Executive Memo: Martyn's Law

Strategic Briefing for Senior Leadership

A Cambridge Sentinel Executive Briefing
Published by Rittel Consulting Limited

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

Executive Summary

The Terrorism (Protection of Premises) Act 2025, known as Martyn's Law, introduces mandatory counter-terrorism preparedness requirements for publicly accessible premises and events across the United Kingdom. The legislation received Royal Assent on 3 April 2025 and is anticipated to come into force in April 2027, providing organisations with a 24-month implementation period [1].

This executive memo provides senior leaders with a concise overview of the Act's requirements, strategic implications, and recommended actions. Organisations that fall within scope must designate a responsible person, implement public protection procedures, and (for larger venues) adopt physical security measures. Non-compliance may result in regulatory sanctions, including financial penalties and prosecution.

Key Strategic Imperatives:

1. **Determine Scope:** Assess whether your organisation operates qualifying premises (200+ capacity) or events (800+ capacity)
2. **Allocate Resources:** Budget for risk assessments, procedure development, staff training, and (for Enhanced Tier) physical security measures
3. **Designate Accountability:** Appoint a competent responsible person with authority and resources to achieve compliance

4. **Commence Planning:** Initiate compliance activities now to avoid last-minute pressures and ensure quality implementation
5. **Integrate Governance:** Align Martyn's Law compliance with existing risk management, health and safety, and fire safety frameworks

Martyn's Law represents both a compliance obligation and an opportunity to enhance organisational resilience, protect people, and demonstrate corporate responsibility. Proactive, strategic engagement will position your organisation for successful compliance whilst achieving genuine security improvements.

---

1. Legislative Context: Why Martyn's Law Matters

The Manchester Arena Attack

On 22 May 2017, a suicide bomber attacked concertgoers leaving the Manchester Arena, killing 22 people and injuring hundreds more [2]. The subsequent public inquiry revealed significant deficiencies in security arrangements, staff training, and emergency response procedures. These findings catalysed a campaign by Figen Murray, mother of victim Martyn Hett, for legislation requiring venues to implement basic protective security measures.

Policy Response

The Government's response evolved through consultations in 2021 and 2023, parliamentary scrutiny, and cross-party support [3]. The resulting Terrorism (Protection of Premises) Act 2025 establishes a tiered, risk-based framework overseen by the Security Industry Authority (SIA). The Act balances public protection with operational practicability, recognising that security requirements must be proportionate to venue size, resources, and risk profile.

Strategic Significance

Martyn's Law is the most significant counter-terrorism legislation affecting commercial and public sector organisations since the introduction of fire safety regulations. It shifts counter-terrorism preparedness from a voluntary best practice to a legal

obligation, creating personal and corporate liability for non-compliance. For senior leaders, this represents:

- **Legal Risk:** Potential for regulatory sanctions, including fines and prosecution
- **Reputational Risk:** Public scrutiny of security arrangements, particularly following incidents
- **Operational Risk:** Need to integrate new procedures and measures into existing operations
- **Financial Risk:** Costs associated with compliance, including assessments, training, and physical security measures

---

2. Scope: Does Martyn's Law Apply to Your Organisation?

Qualifying Premises

Martyn's Law applies to premises where members of the public have access and where it is reasonable to expect a specified number of individuals to be present at the same time from time to time [1]. The capacity thresholds are:

- **Standard Tier:** 200 to 799 individuals
- **Enhanced Tier:** 800 or more individuals

Premises types include entertainment venues, retail premises, food and drink establishments, visitor attractions, places of worship, educational establishments, healthcare facilities, transport hubs, hotels, and office buildings with significant public access.

Excluded premises include private dwellings, premises used exclusively for worship (though ancillary facilities may be included), armed forces and intelligence service premises, and diplomatic premises.

Qualifying Events

The Act also applies to temporary events where 800 or more individuals may be present, including festivals, concerts, sporting events, markets, and public

celebrations [1]. All qualifying events fall within the Enhanced Tier.

Capacity Determination

Determining capacity is a critical compliance step. Organisations must assess maximum occupancy during peak periods, considering:

- Physical layout and usable floor space
- Fire safety capacity limits
- Typical occupancy patterns (time of day, week, year)
- Special events or seasonal variations

A conservative approach is advisable: if capacity regularly approaches threshold levels, assume the higher tier applies.

---

3. Requirements: What Must Your Organisation Do?

Standard Tier (200-799 Capacity)

1. Notify the SIA

Duty holders must register with the Security Industry Authority, providing basic information about the premises, capacity, and responsible person [1].

