

Protect Duty Solution Product Documentation

About Protect Duty Solution



Protect Duty Solution is a technology firm that develops on-demand analytics for physical security threats, using big data and machine learning to assess terrorism risk.

Protect Duty Compliance and Audit Report (PDR) <#>

The Protect Duty Compliance and Audit Report (**PDR**) is an online risk assessment tool that combines national security expertise and best practices. Using real-time and historical data, it delivers a detailed, data-driven terrorism risk assessment in less than 30 minutes.

View the PDR production documentation [here#](#)

Getting Started<#>

View our guide on getting started with your account [here#](#)

About This Website<#>

This website contains the documentation for Protect Duty Solution's product, the Protect Duty Compliance and Audit Report (PDR). Here you will find guides and instructions on PDR

and its technology. If you have any further questions on PDR or the documentation presented here, please contact us at contact@protectdutysolution.com

Your User Account

Access to Protect Duty Solution requires an organisation account. Individual user accounts are then linked to this organisation account for each person accessing Protect Duty Solution.

Your Protect Duty Solution user account comprises of a username and a password. You should have received these as part of your onboarding.

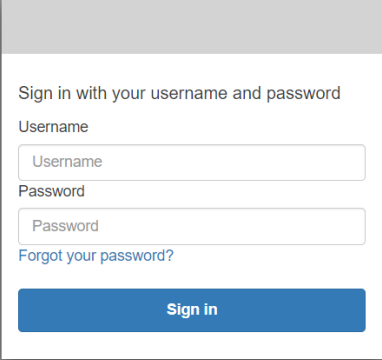
Setting Up Your Protect Duty Solution Account#

When your user account was created, you will have received an email with details about your account. This will have included your username and a temporary password. Once you have received this, go to the [Protect Duty Solution login portal](https://protectduty.live/login/) (<https://protectduty.live/login/>) and log in with the username and temporary password you were provided.

You will be asked to change your temporary password.

Logging into Your Protect Duty Solution Account#

To log into your account, go to the [Protect Duty Solution login portal](https://protectduty.live/login/) (link to <https://protectduty.live/login/>) and click on the "LOGIN" button.

A sign-in form with a light gray header, a title "Sign in with your username and password", fields for "Username" and "Password", a "Forgot your password?" link, and a blue "Sign in" button.

Sign in with your username and password

Username

Password

[Forgot your password?](#)

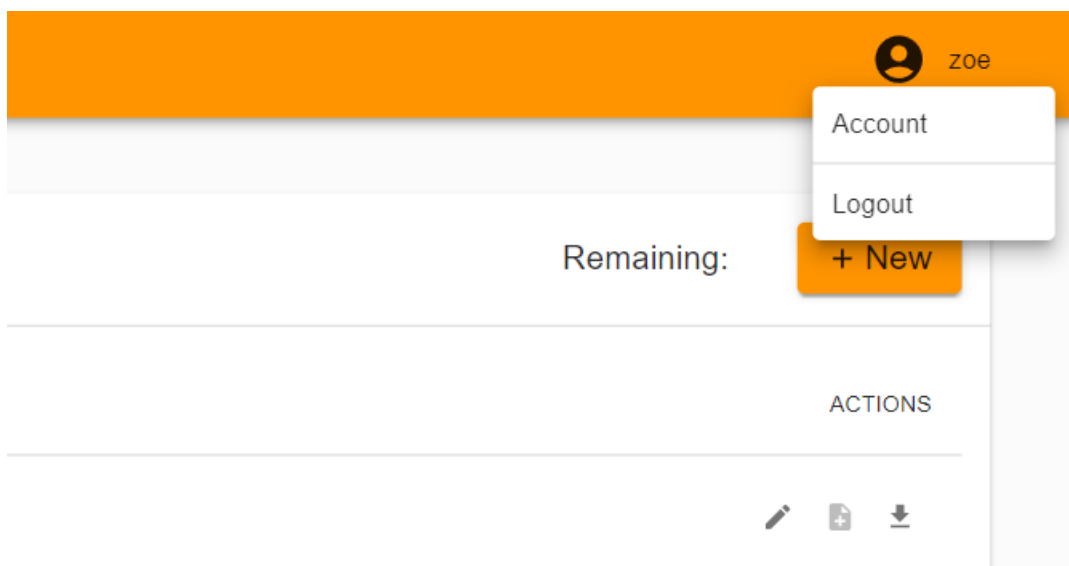
Sign in

Enter your username and password. If you have forgotten your password, click "Forgot your password?" and follow the instructions on the screen.

Once you have logged in successfully, you will be redirected to the Portal Homepage.

Logging Out of Your Account[#]

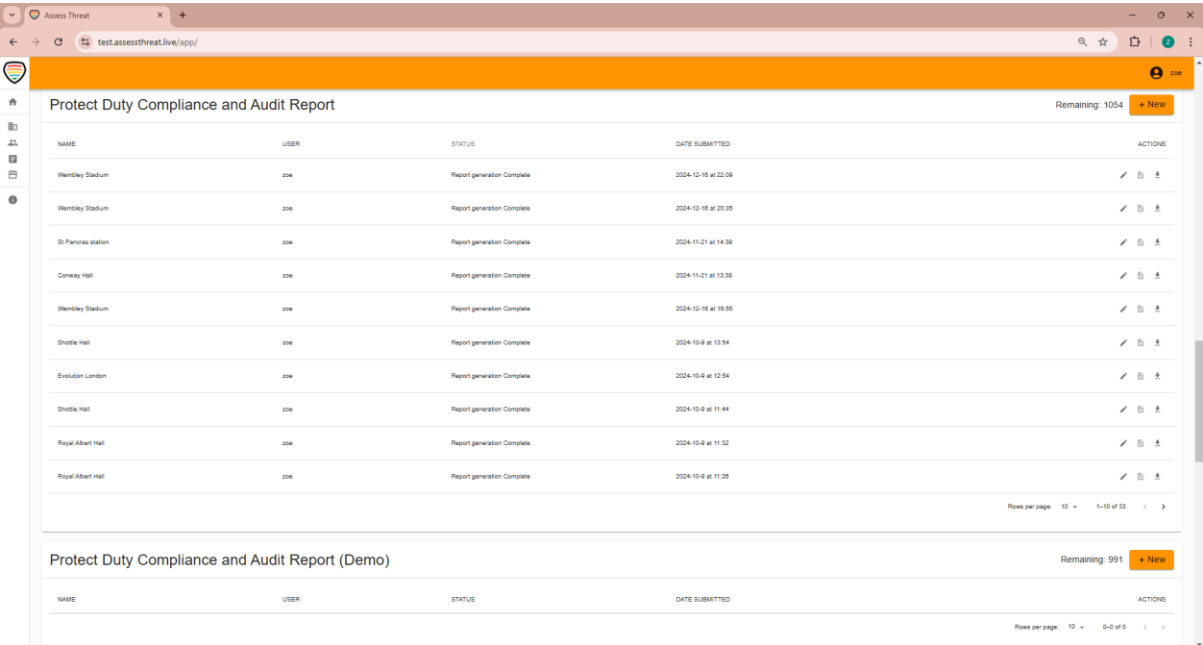
To log out of your account, click your username in the top right-hand corner of the browser and then click "Logout".



For more information on the Poral Homepage click [here](#)

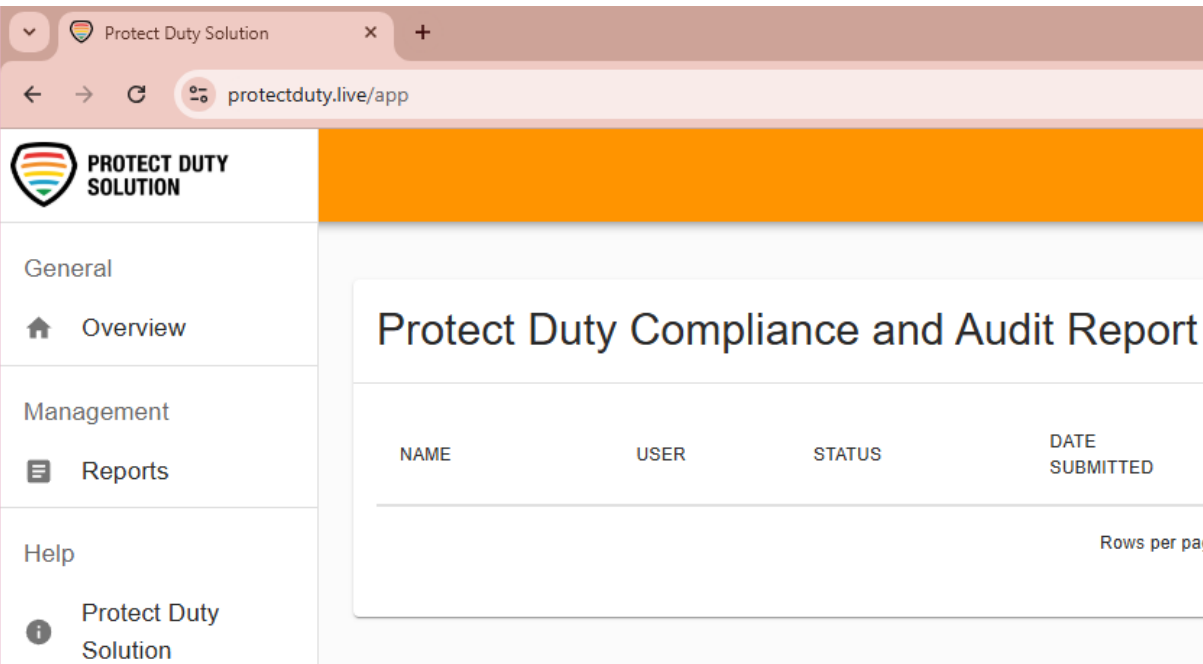
Portal Homepage

The Portal Homepage is where you can access your Protect Duty Compliance and Audit Report.

