Martyn’s Law Implementation Timeline

24-Month Project Plan for Operations Managers

Document Information:

- **Author:** Rittel Consulting Limited
- **Publication:** The Cambridge Sentinel
- **Version:** 1.0
- **Date:** December 2025
- **Document ID:** CS-ML-GNT-001
- **Copyright:** © 2025 Rittel Consulting Limited. All Rights Reserved.

Executive Summary

This implementation timeline provides a structured 24-month roadmap for achieving Martyn’s Law compliance. The plan is designed for operations managers and directors responsible for implementing protective security measures across Standard Tier (200+ capacity) and Enhanced Tier (800+ capacity) premises.

The timeline is organized into six key phases with clear milestones, resource requirements, and deliverables. Color coding indicates phase type: **Assessment** (Blue), **Planning** (Green), **Implementation** (Orange), **Testing** (Purple), **Compliance** (Red), and **Ongoing** (Grey).

Implementation Timeline Overview

PHASE 1: Initial Assessment & Gap Analysis (Months 1-3)

Phase Type: Assessment | **Duration:** 12 weeks | **Resource Level:** Medium

Key Activities:

- Scope determination (Standard vs Enhanced Tier)
- Current security posture assessment
- Gap analysis against Martyn's Law requirements
- Stakeholder identification and engagement
- Budget and resource planning

Milestones:

- Week 4: Scope confirmation and tier classification complete
- Week 8: Gap analysis report delivered
- Week 12: Initial project plan and budget approved

Resource Requirements:

- Project Manager (50% FTE)
- Security Consultant (External, 20 days)
- Operations Manager (25% FTE)
- Finance Representative (10% FTE)

Deliverables:

- Scope determination document
- Gap analysis report
- Risk register
- Initial project plan
- Budget proposal

PHASE 2: Detailed Planning & Design (Months 4-6)

Phase Type: Planning | **Duration:** 12 weeks | **Resource Level:** High

Key Activities:

- Develop comprehensive security plan
- Design physical security enhancements
- Create procedural security measures
- Develop training programs
- Establish governance framework
- Appoint responsible person

Milestones:

- Week 16: Responsible person appointed
- Week 20: Security plan draft complete
- Week 24: All designs and procedures approved

Resource Requirements:

- Project Manager (75% FTE)
- Security Consultant (External, 30 days)
- Facilities Manager (50% FTE)
- HR Representative (25% FTE)
- Legal Advisor (10 days)
- IT Manager (25% FTE)

Deliverables:

- Comprehensive security plan
- Physical security designs
- Standard operating procedures
- Training curriculum
- Governance framework

- Responsible person appointment letter

PHASE 3: Physical Security Implementation (Months 7-12)

Phase Type: Implementation | **Duration:** 24 weeks | **Resource Level:** Very High

Key Activities:

- Install perimeter security enhancements
- Implement access control systems
- Deploy CCTV and surveillance systems
- Enhance lighting and signage
- Establish security control room (Enhanced Tier)
- Install emergency communication systems

Milestones:

- Month 8: Perimeter security complete
- Month 10: Access control systems operational
- Month 12: All physical security measures installed

Resource Requirements:

- Project Manager (100% FTE)
- Facilities Manager (75% FTE)
- Security Contractor (External, full project duration)
- Electrical Contractor (External, 60 days)
- IT Manager (50% FTE)
- Health & Safety Officer (25% FTE)

Deliverables:

- Installed perimeter security
- Operational access control systems
- CCTV and surveillance infrastructure

- Enhanced lighting and signage
- Security control room (Enhanced Tier)
- Emergency communication systems

PHASE 4: Procedural Security & Training (Months 10-15)

Phase Type: Implementation | **Duration:** 24 weeks | **Resource Level:** High

Note: This phase runs partially in parallel with Phase 3

Key Activities:

- Implement security procedures
- Conduct staff training programs
- Establish incident response protocols
- Create evacuation and lockdown procedures
- Develop counter-terrorism awareness
- Implement visitor management systems

Milestones:

- Month 11: All procedures documented and approved
- Month 13: 75% of staff trained
- Month 15: 100% of staff trained and competent

Resource Requirements:

- Training Manager (75% FTE)
- Security Consultant (External, 25 days)
- HR Representative (50% FTE)
- Operations Manager (50% FTE)
- Communications Officer (25% FTE)

Deliverables:

- Documented security procedures

- Trained workforce (100% compliance)
- Incident response protocols
- Evacuation and lockdown procedures
- Counter-terrorism awareness program
- Visitor management system

