NEBOSH International Certificate in Protecting Premises and Events from Terrorism

Qualification guide for Learning Partners

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

Contents

Qualification overview

Qualification overview

Qualification key features

Unit prefixes and title/s	**Unit PTI1**: Protecting Premises and Events from Terrorism
Assessment **Unit PTI1**	**Assessment Type** Multiple format assessment (MFA) **Assessment Time** 60 minutes
Modes of study	Taught (face-to-face) Open, distance, part-time or block release eLearning
Notional learning hours	Taught hours: 17 hours Private study hours: 3 Assessment: 1 hour Total hours: 21 hours
Qualification level	Notional SCQF Level 6 / 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 standard	A 'Pass' (score of 60% or higher) must be achieved in Unit PTI1
Qualification grades	Pass Refer
Parchment issue	Issued within 20 working days of the results declaration date

Qualification summary

Qualification summary

Introduction

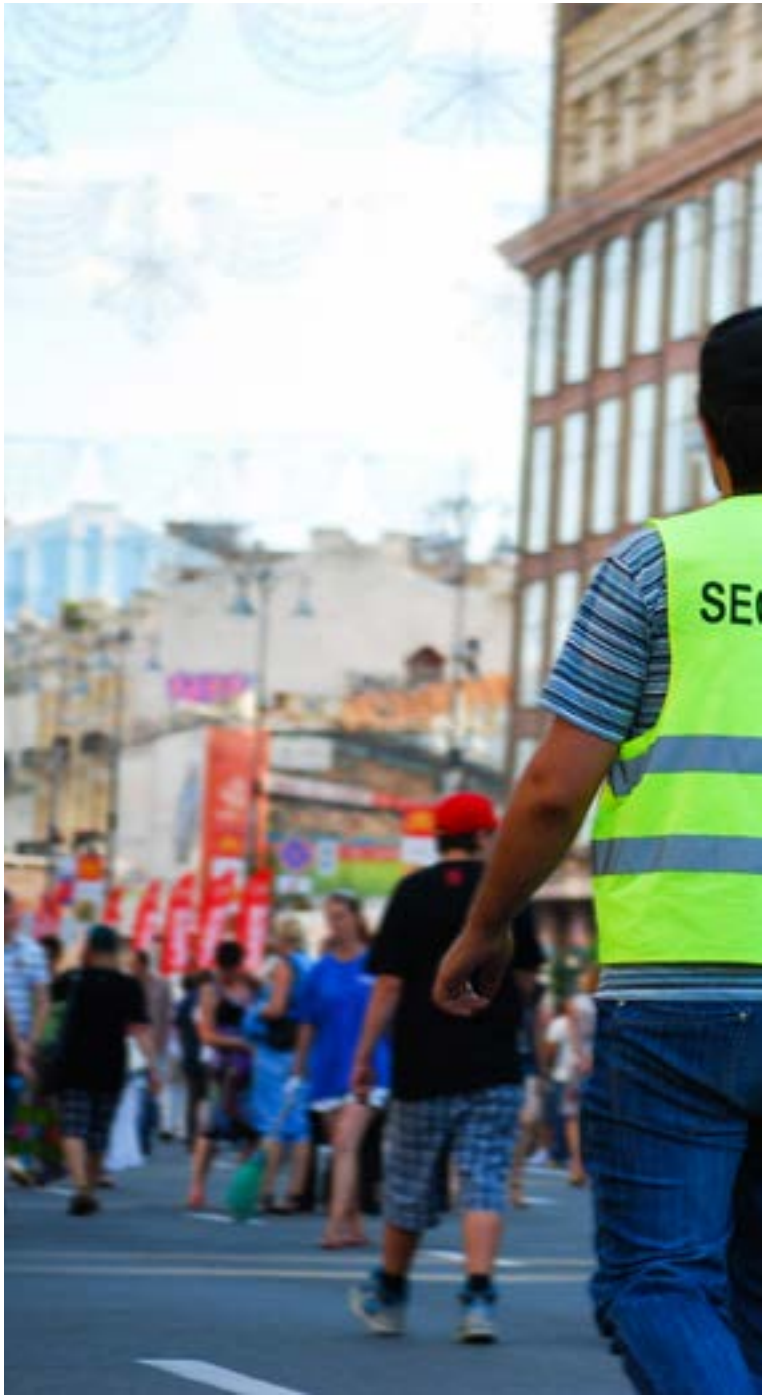
It is vital that publicly-accessible premises consider the threat of terrorism so that vulnerabilities can be identified, reduced and managed. NEBOSH has developed this qualification to help your learners support their organisations with this.