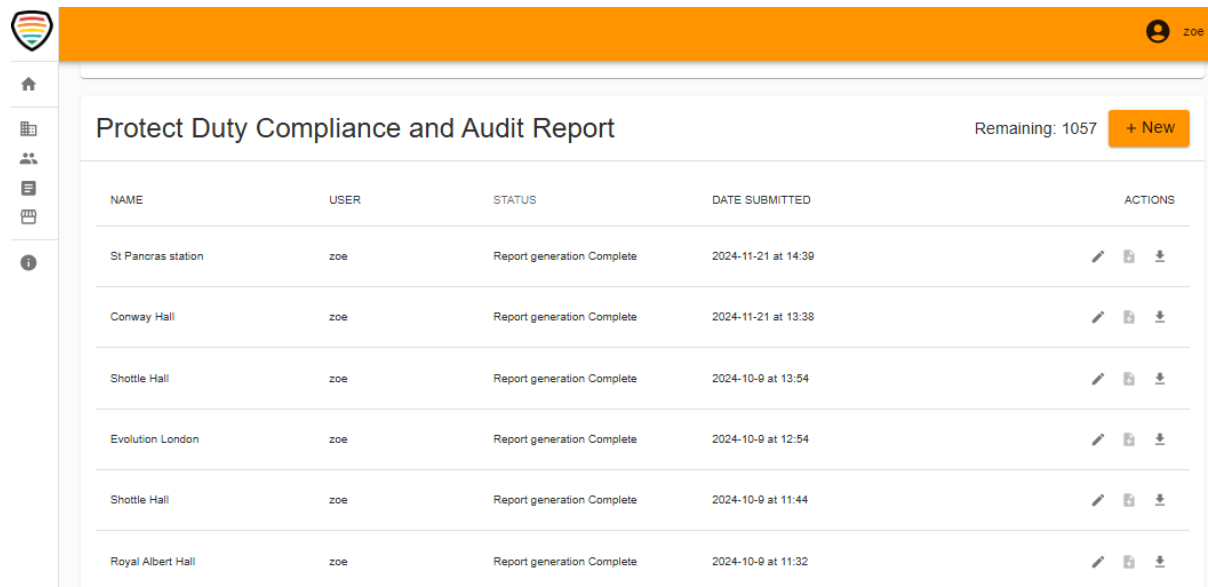




















At the top left-hand corner of the screen, you'll find a drop-down menu. Clicking the Protect Duty Solution logo at the top of the menu will expand it, making the text visible for each button. You can return to the Portal Homepage by clicking "Overview". You can use the "Reports" button to view all the assessments started and completed for each product. Additionally, under the "Help" section, clicking the "Protect Duty Solution" button will direct you to this User Guide.

Navigating the Portal Homepage#



On the Portal Homepage, you can manage and access past assessments and reports, start new assessments, generate and download new reports, and track your usage.

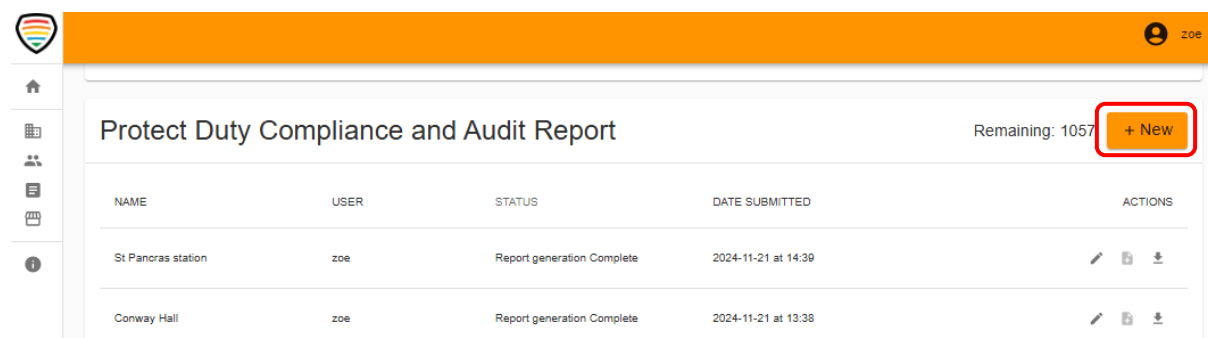








NAME	USER	STATUS	DATE SUBMITTED	ACTIONS
St Pancras station	zoe	Report generation Complete	2024-11-21 at 14:39	  
Conway Hall	zoe	Report generation Complete	2024-11-21 at 13:38	  
Shottle Hall	zoe	Report generation Complete	2024-10-9 at 13:54	  
Evolution London	zoe	Report generation Complete	2024-10-9 at 12:54	  
Shottle Hall	zoe	Report generation Complete	2024-10-9 at 11:44	  
Royal Albert Hall	zoe	Report generation Complete	2024-10-9 at 11:32	  

Under the Protect Duty Compliance and Audit Report (PDR) is a table which will list all the assessments that have been started or completed. The table provides details about each assessment, including its name, the user who conducted it, the submission date and time, and tools to edit the assessment, view analysis, and generate or download the report.

Starting a New Assessment

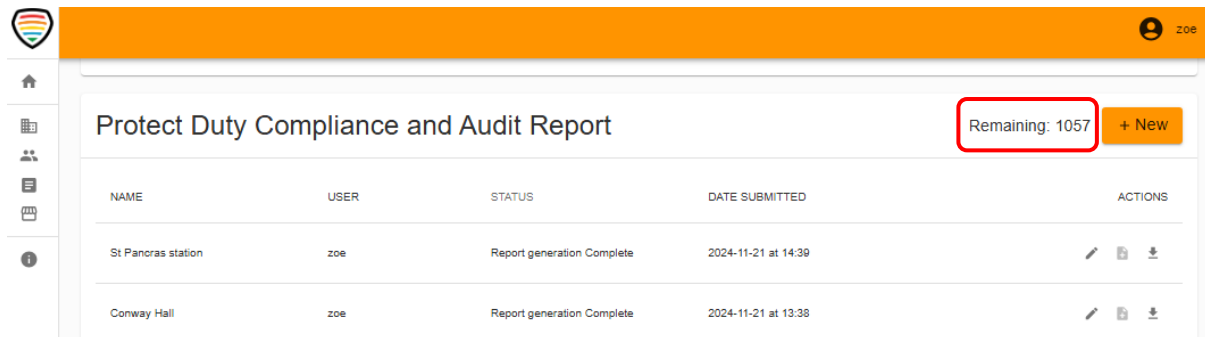
Clicking on “+ NEW” will create a new assessment. A new assessment starts as a blank form, allowing you to input information and either submit it immediately or save your progress and continue later.









NAME	USER	STATUS	DATE SUBMITTED	ACTIONS
St Pancras station	zoe	Report generation Complete	2024-11-21 at 14:39	  
Conway Hall	zoe	Report generation Complete	2024-11-21 at 13:38	  

Tracking Usage of the Product Duty Solution Product

In your Portal Homepage, you will find a "Remaining" counter. This number indicates the number of assessment licences you have remaining in your account for the PDR. This number decreases as assessments are submitted and completed by users in your organisation.

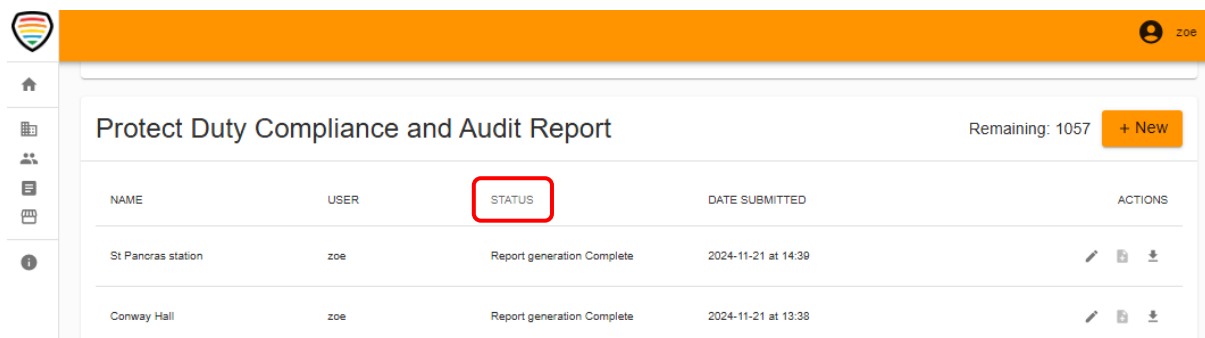


The screenshot shows the 'Protect Duty Compliance and Audit Report' page. The 'Remaining: 1057' counter is highlighted with a red box. The table below shows two completed assessments.







NAME	USER	STATUS	DATE SUBMITTED	ACTIONS
St Pancras station	zoe	Report generation Complete	2024-11-21 at 14:39	  
Conway Hall	zoe	Report generation Complete	2024-11-21 at 13:38	  

Assessment Status

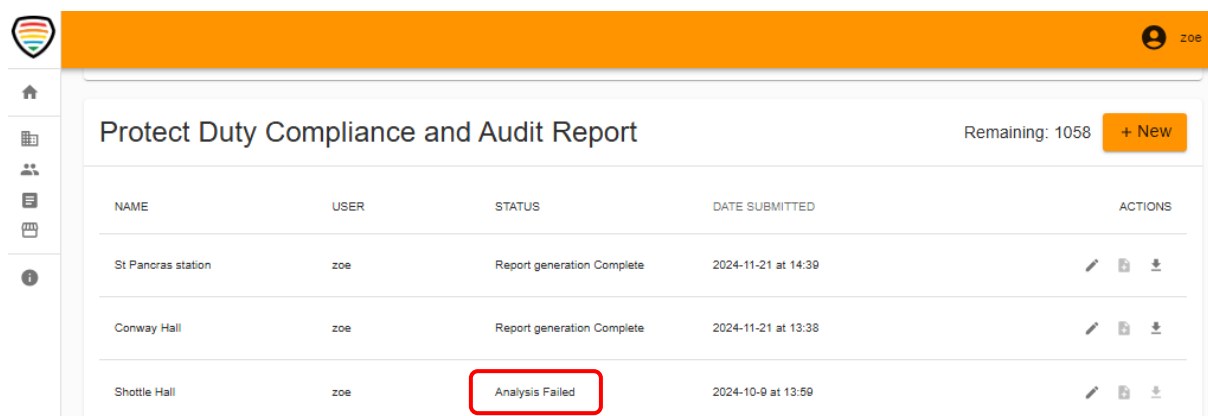
You can monitor the progress of assessments in the "STATUS" column of the table. When an assessment has been completed, the status will show as "Report generation Complete", while assessments that have been started but not submitted are displayed as "Analysis Started".












The screenshot shows the 'Protect Duty Compliance and Audit Report' page. The 'STATUS' column header is highlighted with a red box. The table below shows two completed assessments.