PHASE 5: Testing, Validation & Certification (Months 16-20)

Phase Type: Testing | **Duration:** 20 weeks | **Resource Level:** Medium

Key Activities:

- Conduct tabletop exercises
- Perform live evacuation drills
- Test all security systems
- Validate procedures and training
- Conduct third-party security audit
- Prepare compliance documentation

Milestones:

- Month 17: All systems tested and validated
- Month 18: Tabletop exercises complete
- Month 19: Live drills successful
- Month 20: Third-party audit passed

Resource Requirements:

- Project Manager (50% FTE)
- Security Consultant (External, 20 days)
- Operations Manager (50% FTE)
- All Department Heads (10% FTE each)
- Third-Party Auditor (External, 10 days)

Deliverables:

- System test reports
- Exercise and drill reports
- Validated procedures
- Third-party audit report
- Compliance documentation package
- Lessons learned register

PHASE 6: Compliance & Ongoing Operations (Months 21-24+)

Phase Type: Compliance & Ongoing | **Duration:** Ongoing | **Resource Level:** Low-Medium

Key Activities:

- Submit compliance documentation to regulator
- Establish ongoing review and monitoring
- Implement continuous improvement program
- Conduct regular drills and exercises
- Maintain training currency
- Update security plans as needed

Milestones:

- Month 21: Compliance submission prepared
- Month 22: Compliance documentation submitted
- Month 24: Regulatory approval received (target)
- Ongoing: Quarterly reviews and annual audits

Resource Requirements:

- Responsible Person (25% FTE ongoing)
- Operations Manager (15% FTE ongoing)
- Security Consultant (External, 5 days per quarter)
- Training Coordinator (15% FTE ongoing)

Deliverables:

- Compliance submission to regulator
- Ongoing monitoring reports
- Quarterly review documentation
- Annual audit reports
- Updated security plans
- Continuous improvement register

Resource Planning Summary

Peak Resource Requirements (Months 7-12)

- **Internal Staff:** 4-5 FTE equivalent
- **External Consultants:** 2-3 specialists
- **Contractors:** Security and electrical contractors
- **Budget:** Highest expenditure period (60-70% of total budget)

Steady-State Operations (Month 24+)

- **Internal Staff:** 0.5-1.0 FTE equivalent
- **External Consultants:** Quarterly reviews
- **Budget:** 5-10% of initial implementation budget annually

---

Critical Success Factors

1. **Executive Sponsorship:** Secure board-level commitment and budget approval
2. **Responsible Person:** Appoint competent individual with appropriate authority
3. **Stakeholder Engagement:** Maintain communication with all affected parties
4. **Resource Allocation:** Ensure adequate staffing and budget throughout project

5. **Training Compliance:** Achieve 100% staff training and maintain currency
6. **Documentation:** Maintain comprehensive records for regulatory compliance
7. **Testing & Validation:** Conduct thorough testing before compliance submission

---

Risk Mitigation Strategies

Risk	Mitigation
Budget overruns	Establish contingency fund (15-20%), conduct monthly budget reviews
Timeline delays	Build buffer time into critical path, identify dependencies early
Staff resistance	Engage early, communicate benefits, provide comprehensive training
Technical failures	Conduct thorough testing, establish maintenance contracts
Regulatory changes	Monitor legislation updates, maintain flexibility in design
Resource unavailability	Cross-train staff, establish backup contractors

---

Gantt Chart Legend

Phase Colors:

- 🔵 **Blue:** Assessment phases
- 🟢 **Green:** Planning phases
- 🟠 **Orange:** Implementation phases
- 🟣 **Purple:** Testing phases
- 🔴 **Red:** Compliance phases
- ⚫ **Grey:** Ongoing operations

