Martyn's Law Compliance Roadmap

Implementation Timeline and Strategic Framework

A Cambridge Sentinel Resource
Published by Rittel Consulting Limited

Document Version: 1.0
Publication Date: December 2025
Document ID: CS-ML-RMP-001

Executive Summary

The Terrorism (Protection of Premises) Act 2025, commonly known as Martyn's Law, represents the most significant legislative development in protective security for public venues since the introduction of the Regulatory Reform (Fire Safety) Order 2005. This roadmap provides organisations with a structured, phased approach to achieving compliance ahead of the Act's anticipated implementation in 2027.

Named in memory of Martyn Hett, who was killed in the Manchester Arena attack of May 2017, the legislation emerged from years of campaigning by his mother, Figen Murray, and reflects a fundamental shift in how the United Kingdom approaches counter-terrorism preparedness at publicly accessible locations [1]. The Act received Royal Assent on 3 April 2025, triggering a minimum 24-month implementation period designed to allow duty holders sufficient time to understand their obligations and prepare accordingly [2].

This document is designed for security professionals, estate managers, venue operators, and compliance officers responsible for premises that may fall within the scope of Martyn's Law. It provides a clear timeline, practical guidance, and strategic considerations for organisations navigating the transition from current voluntary protective security measures to mandatory compliance.

Understanding Martyn's Law: Scope and Requirements

Legislative Context

Martyn's Law builds upon the Protect and Prepare strands of the Government's counter-terrorism strategy, CONTEST, which has guided the United Kingdom's approach to terrorism since 2003 [3]. The Act establishes a tiered regulatory framework overseen by the Security Industry Authority (SIA), which will serve as the regulator with powers to provide guidance, monitor compliance, and take enforcement action where necessary [2].

The legislation applies a risk-based, proportionate approach that recognises the diverse nature of public premises and events across the United Kingdom. Duty holders are required to implement measures and procedures that are "reasonably practicable" for their specific circumstances, taking into account the nature of the premises, the activities conducted, and the resources available [4]. This concept of reasonably practicable is well-established in United Kingdom law, particularly in fire safety and health and safety legislation, and provides flexibility whilst maintaining clear accountability.

Scope: Which Premises and Events Are Affected?

Martyn's Law applies to **qualifying premises** and **qualifying events** where members of the public have access. The determining factor is the **capacity** of the venue, specifically the number of individuals it is reasonable to expect may be present at the same time from time to time [2].

Qualifying premises include, but are not limited to:

- Entertainment and assembly venues (theatres, concert halls, sports stadiums)
- Retail premises (shopping centres, department stores, markets)
- Food and drink establishments (restaurants, pubs, nightclubs)
- Museums, galleries, and visitor attractions
- Places of worship
- Educational establishments with public access areas

- Healthcare facilities with public-facing departments
- Transport hubs (stations, airports, bus terminals)
- Hotels and accommodation facilities
- Office buildings with significant public access

Qualifying events are temporary gatherings where 800 or more individuals may be present, including festivals, concerts, sporting events, markets, and public celebrations [4].

The Two-Tier Framework

Martyn's Law establishes two tiers of requirements based on venue capacity, ensuring proportionality whilst maintaining public protection.

Standard Tier (200-799 Capacity)

Premises where it is reasonable to expect between 200 and 799 individuals to be present at the same time fall within the Standard Tier. These duty holders must [2]:

1. **Notify the SIA** that they are responsible for qualifying premises
2. **Implement public protection procedures** that could reasonably be expected to reduce the risk of physical harm to individuals if a terrorist attack were to occur at or near the premises

Standard Tier requirements focus on **procedural measures** rather than physical security infrastructure. The emphasis is on low-cost, practical activities that enhance preparedness and response capabilities. Examples include [4]:

- Developing and communicating evacuation procedures
- Identifying safe areas and routes to cover within the premises
- Training staff to recognise suspicious behaviour and items
- Establishing protocols for lockdown scenarios
- Creating communication plans for emergencies
- Designating responsible persons for security coordination

Crucially, there is **no requirement** for Standard Tier premises to install physical security measures such as barriers, CCTV systems, or access control infrastructure [2].