NAME	USER	STATUS	DATE SUBMITTED	ACTIONS
St Pancras station	zoe	Report generation Complete	2024-11-21 at 14:39	  
Conway Hall	zoe	Report generation Complete	2024-11-21 at 13:38	  

If there is an issue during a PDR analysis, a status of "Analysis Failed" will appear.



The screenshot shows the 'Protect Duty Compliance and Audit Report' page. The 'Analysis Failed' status for Shottle Hall is highlighted with a red box. The 'Remaining' counter is now 1058.

NAME	USER	STATUS	DATE SUBMITTED	ACTIONS
St Pancras station	zoe	Report generation Complete	2024-11-21 at 14:39	  
Conway Hall	zoe	Report generation Complete	2024-11-21 at 13:38	  
Shottle Hall	zoe	Analysis Failed	2024-10-9 at 13:59	  

For more information on why an analysis failed and recommended solutions click [here](#). (Link to PDR Troubleshooting page).

Assessment Actions


The tools listed under “ACTIONS” in the table of assessments allow you to modify assessments and generate reports. Actions that you can perform are highlighted in dark grey, while actions that are unavailable are displayed in light grey.

In the PDR portal, you can edit analyses of started and completed assessments, generate reports, and download reports for completed assessments.



Protect Duty Compliance and Audit Report

Remaining: 1057 + New

NAME	USER	STATUS	DATE SUBMITTED	ACTIONS
St Pancras station	zoe	Report generation Complete	2024-11-21 at 14:39	  
Conway Hall	zoe	Report generation Complete	2024-11-21 at 13:38	  

Editing an Analysis

Editing an analysis will reopen the assessment, allowing you to continue or make changes from the beginning of the assessment.



Protect Duty Compliance and Audit Report

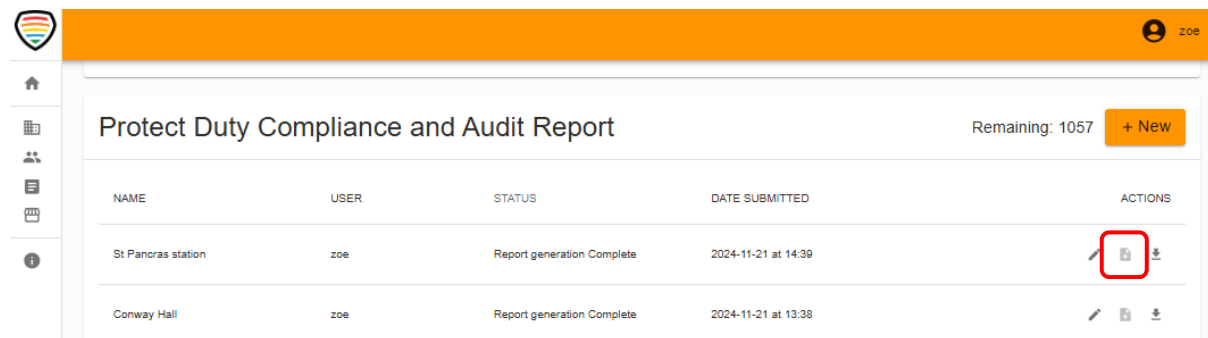
Remaining: 1057 + New

NAME	USER	STATUS	DATE SUBMITTED	ACTIONS
St Pancras station	zoe	Report generation Complete	2024-11-21 at 14:39	  
Conway Hall	zoe	Report generation Complete	2024-11-21 at 13:38	  







Please note: when you edit and save or edit and submit a previously submitted assessment, the system will create a new version. The original completed assessment stays unchanged in your Portal Homepage, and the new edited assessment is a copy with the original answers pre-filled. However, editing and saving an assessment that has not been submitted will not create a new version.

Regenerate Report

Regenerating a report allows you to create a new version of a report for a completed assessment. This process updates the report with the latest data or parameters, ensuring that it reflects the most current information available. However, it's important to note that this process may produce different results due to any changes that impact the generated score.

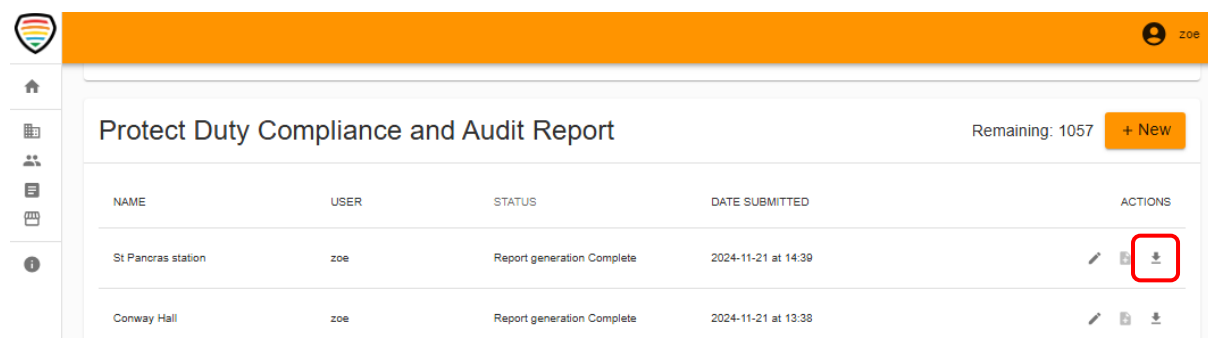


The screenshot shows a web application interface for 'Protect Duty Compliance and Audit Report'. The header is orange with a shield icon on the left and a user profile 'zoe' on the right. A sidebar on the left contains icons for home, reports, users, settings, and help. The main content area has a title 'Protect Duty Compliance and Audit Report' and a 'Remaining: 1057' indicator with a '+ New' button. Below this is a table with columns: NAME, USER, STATUS, DATE SUBMITTED, and ACTIONS. The table contains two rows: 'St Pancras station' and 'Conway Hall', both with 'zoe' as the user and 'Report generation Complete' as the status. The 'ACTIONS' column for 'St Pancras station' has three icons: a pencil, a document with a lock, and a download icon. The download icon is highlighted with a red box.







NAME	USER	STATUS	DATE SUBMITTED	ACTIONS
St Pancras station	zoe	Report generation Complete	2024-11-21 at 14:39	  
Conway Hall	zoe	Report generation Complete	2024-11-21 at 13:38	  

Downloading a Report

You can download the reports for completed assessments by clicking the "Download Report" button next to the assessment in the Portal Homepage. This action will automatically download a comprehensive PDF report to your device.



This screenshot is identical to the one above, showing the 'Protect Duty Compliance and Audit Report' interface. The 'Download' icon in the 'ACTIONS' column for 'St Pancras station' is highlighted with a red box.

NAME	USER	STATUS	DATE SUBMITTED	ACTIONS
St Pancras station	zoe	Report generation Complete	2024-11-21 at 14:39	  
Conway Hall	zoe	Report generation Complete	2024-11-21 at 13:38	  

Introduction to PDR

The Protect Duty Compliance and Audit Report is an automated terrorism risk assessment tool designed to align with the Terrorism (Protection of Premises) Bill. It is based on public protection procedures and measures informed by guidance from Protect UK, the '*Publicly Accessible Locations (PALs) Guidance*' (2022), and the National Protective Security Authority (NPSA). The tool enables users to conduct self-assessments of terrorism risks at premises, with results generated through an automated analysis system that integrates user responses with real-time, historical, and geospatial data to identify vulnerabilities and assess resilience.

PDR comprises of several components: a threat score, a resilience score, analysis based on the historical data and recommended public protection procedures and measures. This document provides additional information on how each of these components works, including the sources of data and information it uses and how it generates and calculates its results using formulas and algorithms.

This documentation is relevant for the standard version of PDR, that is, PDR without any additional customisation, adjustments or modifications specific to any use case, user, or organisation. It should be noted that this standard version of PDR represents one method for assessing terrorism risk in alignment with the Terrorism (Protection of Premises) Bill. However, it can be modified by individual users or organisations to meet their specific requirements.

Threat#

Threat is a measurement of the risk that a site will be targeted or attacked. PDR quantifies this risk in terms of whether a site possesses features and characteristics which make it an attractive target for an attack. The threat score is determined via an algorithm which has two components: a background risk component and a site-specific risk component. These components are comprised of various features outlined in more detail below. The background risk component is determined via analysis of trends in number and type of terrorist attacks occurring globally, regionally, within a given nation and within the immediate vicinity of a site. The site-specific risk component is determined by gathering information on the site and analysing its online profile, its function and industry type, and the nature of where it is located.

WARNING

The method used to calculate the threat score in the standard version of PDR should be treated as a general approach which has been developed and optimised to work with the broadest range of sites around the world as possible. Individual users and organisations may have their own risk scoring methodology or may be required to adhere to more local and specific risk scoring methodologies. Adjustments or customisation of the standard PDR scoring method may be required to align PDR with these methodologies.

Background risk score#

The background risk score is calculated using historical data of past terrorist attacks. The purpose of this score is to contextualise the risk exposure of a site based on its location and by looking at historical trends, taking into account the proportion of global terrorist attacks which have occurred within the region, the number of terrorist attacks in the region which have occurred within the country, and the number of terrorist attacks in the country which have occurred within a 10km radius.

Site score#

The site risk score is based on the number of online results returned for the reference name provided in the assessment. This is determined using open-source data, web-scraping and search engines which provide a count of the number of references made to the search terms provided in the assessment on websites, online media sources and so on.

Resilience#

Resilience is defined as the ability for a site to recover from an incident or attack. PDR uses threat and resilience as its primary metrics for assessing terrorism risk. This differs from other methods to assess terrorism risk which typically use a combination of threat and vulnerability.

Vulnerability is defined as the probability that damage occurs to a site, given a particular threat. The decision to move from vulnerability to resilience was based on the difficulty of quantifying vulnerability given that it can only be calculated in relation to a specific threat i.e. vulnerability to an IED attack, vulnerability to a vehicle attack, vulnerability to a drone attack and so on. As the nature of the threat, and more specifically, the types of attacks, weapons and methods used by terrorists change and are often unknown, this makes vulnerability a less stable basis for assessment, planning and decision making in relation to terrorism risk. In contrast, the primary reference point for the assessment of resilience is on the ability for a site to return to a particular state, that is, the pre-incident or pre-attack state. As the pre-incident or pre-attack state of a system or a site is a known value, it provides a more stable basis for assessment, planning and decision making in relation to terrorism risk.

