



**The National Examination
Board in Occupational Safety
and Health (NEBOSH)**

Dominus Way,
Meridian Business Park,
Leicester LE19 1QW

Tel: +44 (0) 116 263 4700

Fax: +44 (0) 116 282 4000

Email: info@nebosh.org.uk

www.nebosh.org.uk

Version: 1

Specification date: October 2025

Publication date: November 2025

Registered Charity Number: 1010444

© NEBOSH. All rights reserved. No part of this publication
may be reproduced, stored in a retrieval system or transmitted
in any form, or by any means, electronic, electrostatic,
mechanical, photocopied or otherwise, without the express
permission in writing from NEBOSH.

NEBOSH National Certificate in Protecting Enhanced Duty Premises and Events from Terrorism

Qualification guide for Learning Partners

Contents

Qualification overview

Qualification key features	4
----------------------------	---

Qualification summary

Introduction	6
Notional learning hours	6
Teaching of syllabus content	6
Minimum standard of English requirements	6
Achieving the qualification	7
Date of assessment	7
Registration	7
Submission of the assessment	7
Identifying learners	7
Marking	8
Individual learner feedback	8
Results	8
Conflict of Interest	8

Syllabus

Syllabus summary	10
Learning outcomes and assessment criteria	11
Syllabus content	14

Qualification overview

Qualification overview

Qualification key features

Unit prefixes and title/s	Unit PTE1: Protecting Enhanced Duty Premises and Events from Terrorism	
Assessment	Assessment Type	Assessment Time
Unit PTE1	Multiple format assessment (MFA)	60 minutes
Modes of study	Taught (face-to-face) Open, distance, part-time or block release eLearning	
Notional learning hours	Taught hours: 16 hours Private study hours: 3 hours Assessment: 1 hour Total hours: 20 hours	
Qualification level	Notional SCQF Level 6 / Equivalent to RQF Level 3	
Entry requirements	None	
Recommended minimum standards of English	Learners: International English Language Testing System (IELTS) 6.0 or higher Tutors: International English Language Testing System (IELTS) score of 7.0 or higher.	
Languages available	English	
Assessment dates/ registration	Monthly fixed date examinations. Registrations can be made at any time pre-course and up to 10 working days before the assessment date.	
Pass standards	A 'Pass' (score of 60% or higher) must be achieved in Unit PTE1	
Qualification grades	Pass Refer	
Parchment issue	Issued within 20 working days of the results declaration date	

Qualification summary

Qualification summary

Introduction

The Terrorism (Protection of Premises) Act 2025 (“Martyn’s Law”) places legal duties on certain public premises to consider the threat of terrorism, so that steps can be taken to protect against a potential attack and to keep people safe should an attack occur. Certain premises must also take steps to reduce their vulnerability to acts of terrorism.

NEBOSH has developed a suite of qualifications to support your learners in understanding and complying with these duties. This qualification is designed for those responsible for enhanced duty premises or events.

This course is for health and safety professionals and other workers involved in managing premises and events that fall under the **enhanced duty requirements** of the Terrorism (Protection of Premises) Act 2025.

Enhanced tier premises and qualifying events refers to publicly accessible premises or events where it is reasonable to expect that **800 or more** individuals may be present at the same time. Stricter legal duties are imposed due to the higher potential impact of any terrorist attack.

The syllabus and accompanying course book have been developed by NEBOSH, in conjunction with industry experts, and are based on the legal requirements of the Terrorism (Protection of Premises) Act 2025. Special thanks are given to Premier Partnership for their contributions to the syllabus and course materials.

On completion of this course, your learners will have a good understanding of:

- The nature of terrorism and the legal framework of the Terrorism (Protection of Premises) Act 2025
- Identifying and monitoring potential threats
- Understanding terrorist threats and site vulnerabilities
- Implementing public protection procedures
- Implementing public protection measures
- Documenting compliance with the Terrorism (Protection of Premises) 2025 Act
- Business continuity and recovery
- Developing a strong security culture

Notional learning hours

A programme of study needs to be based around a minimum of 16 taught hours and approximately 3 hours of private study for an overall total of 19 hours.

A full-time block release course would be expected to last for a minimum of three working days, and a part-time day release course would be spread over at least three weeks.