Enhanced Tier (800+ Capacity)

Premises and qualifying events where 800 or more individuals may be present fall within the Enhanced Tier. These duty holders must meet all Standard Tier requirements **plus** additional obligations [2]:

1. **Implement public protection measures** (in addition to procedures) that could reasonably be expected to reduce both:
    - The vulnerability of the premises or event to a terrorist attack occurring
    - The risk of physical harm to individuals if an attack were to occur
2. **Document procedures and measures** in a written format and provide this documentation to the SIA

Enhanced Tier requirements may include physical and technological security measures, tailored to the specific risk profile and operational context of the premises or event. Examples include [4]:

- Bag search policies and screening procedures
- CCTV surveillance systems with appropriate monitoring
- Vehicle access controls and hostile vehicle mitigation measures
- Perimeter security enhancements
- Access control systems for restricted areas
- Security staffing arrangements
- Counter-drone capabilities for outdoor events
- Integration with local counter-terrorism policing structures

The specific measures adopted will vary significantly depending on the nature of the venue, its location, the activities conducted, and the resources available to the duty holder.

Implementation Timeline: 24-Month Roadmap

The Government has committed to a minimum 24-month implementation period between Royal Assent (April 2025) and the Act coming into force (anticipated April

2027) [2]. This roadmap divides this period into six strategic phases, each with defined objectives and deliverables.

Phase 1: Assessment and Scoping (Months 1-4)

Objective: Determine whether your organisation falls within scope and identify the applicable tier.

Key Activities:

Capacity Assessment

- Conduct thorough capacity assessments for all premises under your control
- Consider maximum occupancy during peak periods, special events, and seasonal variations
- Document the methodology used to determine capacity figures
- Identify premises that may fluctuate between Standard and Enhanced Tier thresholds

Scope Determination

- Review the statutory guidance published by the Home Office (expected during the implementation period)
- Consult with legal advisors to confirm interpretation of qualifying premises definitions
- Engage with the SIA's guidance materials and support services
- Document the rationale for scope determinations for audit purposes

Stakeholder Engagement

- Brief senior leadership and board members on Martyn's Law implications
- Identify internal stakeholders across operations, facilities, HR, legal, and finance
- Establish a cross-functional working group to oversee compliance efforts
- Engage with industry bodies and peer organisations to share insights

Deliverables:

- Comprehensive premises inventory with capacity assessments

- Scope determination report identifying Standard Tier and Enhanced Tier premises
- Stakeholder engagement plan
- Initial budget estimate for compliance activities

Phase 2: Gap Analysis and Risk Assessment (Months 5-8)

Objective: Understand current security posture and identify gaps against Martyn's Law requirements.

Key Activities:

Current State Assessment

- Audit existing security procedures, policies, and physical measures
- Review staff training records and competency levels
- Assess current relationships with local counter-terrorism policing and emergency services
- Evaluate incident response plans and business continuity arrangements

Risk Assessment

- Conduct terrorism risk assessments for each qualifying premises
- Consider location-specific threat intelligence and vulnerability factors
- Evaluate potential attack methodologies relevant to the venue type
- Assess consequences of different attack scenarios

Gap Identification

- Compare current arrangements against anticipated Standard or Enhanced Tier requirements
- Identify procedural gaps (policies, training, communication)
- Identify physical security gaps (infrastructure, technology, staffing)
- Prioritise gaps based on risk and regulatory urgency

Resource Planning

- Estimate costs for closing identified gaps
- Identify internal capabilities and external support requirements
- Develop procurement strategies for security technology and services
- Plan workforce implications (recruitment, training, role changes)

Deliverables:

- Gap analysis report for each qualifying premises
- Terrorism risk assessment documentation
- Prioritised action plan with cost estimates
- Resource allocation proposal for leadership approval

Phase 3: Policy and Procedure Development (Months 9-12)

Objective: Develop compliant public protection procedures and document Enhanced Tier measures.

Key Activities:

Standard Tier Procedure Development

- Draft evacuation procedures tailored to premises layout and occupancy patterns
- Develop lockdown protocols with clear trigger criteria and communication methods
- Create suspicious behaviour and item reporting procedures
- Establish incident command structures and roles
- Design staff briefing materials and quick reference guides

Enhanced Tier Documentation

- Document public protection measures in the format required by SIA guidance
- Describe the rationale for selected measures and their expected effectiveness
- Detail maintenance, testing, and review schedules for physical security systems
- Create operational procedures for security staffing and technology use

Integration with Existing Frameworks

- Align Martyn's Law procedures with fire safety, health and safety, and safeguarding policies
- Ensure consistency with business continuity and crisis management plans
- Coordinate with data protection requirements for surveillance and monitoring systems
- Integrate with existing security management systems (e.g., ISO 27001, ISO 22301)

Consultation and Review

- Engage staff representatives and trade unions in procedure development
- Consult with local counter-terrorism security advisers (CTSAs)
- Seek feedback from emergency services on response protocols
- Conduct internal peer review and legal compliance checks

Deliverables:

- Approved public protection procedures for all Standard Tier premises
- Documented public protection measures for all Enhanced Tier premises
- Integration plan with existing policies and management systems
- Consultation records and stakeholder sign-off

Phase 4: Physical Measures Implementation (Months 13-18)

Objective: Procure and install physical security measures for Enhanced Tier premises.