Every question related to the security measures in place are assigned to one of these seven categories. A user's answer to a question is converted into one of two response types: a positive or a negative response. A positive answer means that the answer reflects a positive impact on the risk of the site, that is, it decreases its vulnerability or risk exposure. A negative answer means that an answer reflects a negative impact on the risk of the site, that is, it increases its vulnerability or risk exposure. This conversion is necessary as there are instances where an answer to a question, such as "yes", will be considered positive (e.g. "Do you have CCTV cameras in place") and other instances where it will be considered negative (e.g. "Is the site exposed to vehicle traffic").

The resilience score comprises of seven categories: planning, deterrence, detection, prevention, protection, response, and recovery.

Planning#

The planning capability of a site measures the extent of which terrorism risk management has been embedded into systems, processes and procedures, and forms a critical part of the overall preparedness of a site to deal with a terrorism incident or scenario. Comprehensive and detailed planning indicates that a site has taken time to consider the threats and risks presented by terrorism and set out a structured way in which these threats and risks can be dealt with in an effective and proportionate manner. Sites with poor planning capability will tend to perform poorly across other capability areas, or poorly manage their other capability areas and compromise their effectiveness in these areas.

Deterrence#

Deterrence is defined as the attributes which discourage a certain action before that action is taken, such as discouraging an attacker from attempting to attack or target a site. Deterrence is created by projecting the defensive capability of a site in a manner that is highly visible or would be noticed by a potential attacker, and thereby presenting the site as difficult or risky to attack successfully.

Deterrence can be facilitated through signage indicating that there are security measures in place, use of highly visible access controls such as bollards or barriers in public areas, having a highly visible security guard presence, or how the site is generally laid out. A site may be a prominent or high-profile target, but if it has strong deterrence capability, it dissuades a potential attacker by making it known that it is well secured and that any attack would be risky for the attacker.

Sites with poor deterrence capability may have effective security controls and measures in place, but without projecting the presence of these measures to outsiders and potential attackers, it may not exert a deterrent effect which would dissuade an attacker from attempting to attack the site.

Detection#

The detection capability of a site specifically relates to how well and quickly a site would be able to detect an unauthorised intruder or attacker within the site grounds, or otherwise detect any suspicious activity, items or objects. Detection covers measures and controls such as CCTV surveillance, as well as searches and inspections of the site area and of persons and vehicles entering the site. Sites with strong detection capability are able to quickly detect possible signs or indications of an incoming threat, such as an attacker conducting pre-attack planning or placing weapons or explosive devices within a site for an attack. This allows for faster response time and interception of threats before they can materialise into an actual attack or harm. Sites with poor detection capability lack the ability to quickly detect and react to potential threats, which may result in some threats which could have been stopped or intercepted developing into actual attacks or harm.

Prevention#

The prevention capability of a site relates to its ability to prevent an attacker or intruder from entering or accessing the site or reaching within the required range of their target to undertake an attack. This encompasses both measures to prevent persons or vehicles from physically entering a site or areas within a site, as well as non-physical measures such as software to prevent an attacker from gaining access to systems, data or information stored or used by the site. Sites with strong prevention capability are able to secure and control access into and out of their site and prevent an intruder or attacker from easily reaching possible targets such as people, property or information.

The stronger the prevention capability, the harder or longer it would take for an attacker to enter or reach within range of their target within the site, thereby diminishing the velocity of any potential attack. Sites with weak prevention capability allow an attacker to more easily and quickly access and engage their targets, which in turn increases the potential harm and damage they are able to inflict.

Protection#

The protection capability of a site measures how well a site can remove persons, property or information away from harm once an attack has started and can involve procedures to place people in protected and sheltered areas such as safe rooms, or reinforcement of existing structures to provide more protection against attacks such as explosives. The key elements of

protective capability are to remove targets from attacking range, and thereby delay or disrupt the velocity of an attack.

Sites with strong protective capabilities minimise the potential harm that an attacker can cause, thereby diminishing the effectiveness of an attack. Sites with poor protective capability provide an attacker with substantial control over the direction and velocity of their attack, allowing an attacker to maximise the harm or damage they can cause or achieve their desired objective.

Response#

The response capability of a site measures how well a site can respond to an attack and either eliminate or render an attacker ineffective. Response capability typically focusses on measures or procedures which could be considered counter-offensive, such as having armed guards or police on site who can respond to an attack using force. It also includes measures which suppress or mitigate the impacts of an attack, such as fire suppression systems, and emergency response plans and procedures which are activated once an attack is taking place.

Sites with strong response capability are able to counteract an attacker to stop or diminish the direction and velocity of an attack, thereby bringing it to an end quicker. Attacks which have weak response capability provide an attacker with substantial control over the direction and velocity of their attack, allowing an attacker to maximise the harm or damage they can cause or achieve their desired objective.


Recovery#






The recovery capability of a site measures how quickly a site can recover after an attack or incident has ended, including its ability to control and mitigate any ongoing impacts or harm that may stem from an attack or incident. This can include areas such as resumption of business operations, repairs to damaged property or sites, participation in investigation procedures, helping staff who may have been harmed in the attack, as well as managing potential impacts to non-tangible areas such as reputation and public perception. Sites with strong recovery capability are able to quickly return to normal operations after an attack has occurred and enhance their survivability to an attack. Sites with poor recovery capability may experience a delayed and costly recovery period and may possibly not be able to survive due to ineffective management of the impacts and costs inflicted by the attack.

Entering Site Information

To start a PDR assessment, click "+ NEW" in the PDR portal on the Protect Duty Solution Portal Homepage. This will open the PDR assessment in the same window.

The first page will contain some basic instructions. Check "Confirm" and then click "NEXT" to proceed.





Start

About the Assessor

Asset Details

Responsible Party

Associations and Connections

Prominence and Profile

Events

Basic Security Layout

Plans, Policies and Procedures

Physical Security

Access Controls

Perimeter Security

Hostile Vehicle Mitigation

CCTV

Improvised Explosive Devices Blast Mitigation

Hostile Reconnaissance Detection

Information Security

Personnel Security

Start

Instructions

Confirmation

You will now be guided through a series of questions. Please ensure that you read each question carefully before answering. If you are unsure of how to answer a question, please contact us at support@vardogyr.com. You can also save your progress at any time by pressing the "save" button on the top right. Be sure to keep the unique URL link somewhere safe so you can reload your progress at a later time. Version 20190825.

I have read and understood the instructions for this assessment. I understand that not correctly following the assessment instructions may result in lower accuracy results.

☒ Confirm

SAVE

NEXT →

You will then be asked to provide your name as you will be identified as the Assessor in both the PDR report and the email notification.

Start

About the Assessor

Asset Details

Responsible Party

Associations and Connections

Prominence and Profile

Events

Basic Security Layout

Plans, Policies and Procedures

Physical Security

Access Controls

Perimeter Security

Hostile Vehicle Mitigation

CCTV

Improvised Explosive Devices Blast Mitigation

Hostile Reconnaissance Detection

Information Security

Personnel Security

About the Assessor

What is your name?

You will be identified as the assessor for this report in both in the report document and the email notification.

SAVE

← BACK

NEXT →

The next part of PDR is entering in site information which will be used in the threat analysis. We will go through how to properly answer and configure each question.

Reference name#

The reference name serves two purposes. Firstly, it will be the name used to reference the report and will be included as the name of the report in any emails and reports generated. More importantly however, it also sets the terms that will be used in the online search for reference to the site. As such, it is important that you provide an accurate name that reflects the most common or likely reference to the site.

Provide a reference name for the asset being assessed

IMPORTANT: please provide the most common name or most widely recognised name for the asset. In addition to the geographical location of the asset, this name will be used to collect data about the asset which will be used in the calculation of the threat score.

Wembley Stadium

You can add multiple terms to the online search by using "#" in front of each term that you want to include. For example, your site name may be "Wembley Stadium" but you want the search to also include "FA Cup Final 2025". To do this, insert "#Wembley Stadium #FA Cup Final 2025" into the reference name.

Provide a reference name for the asset being assessed

IMPORTANT: please provide the most common name or most widely recognised name for the asset. In addition to the geographical location of the asset, this name will be used to collect data about the asset which will be used in the calculation of the threat score.

#Wembley Stadium #FA Cup Final 2025

WARNING

Avoid configuring the reference name in the following ways:

1. Using the full address of the site e.g. " Wembley HA9 0WS, United Kingdom"

2. Adding in additional information to the name of the site e.g. "Wembley Stadium, near Wembley Park Station, London HA9 0WS."

Doing so may result in a more restrictive search being performed, resulting in underscoring of the site score component of the threat score.

Site Location#

Using the interactive map, place a marker on the location of the site being assessed. You can also use the search bar on the left-hand side to search for an address.



If the site is a building or spread across a large area, place the marker in the approximate centre of the site.

CAUTION

We are aware of a bug which causes the marker to be placed on the map when the search bar is clicked.

Additional Site Information#

The following questions cover additional information about the site including its industry classification, total area, total insurable value and a description of the site.

Industry#

Select the industry classification that best matches the industry or function of the site being assessed, or the owner/operator of the site.

Please select an industry classification for the asset

Select the industry classification that best matches the industry or function of the asset being assessed.

- ☐ Accommodation and Food Services
- ☐ Administrative and Support and Waste Management and Remediation Services
- ☐ Agriculture, Forestry, Fishing and Hunting
- ☒ Arts, Entertainment, and Recreation
- ☐ Construction
- ☐ Educational Services
- ☐ Finance and Insurance
- ☐ Health Care and Social Assistance
- ☐ Information
- ☐ Management of Companies and Enterprises
- ☐ Manufacturing
- ☐ Mining, Quarrying, and Oil and Gas Extraction
- ☐ Other Services (except Public Administration)
- ☐ Professional, Scientific, and Technical Services
- ☐ Public Administration
- ☐ Retail Trade
- ☐ Real Estate and Rental and Leasing
- ☐ Transportation and Warehousing
- ☐ Utilities
- ☐ Wholesale Trade

Total area#

Provide the total area of the site, if available. This question is optional, so if you do not have this information on hand, enter "0".

Total Insurable Value#

Total Insurable Value (TIV) is the value of property, inventory, equipment, and business income covered in an insurance policy. It is the maximum dollar amount that an insurance company will pay out if an asset that it has insured is deemed a constructive or actual total loss.