This course is for health and safety professionals and other workers involved in ensuring that that their organisation has considered and addressed the threat of terrorism in premises and events open to the public.

The syllabus and accompanying course book have been developed by NEBOSH, in conjunction with industry experts. 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 its motivating factors
- Identifying and monitoring potential threats
- Understanding terrorist threats and site vulnerabilities
- Implementing protection procedure
- Implementing protection measures
- Documenting requirements
- Business continuity and recovery
- Developing a strong security culture.



Qualification summary

Notional learning hours

A programme of study needs to be based around a minimum of 17 taught hours and approximately 3 hours of private study for an overall total of 20 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.

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.

Qualification summary

Registration

The Learning Partner must register learners for the PTI1 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.

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 PTI1 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 its motivating factors	2	**Unit PTI1: Protecting Premises and Events from Terrorism** Multiple-format assessment (MFA)
2	Identifying and monitoring potential threats	2	
3	Understanding terrorist threats and site vulnerabilities	2	
4	Implementing protection procedures	2	
5	Implementing protection measures	3	
6	Documenting requirements	3	
7	Business continuity and recovery	2	
8	Developing a strong security culture	1	
	Total hours	**17**	**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. Understand relevant legislation, health and safety frameworks and enforcement agencies to protect against terrorism-related activities.	**1.1** **1.2**	Recognise the nature of terrorism and its motivating factors. Identify key anti-terrorism legislation, frameworks and enforcement agencies.	MFA
Interpret national terrorism threat levels, target attractiveness and intelligence guidance, and use this information to inform proportionate and context-specific decision-making.	**2.1** **2.2** **2.3**	Understand the 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

Syllabus

Learning outcome The learner will be able to:	Related content	Assessment criteria	Assessment
Implement effective anti-terrorism protection procedures. 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 protection procedures. Recognise emergency response options for different types of terrorist threat. Identify effective internal and external communication processes. Identify trauma first aid and worker competency in the event of a terrorist attack.	MFA
Implement effective anti-terrorism protection measures. Select, implement and justify layered protective security measures appropriate to the identified threat, using established security models.	**5.1** **5.2** **5.3**	Explain the meaning and scope of protection measures. Apply the Deter–Detect–Delay–Deny model. Explain scenario-based control selection.	MFA

Syllabus

Learning outcome The learner will be able to:	Related content	Assessment criteria	Assessment
Understand the documenting requirements for protection procedures and measures. Conduct and document assessments using recognised principles to identify vulnerabilities, evaluate risks and prioritise control measures.	**6.1** **6.2** **6.3**	Describe the requirements for documenting protection procedures and measures. Assess the likelihood and impact of terrorist threat. Outline recording and reviewing findings.	MFA
Explain the immediate and longer-term organisational actions required following a terrorist incident, including documentation, investigation, workers' welfare and continuous improvement.	**7.1** **7.2**	Outline casualty care and triage. Outline post-incident documentation and investigation.	MFA
Promote a positive security culture within organisations by recognising the importance of effective leadership and engaging workers at all levels.	**8.1** **8.2** **8.3**	Identify the characteristics of a positive security culture. Outline leadership's role in promoting positive counter terrorism behaviours. Identify the benefits of a positive security culture.	MFA

Syllabus

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.