Key Activities:

Procurement

- Issue tenders for security technology (CCTV, access control, screening equipment)
- Engage specialist contractors for physical security works (barriers, fencing, lighting)
- Procure security staffing services where required
- Establish maintenance and support contracts for installed systems

Installation and Integration

- Coordinate installation works to minimise operational disruption
- Ensure integration between security systems (CCTV, access control, alarms)
- Test systems thoroughly before operational deployment
- Commission systems with appropriate documentation and training

Operational Readiness

- Develop standard operating procedures for security technology use
- Train security staff and control room operators
- Establish monitoring and response protocols
- Conduct tabletop exercises to test system effectiveness

Compliance Verification

- Verify that installed measures meet regulatory expectations
- Document compliance evidence for SIA submission
- Conduct independent security audits where appropriate
- Address any deficiencies identified during testing

Deliverables:

- Installed and operational physical security measures for Enhanced Tier premises
- System integration documentation and operational procedures
- Training records for security staff and operators
- Compliance verification reports

Phase 5: Training and Awareness (Months 19-21)

Objective: Ensure all staff are competent to fulfil their roles under Martyn's Law.

Key Activities:

Training Needs Analysis

- Identify role-specific training requirements (frontline staff, managers, security personnel)
- Determine appropriate training delivery methods (e-learning, classroom, practical exercises)
- Establish competency standards and assessment criteria
- Plan training schedules to achieve full workforce coverage before go-live

Training Delivery

- Deliver ACT Awareness training (Action Counters Terrorism) to all staff
- Provide role-specific training on evacuation, lockdown, and incident response procedures
- Train security staff on physical security systems and response protocols
- Conduct scenario-based exercises and drills to test competency

Awareness Campaigns

- Communicate Martyn's Law requirements and organisational preparations to all staff
- Develop visual aids, posters, and quick reference guides for staff areas
- Brief contractors, tenants, and third parties operating within premises
- Engage with customers and visitors through public-facing communications

Competency Assurance

- Assess staff competency through practical exercises and knowledge checks
- Maintain training records for regulatory compliance and audit purposes
- Establish refresher training schedules to maintain competency over time
- Address identified competency gaps through additional training interventions

Deliverables:

- Comprehensive training programme delivered to all staff
- Training records and competency assessments
- Awareness materials and communication outputs
- Refresher training schedule

Phase 6: Registration, Testing, and Go-Live (Months 22-24)

Objective: Register with the SIA, conduct final testing, and achieve full operational compliance.

Key Activities:

SIA Registration

- Complete SIA notification process for all qualifying premises
- Submit Enhanced Tier documentation as required
- Respond to any SIA queries or requests for additional information
- Confirm registration acceptance and compliance status

Final Testing

- Conduct full-scale exercises simulating terrorist attack scenarios
- Test evacuation, lockdown, and incident response procedures under realistic conditions
- Evaluate security system performance and staff competency
- Identify and address any deficiencies revealed during testing

Continuous Improvement

- Establish governance structures for ongoing compliance monitoring
- Implement regular review cycles for procedures and measures
- Create feedback mechanisms to capture lessons from exercises and real incidents
- Plan for periodic re-assessment of risk and capacity as circumstances change

Go-Live Preparation

- Confirm readiness across all qualifying premises
- Brief leadership on compliance status and residual risks
- Communicate go-live status to staff, contractors, and stakeholders
- Prepare for regulatory inspections and audits

Deliverables:

- SIA registration confirmation for all qualifying premises
- Exercise reports and lessons learned documentation
- Governance framework for ongoing compliance
- Go-live readiness declaration

Governance and Ongoing Compliance

Achieving initial compliance with Martyn's Law is only the beginning. Organisations must establish robust governance structures to maintain compliance over time, adapt to evolving threats, and demonstrate continuous improvement.

