as chat-based support tools); or
- controlled access by authorised development or support personnel for troubleshooting.

Where such access or transfers occur, they are minimised and subject to appropriate safeguards and transfer mechanisms in accordance with UK data protection law and applicable contractual commitments. Access controls are configured on a least-privilege basis and may be restricted to UK locations where contractually required.

10.2 Data Sovereignty and Control.

Customers retain full ownership and control of their data at all times. PROVA Risk does not, without the Customer's permission:

- assert ownership over customer data
- sell, monetise, or repurpose customer data
- transfer data to third parties for non-service purposes

Access to customer data is restricted to authorised users and authorised PROVA Risk personnel and is controlled through role-based access mechanisms and appropriate technical and organisational measures.

10.3 Encryption and Protection.

All customer data is protected using industry-standard security controls, including:

- encryption of data at rest.
- encryption of data in transit.

These protections are applied consistently across the platform and form part of the broader security controls described in Section 11.

10.4 Cross-Border Transfers.

Any transfers of personal data outside the UK (or access to such data from outside the UK) are limited, controlled, and carried out only where necessary for service provision or support. Where such transfers or access occur, they are subject to appropriate contractual, technical, and organisational safeguards (including UK-approved international data transfer mechanisms where required) in order to ensure an adequate level of protection for the data.

11 Security and Compliance.

Security within PROVA Risk is designed to protect the confidentiality, integrity, and availability of data used to demonstrate compliance with the Terrorism (Protection of Premises) Act (2025). Controls are proportionate to the platform's role as a compliance, training, and assurance system rather than a live operational or intelligence system.

Security responsibilities are managed through a shared responsibility model between PROVA Risk and its cloud hosting provider.

11.1 Security Governance and Responsibility.

PROVA Risk maintains internal security governance arrangements covering:

- access control and user management.
- data protection and privacy.
- incident management and escalation.
- supplier and dependency assurance.

These arrangements are reviewed periodically to ensure continued suitability as the platform evolves and as regulatory expectations change.

11.2 Hosting Provider Security Controls.

The platform is hosted on Google Cloud Platform, utilising the native security capabilities and controls available within that environment. This includes, where applicable:

- hardened cloud infrastructure.
- platform-level monitoring and threat detection.
- resilience and fault isolation.
- managed patching and infrastructure security updates.

These provider-managed controls form the primary technical security baseline for the service, and are complemented by PROVA Risk's ISO 27001-certified security management and operational processes.

11.3 **Access Control and User Management.**

Access to PROVA Risk is controlled through role-based access mechanisms. This ensures that:

- users only access sites, buildings, and functions relevant to their role.
- responsibility can be delegated to site level without loss of oversight.
- sensitive compliance and assurance data is protected from unauthorised access.

Authentication mechanisms are designed to support secure access while remaining usable for large and diverse user groups.

11.4 **Data Protection and Privacy.**

Customer data is handled in accordance with applicable UK data protection legislation, including the UK GDPR and Data Protection Act 2018. Key principles include:

- customer ownership and control of data.
- data minimisation appropriate to compliance needs.
- secure deletion on exit or termination.

Further detail on data location and sovereignty is set out in Section 10.

11.5 **Encryption and Data Security.**

PROVA Risk applies encryption to protect data:

- in transit, to prevent interception or unauthorised access.
- at rest, to protect stored compliance, training, and assurance records.

Encryption is implemented using industry-standard methods provided within the hosting environment.

11.6 **Vulnerability and Incident Management**

Security vulnerabilities and incidents are managed through defined internal processes.

This includes:

- monitoring for potential security issues.
- assessment of impact and risk.
- remediation and corrective action where required.

Security-related incidents are prioritised and handled in line with established incident management procedures.

11.7 **Alignment with Recognised Standards and Guidance.**

PROVA Risk is designed to align with recognised security and resilience principles, including:

- UK National Cyber Security Centre (NCSC) guidance.
- ISO 27001 and ISO 22301 principles (information security and business continuity).
- cloud security best practice appropriate to public-sector SaaS services.

Alignment reflects design intent and operational practice rather than claims of certification, unless explicitly stated elsewhere.

12 **Accessibility.**

PROVA Risk is designed to be accessible to users across public-sector organisations, including individuals with varying access needs, technical confidence, and learning preferences. Accessibility is treated as an integral part of platform design rather than a separate or optional consideration.

The service is designed to align with **WCAG 2.2 AA** standards and the **Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018**. These standards inform interface layout, navigation structure, content presentation, and interaction design across all core workflows within the platform.

Usability and clarity are prioritised to support inclusive use in operational environments. The platform adopts consistent navigation patterns, readable typography, appropriate colour contrast, and keyboard-accessible functionality where applicable. PROVA Risk is designed to be compatible with commonly used assistive technologies, including screen readers, to ensure users can access and interact with content effectively.

Accessibility is further supported through extensive in-platform guidance. Screen-recorded instructional videos, contextual tooltips, and guided walkthroughs delivered by the Capt Chris avatar provide alternative ways for users to understand tasks and compliance concepts. This approach reduces reliance on dense written instructions and supports users who benefit from visual, auditory, or step-by-step explanations.

Accessibility is reviewed as part of ongoing platform development. Feedback from users and testing activity is used to identify and address accessibility issues through the platform's controlled maintenance and update process, ensuring that accessibility is maintained as the service evolves.

This aligns with the Supplier's accessibility commitments set out in the G-Cloud Terms and Conditions and is intended to support the Customer's obligations under the Equality Act 2010.

13 **Exit and Data Retention.**

PROVA Risk is designed to support straightforward exit and data retention arrangements, enabling customers to retain control of their compliance information throughout and beyond the contract lifecycle.

At all times, data entered into the platform remains the property of the customer. PROVA Risk does not assert ownership over customer data and does not restrict the customer's ability to access or retrieve their information.

On exit from the service, customers are able to export all data held within the platform, including Terrorism Reasonably Practicable Tests, site- and building-level terrorism protection procedures, training records, exercise records, and associated compliance evidence. Data is provided in open, non-proprietary formats suitable for long-term retention, regulatory inspection, or transition to an alternative system.

Following confirmation that data export has been completed, customer data is securely deleted from the platform in line with contractual obligations and applicable data protection legislation. Deletion activities are logged to support audit and assurance requirements.

Residual backup data is retained only for the minimum period required to support platform resilience and recovery processes and is securely overwritten or destroyed in accordance with established retention policies.

No exit fees are applied in relation to data export, data deletion, or service termination. This approach supports transparency, data portability, and buyer confidence, in line with G-Cloud principles.

14 **Commercial Model.**

PROVA Risk is provided on an annual subscription basis, with pricing calculated using a per-site licence model under the G-Cloud 15 framework.

Each in-scope site is licensed individually, enabling customers to scale usage proportionately across their estate and align cost directly to the number of premises subject to the Terrorism (Protection of Premises) Act (2025).

The subscription includes access to the full PROVA Risk platform for each licensed site, including the Terrorism Reasonably Practicable Test, site- and building-level terrorism protection procedures, training and exercising functionality, evidence management, maintenance, and support.

Pricing is transparent and published in the associated G-Cloud Pricing Document. There are no mandatory onboarding fees, no charges for platform updates, and no additional fees for standard support.

Contract duration, payment arrangements, and renewal terms are governed by the applicable G-Cloud call-off contract and associated schedules.