For learners studying by open or distance learning, the tuition hours should be added to the recommended private study hours to give the minimum number of hours that this mode of study will require.

Teaching of syllabus content

Although the syllabus sets out the elements in a specific order, you can teach the elements in any order you feel is appropriate.

Minimum standard of English requirements

The standard of English required by your learners studying for this qualification must be such that they can both understand and articulate the concepts contained in the syllabus. We recommend that learners have reached a minimum standard of English equivalent to an International English Language Testing System (IELTS) score of 6.0 or higher in IELTS tests. It is important to stress that it is your responsibility to determine your learners’ standards of proficiency in English.

Tutors who are based overseas and wish to deliver this qualification must have a good standard of English. They must be able to articulate the concepts contained in the syllabus. The Learning Partner must provide evidence of the tutor’s standard of English when submitting the tutor’s CV for approval. NEBOSH’s requirement is for tutors delivering this qualification to have reached a minimum standard of English equivalent to an International English Language Testing System score of 7.0 or higher in IELTS tests.

More information on IELTS can be found on the IELTS website.

Qualification summary

Achieving the qualification

The qualification has one unit assessment: a 60 minute online multiple-format assessment. 'Multiple format' means assessment papers which have questions with pre-populated answers to choose from. Unlike multiple-choice assessments (where each question only has one correct answer), multiple format assessments include a blend of different styles, such as multiple choice questions (one correct answer); multiple response questions (more than one correct answer), as well as different question styles (e.g. rank, categorise, fill in the blanks etc).

The question paper consists of 30 multiple-format questions; 8 of which are mini scenario questions. Each question is worth one mark. The question paper covers the whole syllabus with at least one question per element. All questions are compulsory. It is a closed-book assessment, so learners will not be able to refer to your course book and notes.

Learners must achieve a 'pass' (60% or higher) in order to be awarded the qualification.

Date of assessment

Assessments are taken after completion of the course learning. Assessments are held monthly, with the assessment being available for a 24 hour period. Learners will be able to start their assessment at any time during this 24 hour window, but will have 60 minutes in total to complete their assessment.

More information, including upcoming assessment dates are available on the NEBOSH website.

Registration

The Learning Partner must register learners for the PTE1 unit assessment. Registration can be made at any time precourse delivery, and up to 10 working days pre-assessment.

Submission of the assessment

Learners will complete their assessment online, and submit their assessment through an online assessment platform for marking.

Identifying learners

The course tutor must be sure of the identity of all learners prior to qualification delivery. This should be done ahead of the training; on the day for classroom delivery; or, for distance or eLearning, verification can be undertaken remotely via webcam. This will involve checking photographic identification. Photographic evidence of identity includes driving licences, national identity cards and passports. If you are unable to identify the learner, then you should contact NEBOSH for further advice.



"Martyn's Law positions the UK as a leader in counterterrorism by requiring a consistent approach to terrorism preparedness. It clarifies who is responsible at qualifying premises and events and what they must do. It calls for clear risk understanding, consistent practices, and strong collaboration to foster a safety-focused culture"

Rhian Greaves

Partner Regulatory – Safety, Health & Environment, DAC BEACHCROFT

Qualification summary

Marking

Assessments are marked by NEBOSH. Learners will receive a 'Pass' (60% or higher) or 'Refer' (59% or lower) for their assessments. It is your responsibility as a Learning Partner to provide your learners with more support in the event of a referral result, and register them for another date to re-sit their assessment.

Individual learner feedback

For more information on the assessment feedback provided for this qualification, please visit the NEBOSH website.

Results

We aim to issue results within 15 working days of the date of the assessment. Qualification parchments are issued normally within 20 working days of confirmation of the successful PTE1 unit.

Conflict of Interest

If any of your staff, family or friends want to sit the qualification you must tell NEBOSH first. Further information can be found in the 'Instructions for Conducting Examinations' document on the NEBOSH website.