Provide the Total Insurable Value of the site, if available. This question is optional, so if you do not have this information on hand, enter "0".

Responsible Party and Assessment Date

On the fourth page of the assessment, you will be asked to name the responsible party or organisation for the safety and security at the asset as well as the person responsible for reviewing the assessment.

Start

About the Assessor

Asset Details

Responsible Party

Associations and Connections

Prominence and Profile

Events

Basic Security Layout

Plans, Policies and Procedures

Physical Security

Access Controls

Perimeter Security

Hostile Vehicle Mitigation

CCTV

Improvised Explosive Devices Blast Mitigation

Hostile Reconnaissance Detection

Information Security

Personnel Security

Responsible Party

What is the name of the party or organisation responsible for safety and security at the asset?

What is the name of the person who will be responsible for reviewing the assessment?

The email containing the report will be addressed to this person.

When does the assessment period start?

When does the assessment period end?

SAVE

← BACK

NEXT →

You will also be asked to select the start and end dates for the assessment period from a drop-down calendar.

When does the assessment period start?

<

April 2024

>

Su	Mo	Tu	We	Th	Fr	Sa
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27

When does the assessment period end?

Completing the PDR assessment

Once you have entered in all the site information, you will now start answering the PDR questions. The PDR questions are a series of questions covering different aspects of the site being assessed in a "Yes/No" format.

The screenshot shows a web-based assessment form. On the left is a sidebar with a list of sections: Start, About the Assessor, Asset Details, Responsible Party, Associations and Connections (highlighted), Prominence and Profile, Events, Basic Security Layout, Plans, Policies and Procedures, Physical Security, Access Controls, Perimeter Security, Hostile Vehicle Mitigation, CCTV, Improvised Explosive Devices Blast Mitigation, Hostile Reconnaissance Detection, Information Security, and Personnel Security. Below the list is an orange 'SAVE' button. The main content area is titled 'Associations and Connections' and contains three questions, each with a 'Yes' or 'No' radio button option. The first question is 'Does the asset possess any of the following connections to government?' with a 'No' option selected. The second question is 'Does the asset possess any of the following connections to military?' with a 'Yes' option selected. The third question is 'Does the asset possess any of the following connections to police?' with a 'No' option selected. At the bottom of the form are 'BACK' and 'NEXT' buttons.

Associations and Connections

Does the asset possess any of the following connections to government?
The asset is, or contains, a government office or houses a government agency within its perimeter; The asset performs a government role; The asset is commonly associated with government

☐ Yes
☒ No

Does the asset possess any of the following connections to military?
The asset is, or contains, a military base or site, such as a recruiting office; The asset has military personnel present; The asset is associated with the military, such as a military monument or event

☒ Yes
☐ No

Does the asset possess any of the following connections to police?
The asset is a police station or contains a police station; The asset is associated with police or law enforcement, such as a court or other law enforcement body

☐ Yes
☒ No

Does the asset possess any of the following connections to religion?
The area is, or contains, a place of worship; It is commonly used for a religious purpose or associated with a particular religion; Used by persons of a particular religion on a frequent basis

☐ Yes
☒ No

← BACK

NEXT →

Answering the Questions#

Read the question carefully, and then select the appropriate answer. PDR was designed with simple "Yes/No" questions to make the process of answering each question clearer and less ambiguous when compared to questions which may involve multiple choices. If you have any questions or are uncertain about how to answer a question, contact us at contact@protectduty.com

This is a close-up of the 'Associations and Connections' section. The question 'Does the asset possess any of the following connections to government?' is shown. The 'Yes' radio button is selected, while the 'No' option is unselected.

Associations and Connections

Does the asset possess any of the following connections to government?
The asset is, or contains, a government office or houses a government agency within its perimeter; The asset performs a government role; The asset is commonly associated with government

☒ Yes
☐ No

As you complete these questions, your answer will influence whether further questions will need to be answered, or whether certain questions will be removed when not relevant. For example, when you answer "Yes" to the question "Is there an event taking place at the asset during the assessment period?", additional questions about the event will be revealed.

Start

About the Assessor

Asset Details

Responsible Party

Associations and Connections

Prominence and Profile

Events

Basic Security Layout

Plans, Policies and Procedures

Physical Security

Access Controls

Perimeter Security

Hostile Vehicle Mitigation

CCTV

Improvised Explosive Devices Blast Mitigation

Hostile Reconnaissance Detection

Information Security

Personnel Security

Events

Is there an event taking place at the asset during the assessment period?
An event is defined as a planned gathering of people for a specific purpose or occasion.

☒ Yes

☐ No

Is the event a moving event that takes place over an extended route such as a fun run, parade or similar?
For example, a marathon or parade taking place over an extended area or road.

☐ Yes

☐ No

☒ Not Applicable

Will there be more than 1,000 people in attendance at the event?
Generally an event with greater than 1,000 people will be considered a mass gathering event.

☐ Yes

☐ No

☐ Not Applicable

How many people are/will be present at the event?
Put 0 if you are unsure or not applicable

SAVE

← BACK

NEXT →

Saving your Progress#

You can save your current progress on answering the questions at any time by pressing the “SAVE” button on the left-hand side of the screen below the assessment topics.

Start
About the Assessor
Asset Details
Responsible Party
Associations and Connections
Prominence and Profile
Events
Basic Security Layout
Plans, Policies and Procedures
Physical Security
Access Controls
Perimeter Security
Hostile Vehicle Mitigation
CCTV
Improvised Explosive Devices Blast Mitigation
Hostile Reconnaissance Detection
Information Security
Personnel Security

SAVE

When you click “SAVE”, you will be automatically directed back to the Portal Homepage. To resume an assessment, click the “Edit Analysis” button next to the assessment you want to resume.

Protect Duty Compliance and Audit Report				Remaining: 949	+ New
NAME	USER	STATUS	DATE SUBMITTED	ACTIONS	
Wembley Stadium	zoe	Analysis Started	Not submitted	<div> <div></div> <div></div> <div></div> </div>	Edit analysis

Name and Contact Selection#

Once you have reached the end of the assessment and all of the PDR questions have been answered, you will need to select two email contacts: your email contact and an email contact for the person who will be reviewing the report. Note that if you are both the person completing the assessment and reviewing the report, select your name from the list provided. The email contacts provided are those from your organisation.

The screenshot shows a two-step form for providing email contacts. The first step is titled "Please provide an email contact for the person who will be reviewing this report" with a sub-note "A copy of the report will be sent to this user." It contains four radio button options, each with a redacted email address, and a selected option labeled "zoe". The second step is titled "Please provide your email contact" with the same sub-note. It also contains four radio button options with redacted email addresses and a selected option labeled "zoe". At the bottom, there are "BACK" and "NEXT" buttons.

Submitting the Assessment[#]

The final page will look like this. Click "SUBMIT" to submit your assessment.

The screenshot shows the final submission page. It has a heading "Review and submit your answers" and a paragraph: "Please review your answers and then click submit once you have confirmed that all answers are correct. Your answers have also been automatically saved at this stage, so please keep the URL of this form in a safe place if you wish to access it at a later time." Below this, it says "All steps completed". At the bottom is a large orange button labeled "SUBMIT".

After you submit, you will be directed back to the Portal Homepage where your report will automatically begin generating and where you will be able to access and download the PDR.

Guide to the Report

WARNING

Information which is deemed to be confidential and available only to current users will be marked as "*See official product guide*".

Receiving your PDR[#]

You will receive a link to your PDR via email. The email will contain a link where you can open and download the report. The email will look like this:

Protect Duty Compliance and Audit Report for Wembley Stadium - Mon, 16 Dec 2024 05:55:30 GMT

NR

no-reply@assesstheat.com

To: Zoe

☺

↩ Reply

↩ Reply All

➡ Forward


📧

⋮

Mon 16/12/2024 4:59 PM

Dear customer,

You are receiving this email as you have been identified as the party responsible for reviewing the results of this Protect Duty Compliance and Audit Report report completed on Mon, 16 Dec 2024 05:55:30 GMT.

The analytics and detailed information of the assessment generated in the report can be viewed/downloaded from the dashboard: 

Click on the link (redacted in the image above) to open the report.

A photograph of a busy London street, likely Piccadilly, during the 'golden hour' of sunset. The scene is filled with pedestrians walking across the street, and several red double-decker buses are visible in the background. The architecture consists of grand, classical-style buildings with many windows. Street lamps are illuminated, and the overall atmosphere is warm and vibrant due to the low sun.

Protect Duty Compliance and
Audit Report
Wembley Stadium


Completed by Zoe on 2024-12-16 05:55:30.462041

Structure of the Report#

There are three parts to the PDR report: Part A: Key Findings, Part B: Full Results and Appendix.

- **Part A: Key Findings** contains an executive summary of the PDR analysis results, key highlights for each of the risk and resilience scores, proposed risk improvement measures, and a register of proposed measures.
- **Part B: Full Results** contains more comprehensive information regarding each of the scores, national and local historical attack details, relevant industry historical attack details, a record of all questions and answers, and risk improvement actions.
- **Appendix** contains additional information about the report and how to understand and interpret the results, as well as global threat levels and a terrorism threat briefing.

Contents	
Part A - Key Findings	3
Assessment Details	4
Executive Summary	5
Risk Scores	5
Resilience Scores	5
Risk Improvement Actions	5
Key Highlights	6
Threat Score	6
Asset Specific Risk Score	6
Location next to high-risk assets	6
Background Risk Score	7
Resilience Analysis	7
Risk Improvement Actions	8
Risk Action Plans	9
Critical Actions	9
Recommended Actions	12
Best Practice Actions	17
Part B - Full Results	18
Threat Score	19
Asset Specific Risk Score	20
Location next to high-risk assets	21
Background Risk Score	31
Total attacks on Arts, Entertainment, and Recreation assets around the world, 2001 to 2020	32
Total attacks in Australia, 2001 to 2020	33
Resilience Analysis	35
Risk Improvement Actions	36
Risk Improvement Actions by Priority Level	36
Risk Improvement Actions by Capability	37
Appendix	65
About the Tera Scoring Algorithm	66
Global Threat Levels	67
Australia: National Terrorism Alert Level	67
Canada: National Terrorism Threat Level	67
United Kingdom: Terrorism Threat Level	67
United States: Homeland Threat Assessment	67
Terrorism Threat Briefing	68
Overview	68
Terrorist Tactics and Weapons	68
Terrorist Targeting	69
Disclaimer	70
Handling Instructions	71

 This is an automated report powered by Assess Threat

2

Part A: Key Findings, Risk Scores and Resilience Analysis#

Assessment Details#

The assessment details are presented in a table which summarises all the high-level details of the assessment. This includes the date the assessment was completed, the assessor, terms used in the analysis query, and a map of the site being assessed.