2. Implement Public Protection Procedures

Organisations must have in place, so far as reasonably practicable, appropriate procedures that could be expected to reduce the risk of physical harm if a terrorist attack were to occur [1]. Examples include:

- **Evacuation procedures:** Defined routes, assembly points, staff training
- **Lockdown protocols:** Criteria for initiating lockdown, securing entry points, communication methods
- **Suspicious behaviour reporting:** Staff training, reporting channels, liaison with police

- **Incident command:** Designated commanders, communication systems, coordination with emergency services

Crucially, there is no requirement for Standard Tier premises to install physical security measures such as CCTV, access control, or barriers [4].

Enhanced Tier (800+ Capacity)

Enhanced Tier premises and events must meet all Standard Tier requirements **plus**:

1. Implement Public Protection Measures

In addition to procedures, Enhanced Tier duty holders must implement, so far as reasonably practicable, appropriate measures that could be expected to reduce both the vulnerability of the premises to attack and the risk of harm if an attack occurs [1]. Examples include:

- **Access control and screening:** Bag searches, metal detectors, entry management
- **Surveillance:** CCTV systems with monitoring arrangements
- **Perimeter security:** Hostile vehicle mitigation, fencing, lighting
- **Security staffing:** Trained personnel, control rooms, coordination with police
- **Technology:** Intrusion detection, public address systems, integrated security systems

2. Document and Submit to the SIA

Enhanced Tier duty holders must document their procedures and measures and provide this documentation to the SIA [1]. This creates an auditable compliance record and enables regulatory oversight.

---

4. The Responsible Person: Accountability and Competence

The Act requires designation of a “responsible person” for each qualifying premises or event [1]. This individual holds legal accountability for compliance and must possess:

- **Authority:** Ability to make decisions and allocate resources
- **Competence:** Knowledge of terrorism risks, protective security, and regulatory requirements
- **Resources:** Access to budget, personnel, and specialist support

The responsible person is typically a senior manager, security director, or compliance officer. In complex organisations, responsibility may be shared, but accountability must remain clear and documented.

Board-Level Implications:

- The responsible person should report directly to the board or executive leadership
- Boards should ensure the responsible person has adequate authority and resources
- Compliance status should be a standing agenda item for risk and audit committees
- Directors may face personal liability if governance failures contribute to non-compliance

---

5. Reasonably Practicable: The Compliance Standard

The phrase “so far as reasonably practicable” appears throughout the Act and is central to compliance [1]. This term has a well-established legal meaning: duty holders must balance the risk of harm against the cost, time, and effort required to mitigate that risk [5].

Reasonably practicable is not the same as possible. Organisations are not required to implement every conceivable security measure, only those where the risk reduction justifies the expenditure.

Factors to consider:

- Nature of the premises or event
- Threat and risk profile
- Resources available (financial, operational, personnel)

- Effectiveness of proposed measures
- Integration with existing safety and security arrangements

This standard provides flexibility whilst maintaining accountability. However, it also places the onus on duty holders to demonstrate that they have systematically assessed risks and adopted appropriate measures.

---

6. The Regulator: Security Industry Authority

The Security Industry Authority (SIA) will oversee compliance with Martyn's Law [6]. The SIA's regulatory functions include:

- **Guidance:** Publishing operational guidance and supporting duty holders
- **Monitoring:** Maintaining a register of premises, conducting inspections, reviewing documentation
- **Enforcement:** Issuing compliance notices, imposing financial penalties, prosecuting serious breaches

The SIA has indicated a proportionate, supportive approach, prioritising education over enforcement during the initial implementation period [6]. However, serious or persistent non-compliance may result in sanctions, including:

- Compliance notices requiring remedial action
- Financial penalties calibrated to the severity of the breach
- Criminal prosecution for reckless disregard or obstruction

---

7. Implementation Timeline: 24-Month Roadmap

The Act provides a minimum 24-month implementation period from Royal Assent (April 2025) to anticipated commencement (April 2027) [1]. Organisations should adopt a phased approach:

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

- Determine scope and applicable tier for all premises

- Brief leadership and establish governance structures
- Allocate initial budget and resources

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

- Audit current security posture
- Conduct terrorism risk assessments
- Identify gaps and prioritise actions

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

- Draft public protection procedures
- Document Enhanced Tier measures
- Integrate with existing policies

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

- Procure and install security technology and infrastructure (Enhanced Tier)
- Test systems and establish operational procedures

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

- Deliver staff training on procedures and measures
- Conduct scenario-based exercises
- Communicate with stakeholders