Syllabus

Syllabus

Syllabus summary

Element		Recommended tuition hours	Assessment
1	The nature of terrorism and the legal framework	2	Unit PTE1: Protecting Enhanced Duty Premises and Events from Terrorism Multiple-format assessment (MFA)
2	Identifying and monitoring potential threats	1	
3	Understanding terrorist threats and site vulnerabilities	2	
4	Implementing public protection procedures	2	
5	Implementing public protection measures	3	
6	Documenting compliance with the 2025 Act	3	
7	Business continuity and recovery	2	
8	Developing a strong security culture	1	
Total hours		16	1

Syllabus

Learning outcomes and assessment criteria

Learning outcome The learner will be able to:	Related content	Assessment criteria	Assessment
Understand the nature of terrorism, including motivating factors and common ideologies.	1.1	Recognise the nature of terrorism and its motivating factors.	MFA
Understand how the main duties of key health and safety legislation apply to the threat of terrorism-related incidents in the workplace.	1.2	Recognise how the Health and Safety at Work etc Act 1974 and the Management of Health and Safety at Work Regulations 1999 apply to the threat of terrorism-related incidents.	
Understand what constitutes a 'qualifying event' and 'qualifying premises' under the 2025 Act, including the distinction between standard and enhanced duty premises.	1.3, 1.4, 1.5	Outline the scope of the 2025 Act, including key definitions, legal duties and the role of the SIA, including civil sanctions, criminal offences and penalties.	
Understand the legal duties placed on those responsible for qualifying premises and qualifying events under the 2025 Act.			
Understand the role of the Security Industry Authority (SIA) and enforcement action taken for non-compliance with the 2025 Act.			

Syllabus

Learning outcome The learner will be able to:	Related content	Assessment criteria	Assessment
Interpret national terrorism threat levels, intelligence guidance and target attractiveness, and use this information to inform proportionate and context-specific decision-making.	2.1 2.2 2.3	Understand the UK's threat level system and its implications. Recognise the available sources of credible information regarding threat levels. Recognise factors that impact the overall threat level. Outline organisational responsibilities for monitoring threat intelligence.	MFA
Understand terrorist threats and site-specific vulnerabilities.	3.1, 3.2	Evaluate terrorist threats. Evaluate site-specific vulnerabilities to terrorism-related activities.	MFA
Implement public protection procedures, as far as is reasonably practicable. Describe appropriate emergency responses to terrorism-related incidents, and explain how to communicate and coordinate effectively with emergency services and other agencies.	4.1 4.2 4.3 4.4	Identify the meaning and scope of public protection procedures. Understand the concept of reasonable practicability as it applies to the 2025 Act. Recognise emergency response options for different types of terrorist threat. Describe effective internal and external communication processes. Identify trauma first aid and worker competency in the event of a terrorist attack.	MFA

Syllabus

Learning outcome The learner will be able to:	Related content	Assessment criteria	Assessment
Implement public protection measures.	5.1	Explain the meaning and scope of public protection measures.	MFA
Select, implement and justify layered protective security measures appropriate to the identified threat, using established security models.	5.2	Apply the Deter–Detect–Delay–Deny model.	
	5.3	Explain scenario-based control selection.	
Document compliance with the Terrorism (Protection of Premises) 2025 Act.	6.1	Describe the requirements for documenting public protection procedures and measures.	MFA
Conduct and document assessments using recognised principles to identify vulnerabilities, evaluate risks and prioritise control measures.	6.2	Assess the likelihood and impact of terrorist threat.	
	6.3	Outline the requirement to record and review findings.	
Explain the immediate and longer-term organisational actions required following a terrorist incident, including documentation, investigation, workers' welfare and continuous improvement.	7.1	Outline casualty care and triage.	MFA
	7.2	Outline post-incident documentation and investigation.	
Promote a positive security culture within organisations by recognising the importance of effective leadership and engaging workers at all levels.	8.1	Identify characteristics of a positive security culture.	MFA
	8.2	Outline leadership's role in promoting positive counter-terrorism behaviours.	
	8.3	Identify the benefits of a positive security culture.	

Syllabus content

Important note: learners are not expected to remember the Section/Regulation numbers but they will need to be familiar with the main requirements of the legislation.