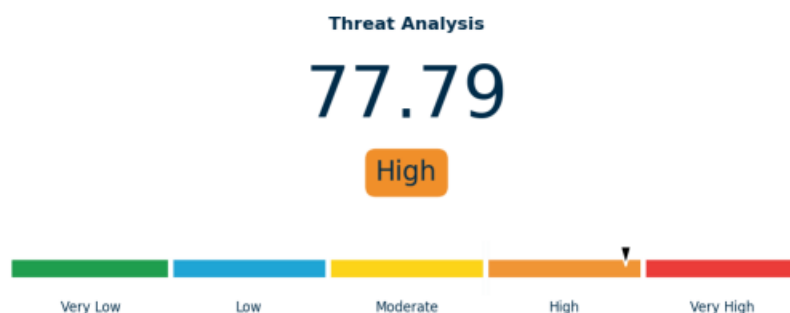
Date of Assessment	2024-12-16 11:09:45.994266
Assessor	Zoe
Reviewer	Zoe
Responsible Party	Private
Name of Premises/Event	Wembley Stadium
Type of Premises/Event	Arts, Entertainment, and Recreation
Latitude/Longitude	51.5558394021597/-0.27948452356605813
Description	Wembley Stadium is a world-renowned sports and entertainment venue located in Wembley, London. It serves as the home of English football and hosts major events, including international matches, domestic cup finals, concerts, and large-scale entertainment events.
Analysis Query	Wembley Stadium, London, England, United Kingdom
Threat Score	62.21
Number of Proposed Measures	20

Threat Score#

Threat is a measurement of the risk that a site will be targeted or attacked. PDR quantifies this risk in terms of whether a site possesses features and characteristics which make it an attractive target for an attack. The threat score is determined via an algorithm which has two components: a background risk component and a site-specific risk component. These components are comprised of various features outlined in more detail below. The background risk component is determined via analysis of trends in number and type of terrorist attacks occurring globally, regionally, nationally, and within the immediate vicinity of the site. The site-specific risk component is determined by gathering information on the site and analysing its online profile, its function and industry type, and the nature of where it is located.

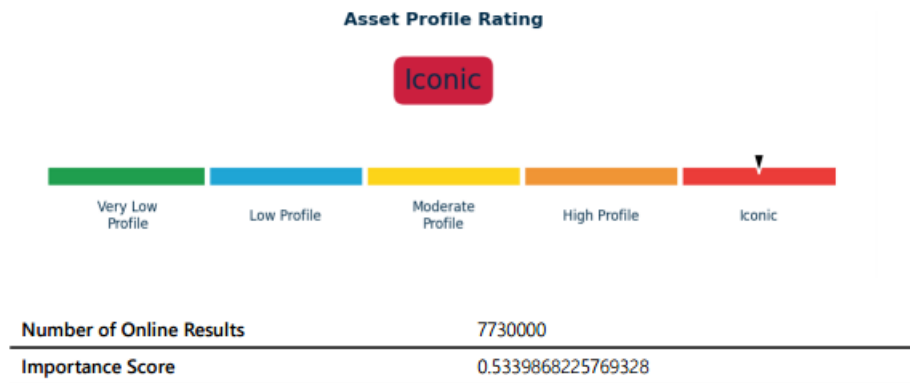
Criteria	Rating	Description
Less than 20	Very Low	This indicates that the site possesses few or no notable features and attributes which make it an attractive target for a terrorist attack. Based on this analysis, the site falls

Criteria	Rating	Description
Between 20 and 40	Low	<p>well below the threat threshold set by PDR through its analysis of past attacks and incidents, and the risk that the site will be targeted or attacked is rated as very low. This indicates that the site possesses some minor features and attributes which make it an attractive target for a terrorist attack. Based on this analysis, the site falls below the threat threshold set by PDR through its analysis of past attacks and incidents, and it is unlikely to be targeted or attacked unless there is a significant change in the current threat environment or choice of targets.</p>
Between 40 and 60	Moderate	<p>This indicates that the site possesses some features and attributes which make it an attractive target for a terrorist attack, but these features and attributes are not sufficient for the analysis to conclude that the site should be classified as high or very high risk. For this reason, the site still falls under the threat threshold set by PDR through its analysis of past attacks and incidents. However, changes in the threat environment or choice of targets in the immediate future may increase the threat score for the site beyond the threat threshold. As such, the site should be vigilant to the threat environment and be prepared for a sudden increase in current security measures, controls and procedures.</p>
Between 60 and 80	High	<p>This indicates that the site falls above the threat threshold set by PDR because it possesses notable features and attributes which make it an attractive target. It is also likely that the site will remain an attractive target for terrorist groups unless there is a noticeable change in the threat environment or choice of targets in the immediate future. Due to its high threat rating, it is recommended that the asset urgently review its current security measures, controls and procedures to ensure that they are effective and up to date, as well as ensuring that any gaps and vulnerabilities are immediately addressed.</p>
Greater than 80	Very High	<p>This indicates that the site falls well above the threat threshold set by PDR through its analysis of past attacks and incidents. At this level, the site possesses a combination of notable features and attributes which make it a very attractive target. Due to its level of prominence, it is likely that the site will remain an attractive target into the foreseeable future. Due to its high threat rating, it is recommended that the asset urgently review its current security measures, controls and procedures to ensure that they are effective and up to date, as well as ensuring that any gaps and vulnerabilities are immediately addressed.</p>



Site Score#

The site risk score is based on the number of online results returned for the reference name provided in the assessment. This is determined using web-scraping and search engines which provide a count of the number of references made to a site online on different websites and online sources.

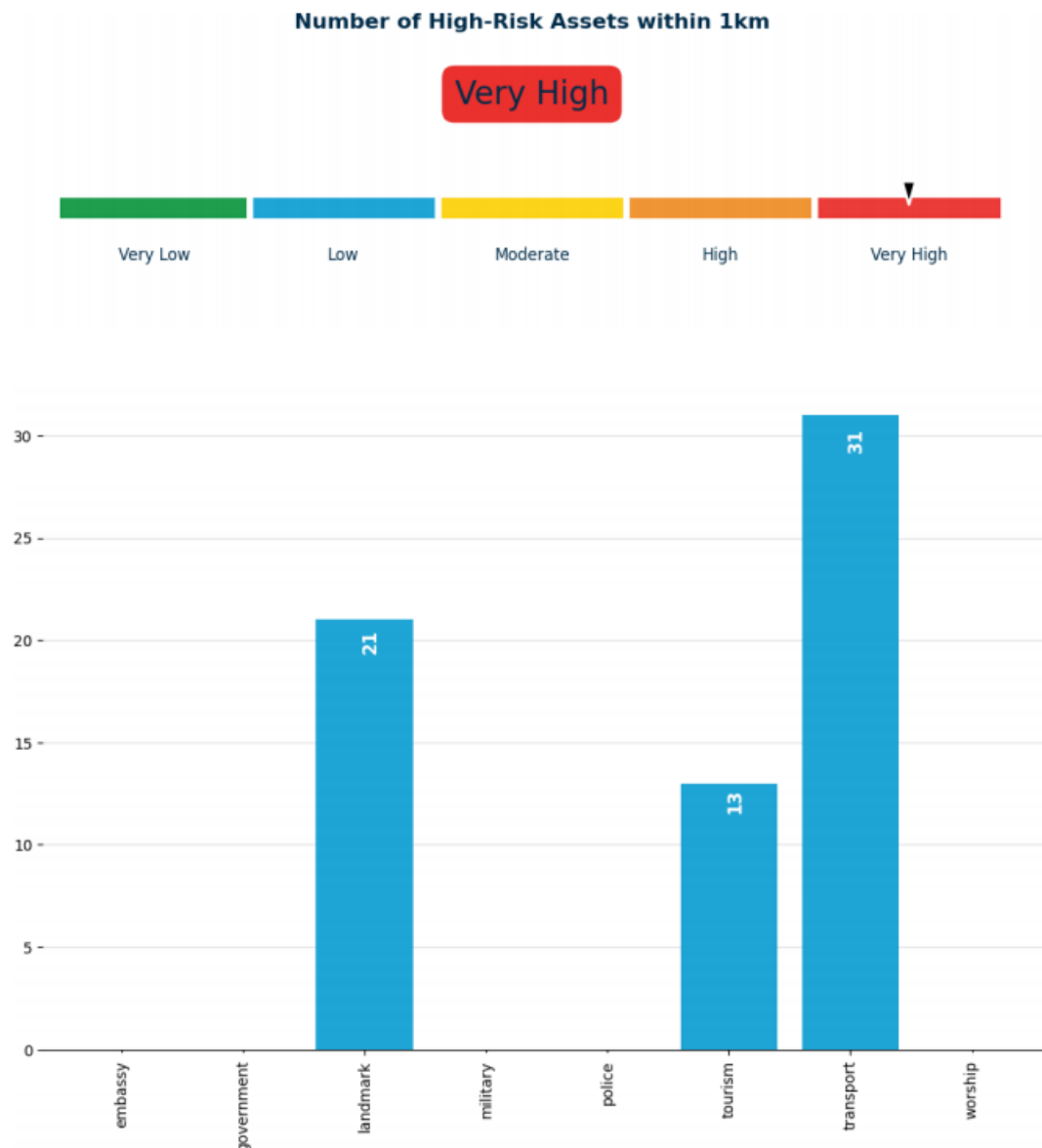


The following criteria is applied to generate a qualitative rating based on the quantitative score.

Criteria	Rating	Description
<i>See official product guide</i>	Very Low Profile	The site has a very low profile suggesting that its location, function or connections are unknown except for those who directly interact with it or live within the immediate local area.
<i>See official product guide</i>	Low Profile	The site has a low profile suggesting that its location, function or connections are well known to those in the local area.
<i>See official product guide</i>	Medium Profile	The site has a medium profile suggesting that it would be well known at a local or state level, but it would not be well known at a national level or beyond.
<i>See official product guide</i>	High Profile	The site has a high profile suggesting that it would be very well known within the country it is located and may be recognised internationally.
<i>See official product guide</i>	Iconic	The site has a very high profile suggesting that it would be considered internationally iconic, with its location, function or connections with a particular country or group internationally recognised or known.