Responsible Person

The Act requires the designation of a "responsible person" for each qualifying premises or event [2]. This individual holds legal accountability for compliance and must possess the authority, competence, and resources necessary to fulfil the role effectively. Organisations should:

- Clearly define the responsible person role in job descriptions and governance documents
- Ensure the responsible person has direct access to senior leadership and decision-making forums
- Provide appropriate training and professional development opportunities
- Establish clear lines of accountability and reporting

Compliance Monitoring

Ongoing compliance requires systematic monitoring and assurance activities:

- **Regular audits** of procedures, measures, and training records
- **Performance metrics** tracking incident response times, system uptime, and staff competency

- **Periodic risk assessments** to reflect changes in threat landscape and operational context
- **Stakeholder feedback** from staff, customers, and emergency services
- **Regulatory engagement** with the SIA, including inspections and information requests

Continuous Improvement

Organisations should adopt a continuous improvement mindset, learning from exercises, incidents, and sector best practice:

- Conduct post-exercise reviews to identify strengths and areas for development
- Analyse security incidents and near-misses to refine procedures
- Engage with industry forums and information-sharing networks
- Monitor emerging security technologies and methodologies
- Update procedures and measures in response to lessons learned

---

Common Challenges and Mitigation Strategies

Challenge 1: Capacity Determination Uncertainty

Issue: Premises with variable occupancy may struggle to determine whether they fall within Standard or Enhanced Tier thresholds.

Mitigation:

- Adopt a conservative approach, assuming Enhanced Tier status if capacity regularly approaches 800
- Maintain detailed occupancy records to support capacity assessments
- Consult with the SIA for guidance on borderline cases
- Review capacity determinations annually or following significant operational changes

Challenge 2: Resource Constraints

Issue: Smaller organisations may face financial and operational challenges in implementing compliance measures.

Mitigation:

- Prioritise low-cost procedural measures that deliver significant risk reduction
- Explore collaborative approaches with neighbouring premises or industry partners
- Seek grants or funding support where available
- Implement measures incrementally, focusing on highest-priority risks first

Challenge 3: Integration with Existing Systems

Issue: Aligning Martyn's Law requirements with existing fire safety, health and safety, and safeguarding frameworks can be complex.

Mitigation:

- Conduct integrated risk assessments that consider multiple regulatory requirements
- Develop unified procedures that address terrorism, fire, and other emergency scenarios
- Engage specialist advisors to ensure regulatory coherence
- Leverage existing governance structures rather than creating parallel systems

Challenge 4: Staff Engagement and Competency

Issue: Achieving consistent staff competency across large, dispersed workforces with high turnover can be challenging.

Mitigation:

- Embed Martyn's Law training in induction programmes for new staff
- Use e-learning platforms to deliver scalable, consistent training
- Conduct regular refresher training and competency assessments

- Recognise and reward staff who demonstrate exemplary security awareness

---

Conclusion

Martyn's Law represents a significant evolution in the United Kingdom's approach to protective security, placing legal obligations on venue operators and event organisers to prepare for and respond to terrorist threats. Whilst the legislation introduces new compliance burdens, it also provides an opportunity for organisations to enhance their resilience, protect their people, and contribute to national security.

This roadmap provides a structured pathway to compliance, breaking down the 24-month implementation period into manageable phases with clear objectives and deliverables. By commencing preparation now, organisations can avoid last-minute pressures, engage stakeholders effectively, and build robust, sustainable compliance frameworks.

Rittel Consulting Limited stands ready to support organisations at every stage of their Martyn's Law journey, from initial scoping and gap analysis through to training delivery and ongoing compliance assurance. Our team of protective security specialists brings deep expertise in counter-terrorism, risk management, and regulatory compliance, ensuring that your organisation not only meets its legal obligations but also achieves genuine security improvements.

References

[1] Home Office. (2025). *Martyn's Law Factsheet*. Retrieved from https://homeofficemedia.blog.gov.uk/2025/04/03/martyns-law-factsheet/

[2] ProtectUK. (2025). *Martyn's Law: What you need to know*. Retrieved from https://www.protectuk.police.uk/martyns-law

[3] HM Government. (2023). *CONTEST: The United Kingdom's Strategy for Countering Terrorism*. Retrieved from https://www.gov.uk/government/publications/contest

[4] ProtectUK. (2025). *Martyn's Law overview and what you need to know*. Retrieved from https://www.protectuk.police.uk/martyns-law/martyns-law-overview-and-what-

you-need-know

Document Information

Author: Rittel Consulting Limited
Publication: The Cambridge Sentinel Resource Library
Version: 1.0
Date: December 2025
Document ID: CS-ML-RMP-001

Disclaimer: This document provides general guidance on Martyn's Law compliance and should not be considered legal advice. Organisations should consult with qualified legal and security professionals to address their specific circumstances.

The Cambridge Sentinel is a service line of Rittel Consulting Limited, providing protective security intelligence and compliance guidance to organisations across the United Kingdom.