Element 1: The nature of terrorism and the legal framework	
1.1	What constitutes terrorism under UK law and common motivating factors • The definition of terrorism under the Terrorism Act 2000, Section 1 • Concept of an ideology • Motivating factors behind terrorism, including: > Ethno-nationalist and separatist causes > Extreme right-wing ideologies > Religiously motivated extremism > Left wing, anarchist and single-issue extremism > Emerging threats such as 'mixed, unclear or unstable' ideologies.
1.2	UK health and safety legislation applicable to counter-terrorism • Health and Safety at Work etc Act 1974, Sections 2, 3 and 4 (places duties on employers and those in charge of premises to take reasonably practicable steps to ensure health and safety) • Management of Health and Safety at Work Regulations 1999, Regulation 3 (require a suitable and sufficient assessment of risks).
1.3	Application of the Terrorism (Protection of Premises) Act 2025 (the '2025 Act') ('Martyn's Law') to premises and events • Definition of 'qualifying premises' (Section 2 and Schedules 1 and 2) • The differences between 'enhanced duty' and 'standard duty' premises (Section 2) • Definition of 'qualifying events' (Section 3) • Methods to assess the number of individuals expected to be present at an event or premises, to determine the extent of the duty.
1.4	Responsible persons and duties under the 2025 Act • Identifying persons responsible for qualifying premises and qualifying events, including situations where there is more than one Responsible Person (Section 4) • The requirements that apply to standard duty premises, including notification and implementing appropriate public protection procedures <i>[cross reference element 4]</i>

Element 1: The nature of terrorism and the legal framework	
	- The requirements that apply to enhanced duty premises and qualifying events, including notification, designation of a senior individual, public protection procedures <i>[cross reference element 4]</i> and measures <i>[cross reference element 5]</i> and documenting compliance <i>[cross reference element 6]</i> - Cooperation and coordination between responsible persons (Section 8).
1.5	Regulation and enforcement of the 2025 Act - The role of the Security Industry Authority (SIA) under the 2025 Act (Section 12 and Schedule 3): - Use investigatory powers to assess compliance - Take enforcement action - Advise on regulatory requirements - Support those responsible for qualifying premises and events to meet their obligations - Review the effectiveness of risk reduction requirements in the 2025 Act and the vulnerability of enhanced duty premises and events to acts of terrorism - Investigatory powers of the SIA (Schedule 3): - Authorised inspectors - Information gathering powers - Entry to premises (with and without a warrant) - Retention of evidence - Types of civil sanctions issued by the SIA and when they would typically be issued: - compliance notices (Section 13) - restriction notices (Section 14) - penalty notices (Section 17) - Criminal offences, penalties and relevant sanctions under the 2025 Act: - Failure to comply with information, compliance or restriction notices (Schedule 3 and Section 24) - Providing false or misleading information to the SIA (Section 25) - Intentionally obstructing or impersonating an authorised inspector (Schedule 3) - Liability of an individual for an offence committed by an organisation (section 26).

Element 2: Identifying and monitoring potential threats	
2.1	UK threat levels and their impact on controls - The national threat level system, including: > How threat levels (low to moderate, substantial to severe, critical) relate to operational decision-making. > Recognition that threat levels are not location-specific and should be considered alongside local threat intelligence.
2.2	Site-specific factors that impact the level of threat - Target attractiveness > Symbolic or reputational profile > Crowded areas > Visitor profile > Publicity > Perceived vulnerabilities > Financial impact > Psychological harm.
2.3	Application of the Terrorism (Protection of Premises) Act 2025 (the '2025 Act') ('Martyn's Law') to premises and events - Importance of: > Regularly monitoring relevant intelligence and threat updates > Maintaining up-to-date situational awareness to inform proportionate responses > Establishing clear processes for escalation, de-escalation and record-keeping - Practical organisational responses to changing threat levels, including: > Reviewing and updating assessments of public protection measures > Enhancing visible security measures > Re-briefing workers and contractors > Pausing high-risk activities or events (if advised) - Communicating expectations: > Ensuring relevant internal workers (including contractors and front-line workers) are made aware of changes > Communicating appropriately with external stakeholders (e.g. emergency services, neighbours, tenants).