High-Risk Sites in Surrounding Area#

Based on the location of the site indicated during the assessment, a search of the surrounding area is performed to identify what are deemed "high-risk sites". These are sites which, based on historical data, have been frequent or popular targets of terrorist groups and include places identified as government buildings, military sites, police stations, public transport, tourist attractions, embassies, places of worship and landmarks.



Background Risk Score#

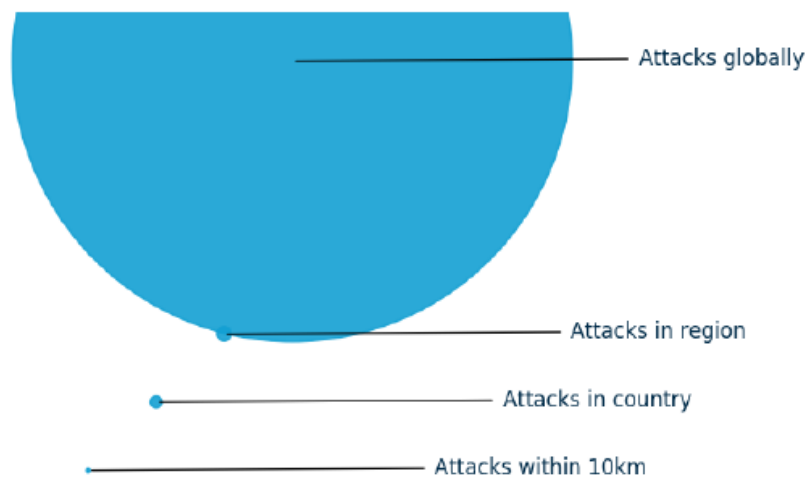
The background risk score is calculated using historical data of past terrorist attacks. The purpose of this score is to contextualise the risk exposure of a site based on its location and by looking at historical trends, taking into account the proportion of global terrorist attacks which have occurred within the region, the number of terrorist attacks in the region which have occurred within the country, and the number of terrorist attacks in the country which have occurred within 10km.

Background Risk Rating

Very Safe



Number of attacks globally	104205
Number of attacks in region	68
Number of attacks in country	45
Number of attacks in 10km radius	5



The following criteria is applied to generate a qualitative rating based on the quantitative score.

Criteria	Rating	Description
See official product guide	Very Safe	The surrounding area, country and region have historically not experienced any notable levels of terrorist activity. Terrorist attacks are rare and do not happen within any regular frequency, with less than 1 attack occurring every year on average since 2001.
See official product guide	Safe	The surrounding area, country and region have historically not experienced any notable levels of terrorist activity. Terrorist attacks are rare but occur with some regularity with at least 1 attack occurring every year on average since 2001.
See official product guide	Moderate	The surrounding area, country and region have experienced high levels of terrorist activity and attacks on a regular and frequent basis

Criteria	Rating	Description
<i>See official product guide</i>	Dangerous	The surrounding area, country and region have experienced high levels of terrorist activity and attacks on a regular and frequent basis.
<i>See official product guide</i>	Very Dangerous	The surrounding area, country and region have experienced globally high levels of terrorist activity and attacks on a regular and frequent basis and at high volume.

Resilience#

Resilience is defined as the ability for a site to recover from an incident or attack. PDR uses threat and resilience as its primary metrics for assessing terrorism risk. This differs from other methods to assess terrorism risk which typically use a combination of threat and vulnerability.

Every question related to the security measures in place are assigned to one of these seven categories. A user's answer to a question is converted into one of two response types: a positive or a negative response. A positive answer means that the answer reflects a positive impact on the risk of the site, that is, it decreases its vulnerability or risk exposure. A negative answer means that an answer reflects a negative impact on the risk of the site, that is, it increases its vulnerability or risk exposure. This conversion is necessary as there are instances where an answer to a question, such as "yes", will be considered positive (e.g. "Do you have CCTV cameras in place") and other instances where it will be considered negative (e.g. "Is the site exposed to vehicle traffic").

The resilience scoring comprises of seven categories: planning, deterrence, detection, prevention, protection, response, and recovery.

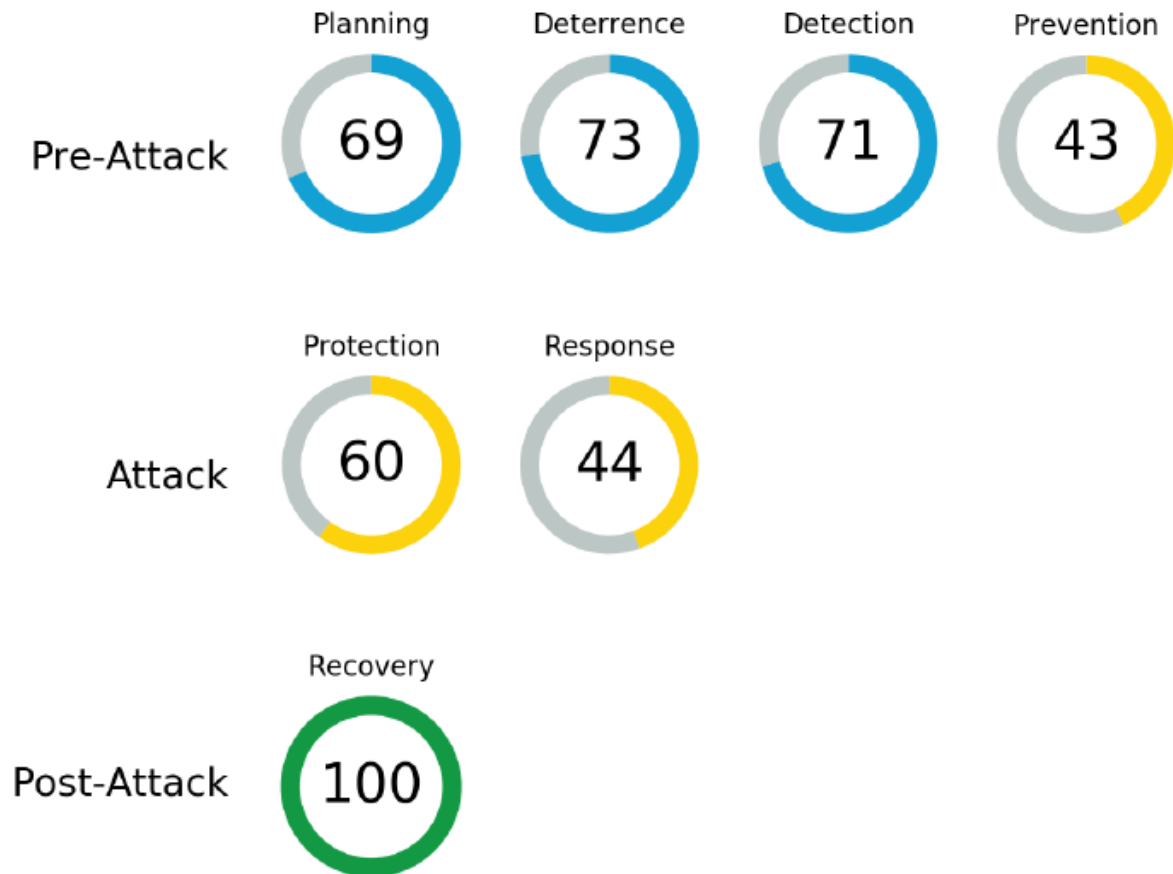
Resilience Scoring#

The report will provide a score for each of the seven resilience categories. The categories themselves are grouped together into Pre-Attack, Attack, and Post-Attack to match the phases of an attack where that resilience category would be most relevant.

The resilience score for a given category is determined according to the following formula:

$$\frac{P_c}{T_c - NA_c}$$

Where P is the total number of questions in a category with a positive response, T is to the total number of questions grouped in a category, and NA is the total number of questions in a category with a "Not Applicable" response, and c is one of the seven categories.



Recommended Level of Security#

The recommended level of security is generated based on a site's threat and vulnerability ratings and correlates with the risk improvement actions provided. The score determines the level of security mitigation measures a site ought to adopt in its protection from a terrorist threat.



Proposed Public Protection Measures#

Each question has a corresponding proposed public protection measure which is inserted if the question is answered in the negative. If a question is answered in the positive, the corresponding recommended action is not included.

WARNING

The recommended actions used in the standard version of PDR have been taken from the security controls and measures outlined by *ProtectUK, the ProtectUK 'Publicly Accessible Locations (PALs) Guidance' (2022)*, and the *National Protective Security Authority (NPSA)*. The actions themselves, as well as the method for selecting and grouping these actions may be further customised by the user to meet their specific requirements.

Each recommended public protection measure is assigned one of three priority levels: critical, recommended and best practice.

Priority	Description
Critical	A critical measure encompasses fundamental or essential measures that are critical to the effective management of security risks and threats. These critical measures should be prioritised for immediate implementation as without them the defensive capability of a site is severely compromised. Critical measures can be considered the minimum standard for effective management of security risks and threats and are therefore relevant for all sites regardless of threat rating.
Recommended	Recommended public protection measures improve defensive capability and effectiveness against security risks and threats beyond a basic or essential level. A site will typically implement a selection of these recommended measures to enhance its defensive capability based on specific security requirements and threat ratings. The number of recommended measures that should be in place increases as the threat level increases.
Best Practice	Best practice public protection measures provide specialised capability or improvements to security in particular scenarios and sites. These measures are highly specialised and address specific threats and risks that may not be relevant for all sites or scenarios. Best practice measures are most relevant for sites where the threat rating is high or very high. The higher risk level justifies the deployment of more specialised measures and controls to provide additional defensive capability.

This designation varies depending on the threat score. For example, a public protection measure "Install CCTV cameras at all entrances and exits" may be designated as critical if the threat score is Very High, High, recommended if it is Moderate and best practice if it is Low or Very Low. An example is demonstrated below:

Action	Very Low	Low	Moderate	High	Very High
A1 Plans are to be extended to cover the entire route. In particular, the plan must identify all potential risks across the entirety of the route and determine possible measures that could be implemented.	Best practice	Best practice	Best practice	Recommended	Recommended

The complete mapping of recommended measures to priority level based on threat rating can be provided for users upon request.

