

Threat, vulnerability and risk

Assessing threat, vulnerability and risk when developing a counter terrorism protective security plan.

First published 1 June 2026

Assessing threat, vulnerability and risk is integral to the development of a counter terrorism (CT) [protective security plan](#). This section sets out the steps that the CT security coordinator should carry out.

Asset assessment

Asset assessment involves deciding what asset(s) needs to be protected. An asset includes any person, place, event or property whose protection is under consideration.

For example, in the context of royal and specialist directed events, the asset may be a member of the Royal Family.

Threat assessment and vulnerability

CT security coordinators should work with the police strategic commander to agree a threat assessment that is specific to the event or operation.

Threat assessment is one of the main drivers in the development of a CT protective security plan. It involves assessing the probability of an attack and the possible methods used, based on an understanding of hostile groups and actors' intentions and capabilities. This assessment process should be used by the CT security coordinator to help identify appropriate and proportionate security measures that reduce vulnerability associated with assets.

CT security coordinators should access local, national and international sources that can help inform the threat assessment. This can include requesting the counter terrorism policing network to provide them with a specific threat assessment product for an event.

The CT security coordinator should consider the following:

- Many different events may share the same threat assessment, but the vulnerability inherent in each event is unique.
- The absence of a known or specific threat in the threat assessment does not preclude recommending increased levels of security. This consideration may be particularly important when working towards a strategic commander's strategic intention or when asking partners to sign off on a memorandum of understanding that sets out clearly where responsibilities for different aspects of security lie. This would provide partners and stakeholders with a clear understanding of roles, responsibilities and the expectations for any service that is provided.
- The vulnerability associated with assets is assessed by considering the predictability of the time and place of the event and security measures to counter the possible method(s) of attack.

Risk assessment

In the context of protective security, risk assessment is based on an understanding of both threat and vulnerability. An important feature of a risk detailed in the CT protective security report should be the recognition of residual risk, as forces are not expected to apply every possible countermeasure to reduce a risk.

The CT security coordinator should base their risk assessment on thorough analysis and assessment of all the available and relevant information. This may include liaising with subject matter experts.

The strategic commander should define what they want the police security profile of the event to look like. This may include:

- the protective security image that the police strategic commander would like to convey
- any relevant budgetary and resourcing constraints

The tactical commander should ensure that the tactical plan meets the risk requirements provided by the strategic commander, considering any agreed mitigation measures recommended by the CT security coordinator.

Risk management

The CT security coordinator should gain the authorisation of the strategic commander for the risk and planning parameters during the creation of the CT protective security plan. The CT security

coordinator should then engage with the tactical commander to plan for the event.

The CT security coordinator should use the risk management process to:

- provide a framework for assessing main factors relevant to protection
- consider a basis for making rational protection decisions
- provide accountability for the decisions made
- allow for review
- provide an acknowledgement that the strategic commander's appetite for risk may conflict with the prevailing threat assessment
- consider the potential deployment of countermeasures to minimise risk to an acceptable level
- consider the operational value of potential countermeasures and resources

For further information, go to:

- [National decision model APP](#)
- [Risk APP](#)

Tags

Counter terrorism