Element 3: Understanding terrorist threats and site vulnerabilities

3.1 Understanding terrorist threats

- Types of credible terrorist threats relevant to publicly accessible locations:
 - > Marauding terrorist attacks
 - > Improvised explosive devices
 - > Vehicle as a weapon
 - > Fire as a weapon
 - > Chemical, biological, radiological and nuclear threats
 - > Cyber-enabled attacks
 - > Unmanned aerial vehicles.

3.2 Understanding possible site vulnerabilities

- What is meant by hostile reconnaissance, and indicators that may suggest its presence
- Types of vulnerability:
 - > Operational vulnerabilities: crowd management (eg avoidance of stampedes), visitor access, worker training and worker/contractor vetting
 - > Physical vulnerabilities: perimeter security, worker access control and site surveillance
 - > Technological vulnerabilities: IT systems, network security and protection of data
- How vulnerabilities may vary based on time of day, event type, occupancy, and external threats
- How attackers may exploit site vulnerabilities
 - > Hostile reconnaissance, and indicators that may suggest its presence
 - > Insider threats.

Element 4: Implementing public protection procedures

4.1 Meaning and scope of public protection procedures under the 2025 Act, Section 5

- Definition of 'public protection procedures'
- Scope of public protection procedures to include:
 - > Evacuation *[cross reference 4.2]*
 - > Invacuation *[cross reference 4.2]*
 - > Lockdown and prevention of entry *[cross reference 4.2]*
 - > Communication and information provision *[cross reference 4.3]*

Element 4: Implementing public protection procedures	
	- Assessing suitability of public protection procedures: - Identify vulnerabilities and at-risk assets - Existing controls to reduce vulnerability to acts of terrorism - Identification of further controls (and the need to apply them) - Communication of the procedures to workers and other relevant people - The importance of regular reviews and the triggers for this - Integration of the procedures into broader site risk registers and/or business continuity plans.
4.2	Emergency responses to a range of terrorism-related incidents - Emergency response options for different types of terrorist threat: - Evacuation - Invacuation - Lockdown - Shelter-in-place with reference to chemical, biological and radiological threats - Good practice in response planning, including: - Identifying trigger points for each response type - Assigning roles and responsibilities for key workers - Selection of communication methods - Accounting for vulnerable people and visitors - Maintaining safe exit routes and assembly points - The concept of Run, Hide, Tell as guidance for public and workers during a marauding terrorist attack - The role of first responders in early casualty care - Requirements for rehearsals, drills and regular testing of emergency plans.
4.3	Effective internal and external communication planning during a terrorist incident - The importance of clear, timely and controlled communication during an incident - Inclusion of communication processes in training exercises and scenario exercises

Element 4: Implementing public protection procedures	
	• External communication requirements, including: > Notifying emergency services > Informing neighbouring premises or tenants (if appropriate) > Managing public and media communications.
4.4	Requirements for trauma first-aid and worker competence • Trauma equipment that may (subject to risk) be needed on site • Strategic placement and availability of first aid kits • Workers who may be expected to act as first responders, likely duties and training requirements.

Element 5: Implementing public protection measures	
5.1	Meaning and scope of public protection measures under the 2025 Act, Section 6 • Definition of 'public protection measures' (Section 6). • The duties imposed on persons responsible for enhanced duty premises or qualifying events. • The objectives of public protection measures: > to reduce vulnerability of a premises or event to an attack > to reduce the risk of harm if there is an attack > to risk assess the premises or event to determine appropriate measures • Scope of public protection measures to include: > Monitoring requirements > Controlling movement of people > Physical safety and security > Security of information • Keep public protection measures under review.

Element 5: Implementing public protection measures

5.2 Apply the Deter-Detect-Delay-Deny model to layered security

- The Deter–Detect–Delay–Deny model and its application in protective security planning:
 - > Deter: Visible measures that discourage hostile intent (i.e. uniformed personnel, signage, lighting)
 - > Detect: Early identification of threats or suspicious behaviour (i.e. motion sensors, alert systems, CCTV analytics)
 - > Delay: Barriers and processes that slow or interrupt a hostile actor’s progress (i.e. turnstiles, lockable doors, layered access zones)
 - > Deny: Final line of protection preventing access or harm (i.e. biometric access, secure areas, encryption).