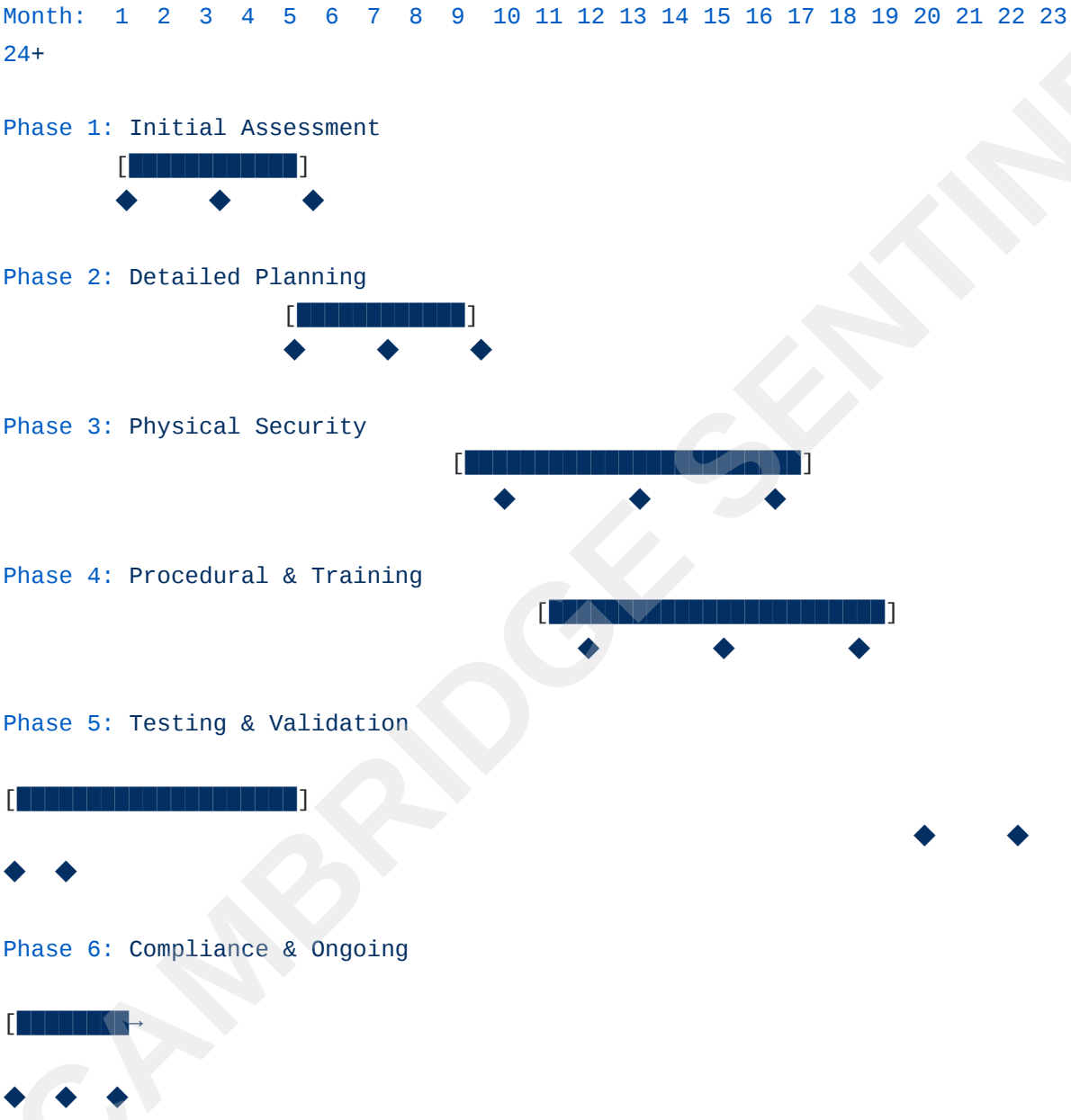
Resource Levels:

- **Low:** 0.5-1.5 FTE equivalent
- **Medium:** 1.5-3.0 FTE equivalent
- **High:** 3.0-5.0 FTE equivalent
- **Very High:** 5.0+ FTE equivalent

Milestone Indicators:

- ◆ Critical milestone
- ○ Standard milestone
- □ Optional milestone (Enhanced Tier only)

Visual Timeline (24 Months)



Detailed Gantt Chart

Months 1-6: Assessment & Planning

Week	Phase 1: Assessment	Phase 2: Planning	Key Milestones	Resources
1-2	Scope determination	-	-	PM, Security Consultant
3-4	Security assessment	-	◆ Scope confirmed	PM, Security Consultant, Ops Mgr
5-6	Gap analysis	-	-	PM, Security Consultant
7-8	Stakeholder engagement	-	◆ Gap analysis complete	PM, Ops Mgr, Finance
9-10	Budget planning	-	-	PM, Finance
11-12	Project plan approval	-	◆ Plan approved	PM, Exec Sponsor
13-14	-	Appoint responsible person	-	Exec Sponsor, HR
15-16	-	Develop security plan	◆ Responsible person appointed	PM, Security Consultant
17-18	-	Design physical security	-	PM, Facilities Mgr
19-20	-	Create procedures	◆ Security plan draft	PM, Ops Mgr, HR
21-22	-	Develop training	-	Training Mgr, HR
23-24	-	Governance framework	◆ All designs approved	PM, Legal, Exec Sponsor