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

- Register with the SIA
- Conduct final testing and exercises
- Achieve full operational compliance

---

8. Strategic Risks and Opportunities

Risks of Non-Compliance

- **Regulatory Sanctions:** Financial penalties, prosecution, reputational damage
- **Operational Disruption:** Compliance notices may require immediate remedial action, disrupting operations
- **Liability Exposure:** Failure to comply may increase civil liability following incidents
- **Stakeholder Confidence:** Customers, employees, and investors expect organisations to take security seriously

Opportunities from Proactive Compliance

- **Enhanced Resilience:** Effective procedures and measures improve preparedness for terrorism and other emergencies
- **Competitive Advantage:** Demonstrating robust security can enhance brand reputation and customer confidence
- **Operational Efficiency:** Integrating Martyn's Law with existing risk management frameworks can streamline compliance
- **Stakeholder Assurance:** Proactive compliance demonstrates corporate responsibility and duty of care

---

9. Recommended Actions for Senior Leadership

Immediate Actions (Next 3 Months)

1. **Conduct Scoping Assessment:** Determine which premises and events fall within scope and identify applicable tiers
2. **Designate Responsible Person:** Appoint a competent individual with authority and resources
3. **Allocate Budget:** Estimate compliance costs and secure funding for assessments, training, and measures

4. **Engage Stakeholders:** Brief board members, senior managers, and operational teams on Martyn's Law implications
5. **Establish Governance:** Create a cross-functional working group to oversee compliance efforts

Medium-Term Actions (Months 4-12)

1. **Commission Risk Assessments:** Engage specialists to conduct terrorism risk assessments for qualifying premises
2. **Develop Procedures:** Draft public protection procedures, integrating with existing emergency plans
3. **Plan Physical Measures:** For Enhanced Tier premises, design and procure security technology and infrastructure
4. **Engage the SIA:** Monitor SIA guidance publications and participate in industry consultations
5. **Communicate Internally:** Keep staff informed of compliance activities and their roles in preparedness

Long-Term Actions (Months 13-24)

1. **Implement Measures:** Install and test physical security measures for Enhanced Tier premises
2. **Deliver Training:** Roll out comprehensive staff training on procedures, measures, and competency requirements
3. **Conduct Exercises:** Test procedures through tabletop and full-scale exercises, incorporating lessons learned
4. **Register with SIA:** Complete notification and submit Enhanced Tier documentation
5. **Establish Continuous Improvement:** Implement governance structures for ongoing compliance monitoring and review

---

10. Conclusion: Leadership Imperative

Martyn's Law represents a fundamental shift in how the United Kingdom approaches counter-terrorism preparedness for publicly accessible locations. For senior leaders, this is not merely a compliance obligation but a strategic imperative that touches upon legal risk, operational resilience, corporate responsibility, and stakeholder confidence.

Organisations that adopt a proactive, strategic approach—commencing planning now, allocating adequate resources, and integrating compliance with existing governance frameworks—will be well-positioned to meet their legal obligations whilst achieving genuine security improvements. Those that delay or adopt a minimalist approach risk regulatory sanctions, operational disruption, and reputational damage.

The 24-month implementation period provides a critical window for preparation. Senior leaders must ensure that their organisations seize this opportunity, demonstrating the duty of care that the public, employees, and stakeholders rightly expect.

Rittel Consulting Limited stands ready to support organisations at every stage of their Martyn's Law journey, from initial scoping and risk assessment 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 lasting security enhancements.

References

[1] UK Parliament. (2025). *Terrorism (Protection of Premises) Act 2025*. Retrieved from https://www.legislation.gov.uk/ukpga/2025/10/contents

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

[3] Home Office. (2023). *Protect Duty: Public Consultation Response*. Retrieved from https://www.gov.uk/government/consultations/protect-duty

[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

[5] Edwards v National Coal Board [1949] 1 KB 704

[6] Home Office. (2025). *Terrorism (Protection of Premises) Act 2025: The regulator, sanctions and enforcement factsheet*. Retrieved from https://www.gov.uk/government/publications/terrorism-protection-of-premises-act-2025-factsheets/terrorism-protection-of-premises-act-2025-the-regulator-sanctions-and-enforcement-factsheet

---

Document Information

Author: Rittel Consulting Limited
Publication: The Cambridge Sentinel Executive Briefing Series
Version: 1.0
Date: December 2025
Document ID: CS-ML-EXM-001

Disclaimer: This executive memo provides general guidance on Martyn's Law 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.