5.3 Scalable scenario-specific measures

- Matching the scale and nature of controls to reflect the requirements of the enhanced tier, the risk level and what is reasonably practicable
- Typical terrorism risk controls tailored to specific scenarios and threats:
 - > Marauding terrorist attack: invacuation procedures, escape routes
 - > Improvised explosive device / vehicle borne improvised explosive device: vehicle exclusion zones, bag search protocols, suspicious item guidance
 - > Vehicle as a weapon: perimeter mitigation, traffic flow controls
 - > Chemical, biological, radiological, and nuclear: air handling isolation, shelter-in-place protocols, liaison with emergency services
 - > Cyber threats: business continuity plans, data protection, penetration testing.

Element 6: Documenting compliance with the 2025 Act

6.1 Scope of documenting compliance under the 2025 Act, Section 7

- Documenting requirements:
 - > Public protection procedures
 - > Public protection measures
 - > Justification as to how those public protection procedures and measures reduce the vulnerabilities and/or risk of harm if a terrorist attack were to occur
- Provision of documentation to the SIA
- Keeping the documents up to date and providing revisions to the SIA

Element 6: Documenting compliance with the 2025 Act

6.2 Assessing likelihood and impact using qualitative factors

- The essential need for assessments to be informed, comprehensive and based on credible sources.
- Likelihood factors: attractiveness of target, history of incidents, threat intelligence, existing controls, activities of others in the immediate vicinity
- Likelihood of attack method being successful
- Impact factors: potential casualties, disruption to business, economic and legal; reputational harm.
- Using informed assumptions, not guesswork or bias.

6.3 Record and review findings

- The components of an effective assessment of public protection measures to include:
 - > Description of the threat type(s)
 - > Identified vulnerabilities and at-risk assets
 - > Likelihood and impact analysis
 - > Use of likelihood impact matrices
 - > Existing controls to reduce vulnerability to acts of terrorism
 - > Further actions required (and the need to apply them)
 - > Review dates
- The importance of regular reviews and the triggers for this
- Integration of measures into broader site risk registers or business continuity plans.

Element 7: Business continuity and recovery

7.1 Priorities in the aftermath of a terrorism-related incident

- Securing the site
- Assisting emergency services with access, intelligence, and ongoing safety intel
- Accounting for workers, visitors, and contractors
- Assisting with triage by directing responders to the most critical injuries
- Supporting those in psychological shock/distress
- Aiding multi-agency coordination and the media, communicating clear, factual updates internally and externally.

Element 7: Business continuity and recovery

7.2 Documentation and post-incident investigation

- Essential need to capture timely and accurate incident documentation, including:
 - > Incident logs (timeline of decisions and actions taken)
 - > CCTV footage – immediate retention and safeguarding of recordings
 - > Witness statements – structured collection of workers and public observations
 - > Retention of internal messages, and any site access records, incident logs and CCTV footage
- Organisational support for formal investigations via:
 - > Ensuring evidence is preserved and secured
 - > Cooperating with police and regulatory bodies
 - > Designating a lead point of contact within the organisation
- The need to review and update all plans and documentation based on findings of subsequent investigation.

Element 8: Developing a strong security culture

8.1 Characteristics of a positive security culture, including:

- Visible leadership commitment to counter-terrorism readiness
- Widespread recognition that security is everyone's responsibility
- Open communication and encouragement of reporting suspicious behaviour or security breaches
- Proactive worker behaviours (e.g. vigilance, questioning unusual activity, supporting emergency procedures).

8.2 Leadership's role in allocating resources, modelling behaviours and typical barriers

- Visible executive sponsorship
- Ring-fenced counter terrorism budget
- Communicating clearly the purpose and importance of security responsibilities
- Involving workers in assessment, planning and review processes
- Holding people to account for security-related responsibilities and behaviours
- Typical barriers to change, including:
 - > Complacency or cultural resistance ("it won't happen here")
 - > Competing operational priorities or time constraints
 - > Fear of getting it wrong or misunderstanding legal duties.

Element 8: Developing a strong security culture

8.3

Benefits of developing and maintaining a positive security culture

- Early identification and escalation of hostile reconnaissance or insider threat indicators
- Effective implementation of physical and procedural controls
- Improved emergency response outcomes and public reassurance
- Reduced organisational risk and liability.