Months 7-12: Physical Implementation

Month	Physical Security	Parallel Activities	Key Milestones	Resources
7	Perimeter security start	Procedure documentation	-	PM, Facilities, Contractors
8	Perimeter completion	Staff communication	◆ Perimeter complete	PM, Facilities, Comms
9	Access control install	Training material prep	-	PM, IT, Contractors
10	CCTV deployment	Pilot training sessions	◆ Access control live	PM, IT, Training Mgr
11	Lighting & signage	Full training rollout	-	PM, Facilities, Training Mgr
12	Emergency systems	Procedure implementation	◆ Physical security complete	PM, IT, Ops Mgr

Months 13-18: Training & Testing

Month	Training & Procedures	Testing Activities	Key Milestones	Resources
13	Continued training	-	◆ 75% staff trained	Training Mgr, HR
14	Visitor management	-	-	Ops Mgr, IT
15	Final training push	-	◆ 100% staff trained	Training Mgr, HR
16	-	System testing start	-	PM, IT, Facilities
17	-	Comprehensive testing	◆ Systems validated	PM, Security Consultant
18	-	Tabletop exercises	◆ Exercises complete	PM, Ops Mgr, Dept Heads

Months 19-24: Validation & Compliance

Month	Validation	Compliance	Key Milestones	Resources
19	Live drills	Documentation prep	◆ Drills successful	PM, Ops Mgr, All Staff
20	Third-party audit	Compliance package	◆ Audit passed	PM, Third-Party Auditor
21	Lessons learned	Submission prep	◆ Submission ready	PM, Responsible Person
22	-	Submit to regulator	◆ Submitted	Responsible Person, Legal
23	-	Regulator review	-	Responsible Person
24	-	Approval received	◆ Compliance achieved	Responsible Person, Exec Sponsor

Budget Allocation by Phase

Phase	% of Total Budget	Typical Activities
Phase 1: Assessment	5-8%	Consultancy, gap analysis, planning
Phase 2: Planning	8-12%	Design, procedures, governance setup
Phase 3: Physical Security	50-60%	Equipment, installation, contractors
Phase 4: Training	10-15%	Training delivery, materials, time
Phase 5: Testing	5-8%	Exercises, audits, validation
Phase 6: Ongoing	5-10% annually	Maintenance, reviews, updates

Dependencies & Critical Path

Critical Path Activities (delays will impact overall timeline):

1. Scope determination → Gap analysis → Budget approval
2. Responsible person appointment → Security plan development
3. Physical security design → Contractor procurement → Installation
4. Training material development → Staff training delivery
5. System testing → Third-party audit → Compliance submission

Parallel Workstreams (can run concurrently):

- Physical security installation + Procedural development
- Training delivery + System testing
- Documentation preparation + Validation activities

Governance & Reporting

Weekly:

- Project team status meetings
- Risk register updates

Monthly:

- Steering committee reports
- Budget variance analysis
- Milestone progress review

Quarterly:

- Executive board updates
- Stakeholder communications
- Phase gate reviews

Annual (Post-Compliance):

- Comprehensive security review
- Training effectiveness assessment

- Regulatory compliance audit

Next Steps

1. **Immediate (Week 1):** Secure executive sponsorship and budget approval
2. **Short-term (Month 1):** Engage security consultant and commence scope determination
3. **Medium-term (Month 4):** Appoint responsible person and initiate detailed planning
4. **Long-term (Month 24):** Achieve regulatory compliance and transition to ongoing operations

---

References

Home Office (2024) *Protect Duty (Martyn's Law): Draft Legislation*. Available at: https://www.gov.uk/government/collections/protect-duty (Accessed: 20 December 2025).

ProtectUK (2024) *Martyn's Law Overview and What You Need to Know*. Available at: https://www.protectuk.police.uk/martyns-law (Accessed: 20 December 2025).

Security Industry Authority (2024) *Counter-Terrorism Preparedness*. Available at: https://www.sia.homeoffice.gov.uk (Accessed: 20 December 2025).

For bespoke implementation support and project management services, contact:

Rittel Consulting Limited
Email: terry.hanley@rittelconsulting.co.uk
Web: www.rittelconsulting.co.uk

This document is published by The Cambridge Sentinel, a Rittel Consulting service providing intelligence and risk assessment for security professionals across the UK.

Document Control:

- Version: 1.0
- Date: December 2025
- Document ID: CS-ML-GNT-001
- Classification: Public
- Review Date: June 2026