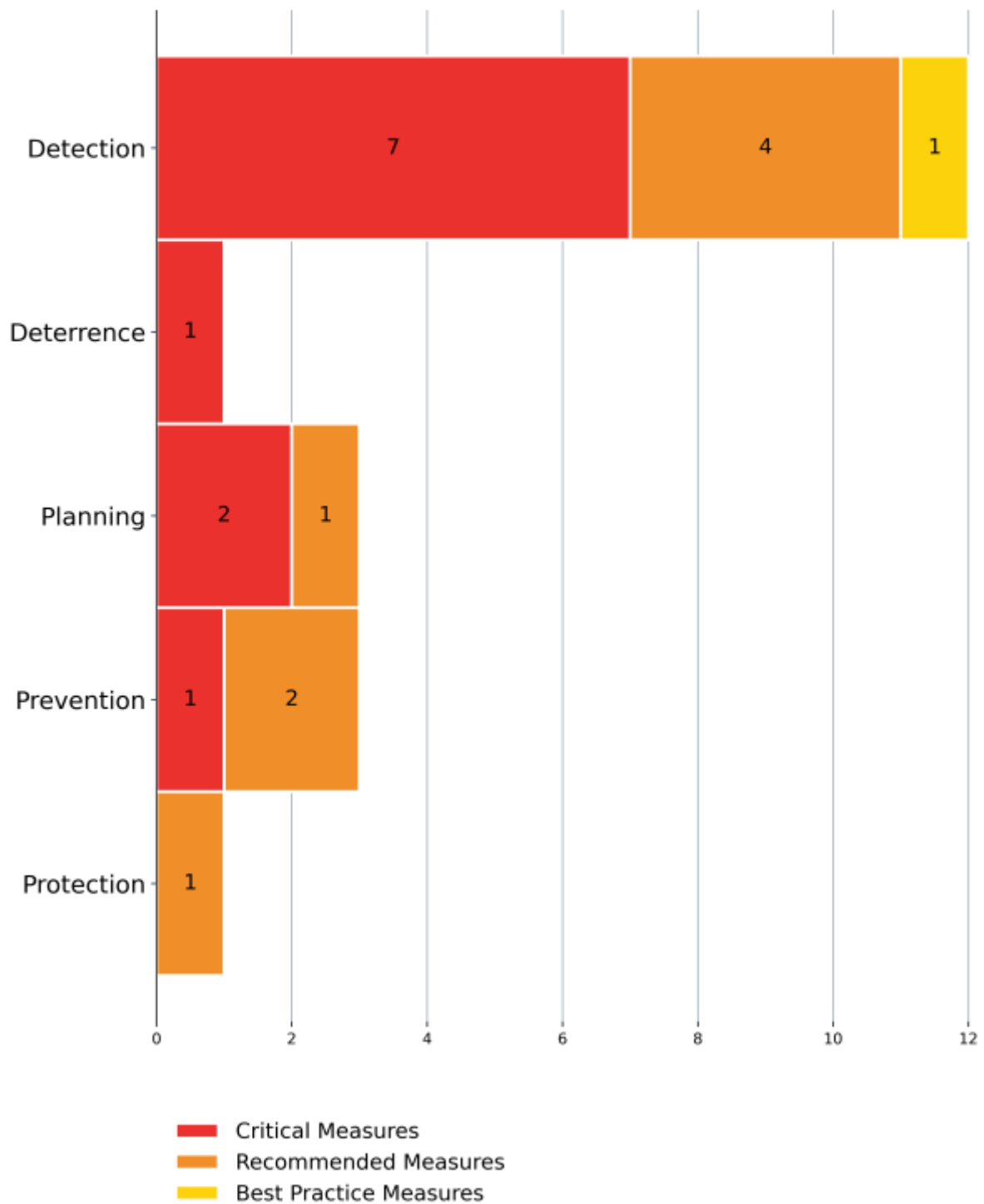
The report generates a chart which provides the number of proposed public protection measures in each priority level:

Proposed Measures by Priority Level



And an additional chart showing the number of proposed measures per priority and per resilience category:

Proposed Measures by Capability




Register of Proposed Measures#

The report also contains an auto-generated Register of Proposed Measures. This register provides a risk description, corresponding recommended measure, and interactive fields for tracking response, action, progress and person responsible.

Register of Proposed Measures

Critical Measures

Critical measures are those that may be critical to the effective management of security risks and threats at the premises or site. It is recommended that these critical measures should be prioritised for implementation as the resilience of the premises or event may be significantly compromised if not implemented. The number of critical measures increases as the threat level increases. Whilst these measures have been classified as critical, the premises should still review each measure and determine whether these measures are appropriate and proportionate to the particular needs and requirements of the building or event.

Risk Description	Recommended Measure	Response	Action	Progress	Person Responsible
 Visitors not properly informed of search procedures.	A73 Signage indicating bag searches and person screening is to be placed at points of entry in highly visible areas. Category: Deterrence Cost: Low				

Part B: Full Results#

In Part B of the report, each risk and resilience score is explained, clarifying the qualitative and quantitative meaning of each result.

Additionally, Part B: Full Results includes a full record of the questions and answers from the assessment, along with further details for each question. The additional details provide recommended security policies and procedures and provide a reference to the relevant standard or guide from which the question was sourced.

Question and Answers	
NA	<p>Q: If you have a moving event, do your security and emergency plans cover the entire route?</p> <p>A: Not applicable.</p> <p>The assessment has indicated that this question is not applicable to the asset.</p> <p><i>Reference: ANZCTC Crowded Places Security Audit (2017)</i></p>
NA	<p>Q: If a moving event is taking place (e.g. Fun Run), is there vehicle protection for the whole route?</p> <p>A: Not applicable.</p> <p>The assessment has indicated that this question is not applicable to the asset.</p> <p><i>Reference: ANZCTC Crowded Places Security Audit (2017)</i></p>
NA	<p>Q: Do roads remain closed for a safe period after the moving event has passed?</p> <p>A: Not applicable.</p> <p>Roads should remain closed for an appropriate period of time after a moving event has passed to ensure that the event has moved on a sufficient distance away.</p> <p>The assessment has indicated that this question is not applicable to the asset.</p> <p><i>Reference: ANZCTC Crowded Places Security Audit (2017)</i></p>
NA	<p>Q: Are alterations to traffic flow monitored during a moving event?</p> <p>A: Not applicable.</p> <p>The assessment has indicated that this question is not applicable to the asset.</p> <p><i>Reference: ANZCTC Crowded Places Security Audit (2017)</i></p>
NA	<p>Q: Are alterations to traffic creating an unexpected hazard?</p> <p>A: Not applicable.</p> <p>Any alterations to traffic due to a moving event may introduce additional or unexpected hazards. This may include increased risk of accidents, or hazards to pedestrians outside the event area. When alterations to traffic flow have been implemented, the risk assessment should also consider potential risks arising from these alterations as well.</p> <p>The assessment has indicated that this question is not applicable to the asset.</p> <p><i>Reference: ANZCTC Crowded Places Security Audit (2017)</i></p>
✓	<p>Q: Are access passes, keys, or tickets which allow for entry into the asset available on an uncontrolled basis?</p> <p>A: Access passes into the asset are restricted or controlled.</p> <p>Where access to an asset is controlled, there must be a mechanism for determining whether a person is authorised or unauthorised to enter the asset. This may come in the form of access passes, keys, tickets, or other forms of entry verification or authorisation. The ease of which these mechanisms allow entry verification or authorisation to be obtained determines how effective access controls are in the first instance.</p> <p>The assessment has identified that keys, access passes, tickets or other form of entry pass that allows for entry into Sydney Opera House are controlled, and they can only be obtained by persons that meet specific identity or security requirements.</p> <p><i>Reference: NaCTSO Crowded Places Guidance (2017)</i></p>

PDR Troubleshooting

I Think the Threat Score Is Too Low or Too High#

Background on How PDR Scores Threat#

It is important to acknowledge that PDR provides a particular perspective and method to measure threat. Your own perception of the threat level may be influenced by factors, considerations and weightings that are very different to those used by PDR. For this reason, you may feel that the threat score provided by PDR is "too high" or "too low" relative to your own assessment of site. PDR employs methods that are different to those that might be performed by a human assessor, and that is its main strength: it thinks and approaches the problem of assessing terrorism risk in a different way that minimises human bias. For this reason, you may instinctively disagree with the results produced by PDR. PDR is not intended to override your own perception or assessment and should not be used as such. PDR is designed to provide an additional perspective, providing data points and insights that may enhance your own assessment of the situation. The following may provide additional insight on how PDR behaves and performs its scoring, which may also provide further insight on why you received a score that was "too high" or "too low".

Why Your Score May Be "Too High" <#>

The threat score is determined by applying a contra-harmonic mean to the site risk score and background risk score. A contra-harmonic mean is used because it allows the overall threat score to moderate between potentially large differences between the site risk score and background risk score. For example, a site may have a high site risk score because it is a very prominent or iconic site but be located in an area which has a historically low amount of terrorist activity. The overall risk score for this site will still be high as the contra-harmonic mean will take the higher value of the site risk score as the dominant feature. Another site may be located in an area which historically high levels of terrorist activity, but not be particularly prominent. In this case, the fact that the site is located in a high-risk area becomes the dominant factor in its overall threat score, so this becomes the dominant feature. In the context of PDR, the contra-harmonic mean therefore behaves in a manner that helps minimise false negatives versus a harmonic mean which would minimise false positives. Simply put, PDR will tend to overscore threat rather than underscore it.

Why Your Score Might Be "Too Low" <#>

The dominant cause of threat scores being seen as "too low" is due to the reference terms used in the online search that in turn drives the site risk score. The reference name/terms used may have been too specific, or configured in a way that overly restricts the scope of the online search performed.

I Disagree with the Recommended Level of Security <#>

The recommended level of security is only meant to be exactly that - a recommendation directly based on the threat score, with each threat score level mapping directly to a recommended level of security. The recommended level of security may not be appropriate for your specific circumstances but can provide a guide for what security measures should be considered.

Sites are Missing from the Surrounding Area Search <#>

The analysis performed to identify surrounding sites is based on open-source data. Sites may be missing from the search as a result of three main issues:

- The site has not yet been mapped
- The site has been deliberately removed (due to security or privacy reasons)
- The site is incorrectly or inaccurately labelled as something else (e.g. a police station labelled as a office building)

PDR has several measures in place to try and minimise these issues with open-source and crowd-sourced data, however these are also issues which are inherent to the use of this type of data.