Learners will not be assessed on local legislation.

While national legislation and responsibilities differ, the course will maintain a consistent emphasis on international standards, recognised good practice, and proportionate protective security principles drawn from global experience.

Element 1: The nature of terrorism and its motivating factors	
1.1	**What constitutes terrorism and motivating factors** • A working definition of terrorism according to the UN Security Council Resolution 1566 (2004) • Motivating factors behind terrorism, including: - Ethno-nationalist and separatist causes - Extreme ideologies (e.g. anti-immigration, racial supremacy) - Religiously motivated extremism - Left wing, anarchist and single-issue extremism - Emerging threats such as 'mixed, unclear or unstable' ideologies.
1.2	**The legal framework and enforcement agencies** • Regional anti-terrorism legislation examples: - India: Unlawful Activities (Prevention) Act 1967 (UAPA) - Pakistan: Anti-Terrorism Act 1997 - Middle East: Gulf Cooperation Council Unified Law on Counter Terrorism; UAE Federal Law No. 7/2014; Saudi Arabia Penal Law for Crimes of Terrorism and its Financing 2017 • Relevant health and safety frameworks: ILO C155 - Occupational Safety and Health Convention, 1981; local civil defence legislation • National Counter-terrorism enforcement agencies (e.g. National Investigation Agency India, National Counter Terrorism Authority Pakistan, Ministries of Interior in Gulf Cooperation Council states).

Syllabus

Element 2: Threat levels and organisational duties	
2.1	**Threat levels and their impact on controls** • Threat level systems to include: - United States Department of Homeland Security National Terrorism Advisory System. - United Kingdom: Joint Terrorism Analysis Centre (JTAC) and MI5 - India: Ministry of Home Affairs threat advisories. - GCC: Ministry of Interior advisories / regional cooperation mechanisms. • Concept that every country interprets threat levels differently, and that organisations must monitor and respond to national guidance and international advisories (INTERPOL, the UN's Counter-Terrorism Committee). • 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.

Syllabus

Element 2: Threat levels and organisational duties	
2.3	**Organisational responsibilities for monitoring threat intelligence** • 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 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).

Syllabus

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 vulnerabilities: - 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.

Syllabus

Element 4: Implementing protection procedures	
4.1	**Meaning and scope of protection procedures in accessible premises and events** • Definition: Protection procedures are plans and actions designed to safeguard people during a terrorism-related incident, regardless of location or sector • Scope of 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*] • Assessing suitability of 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 to prioritise escaping if safe to do so, concealing if escape is not possible, and alerting the authorities at the first safe opportunity • Concept of 'Run, Hide, Fight' used in some jurisdictions; emphasises the same priorities of escape or concealment, but includes fight only as an absolute last resort • The role of first responders in early casualty care • Requirements for rehearsals, drills and regular testing of emergency plans.

Syllabus

Element 4: Implementing protection procedures

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
- 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 protection measures

5.1 Scope of protection measures

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 protection measures to include:
  - Monitoring requirements
  - Controlling movement of people
  - Physical safety and security
  - Security of information
- Keep public protection measures under review.

Syllabus

Element 5: Implementing 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 tier, 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, dynamic barriers - Chemical, biological and radiological: air handling isolation, shelter-in-place protocols, liaison with emergency services - Cyber threats: business continuity plans, data protection, penetration testing.

Syllabus

Element 6: Documenting requirements	
6.1	**Scope of documenting requirements** • Protection procedures • Protection measures • Justification as to how those protection procedures and measures reduce the vulnerabilities and/or risk of harm if a terrorist attack were to occur • Keeping the documents up to date.
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 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) - Named responsible persons and review dates • The importance of regular reviews and the triggers for this. • Integration of measures into broader site risk registers or business continuity plans.

Syllabus

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.
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.

Syllabus

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.
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.