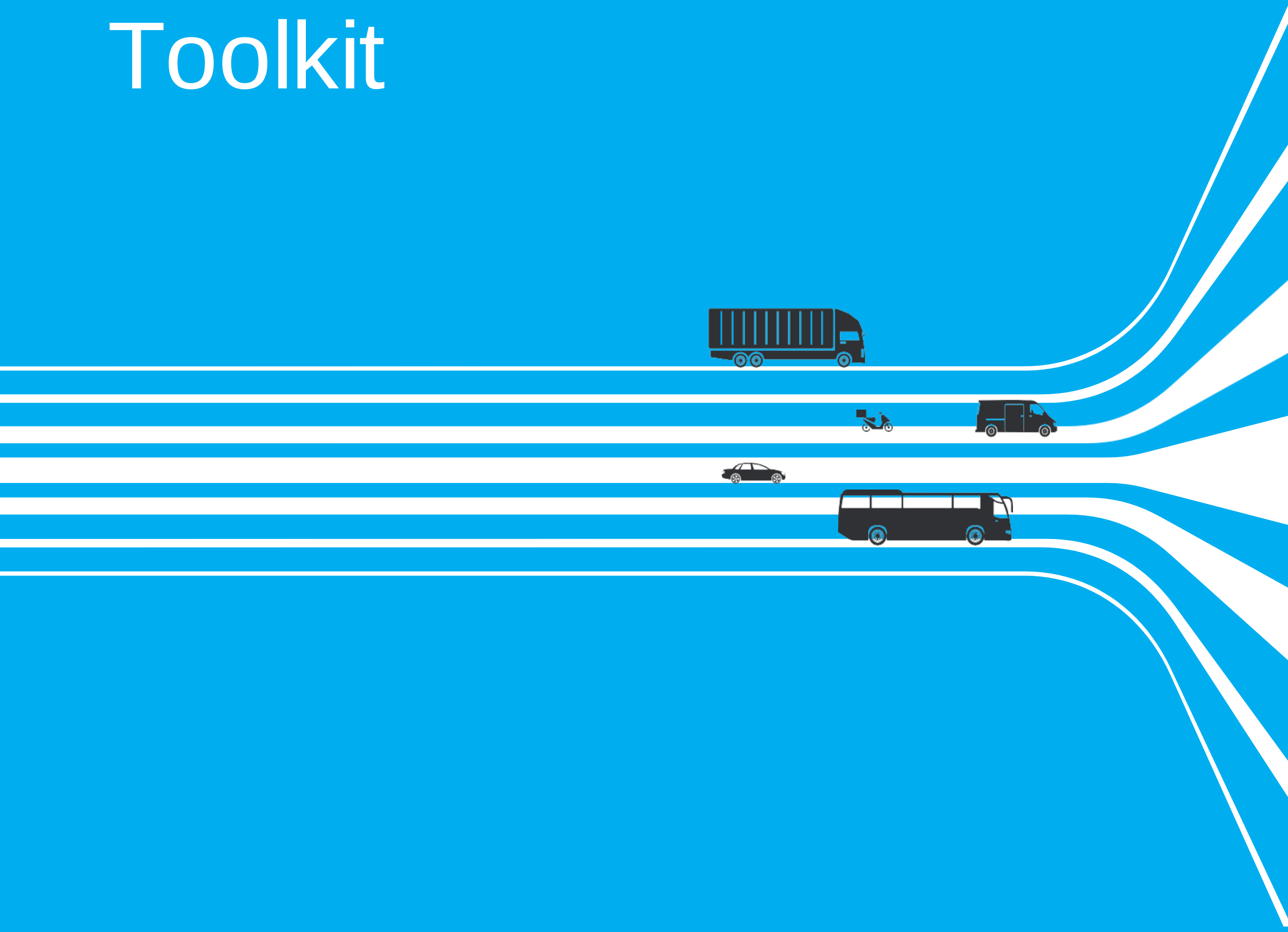
FORS Counter Terrorism Toolkit



Version 1.1
November 2019

Version number	Month	Year
1	January	2019
1.1	November	2019

Summary of main changes to this document between version 1 January 2019 and version 1.1 November 2019

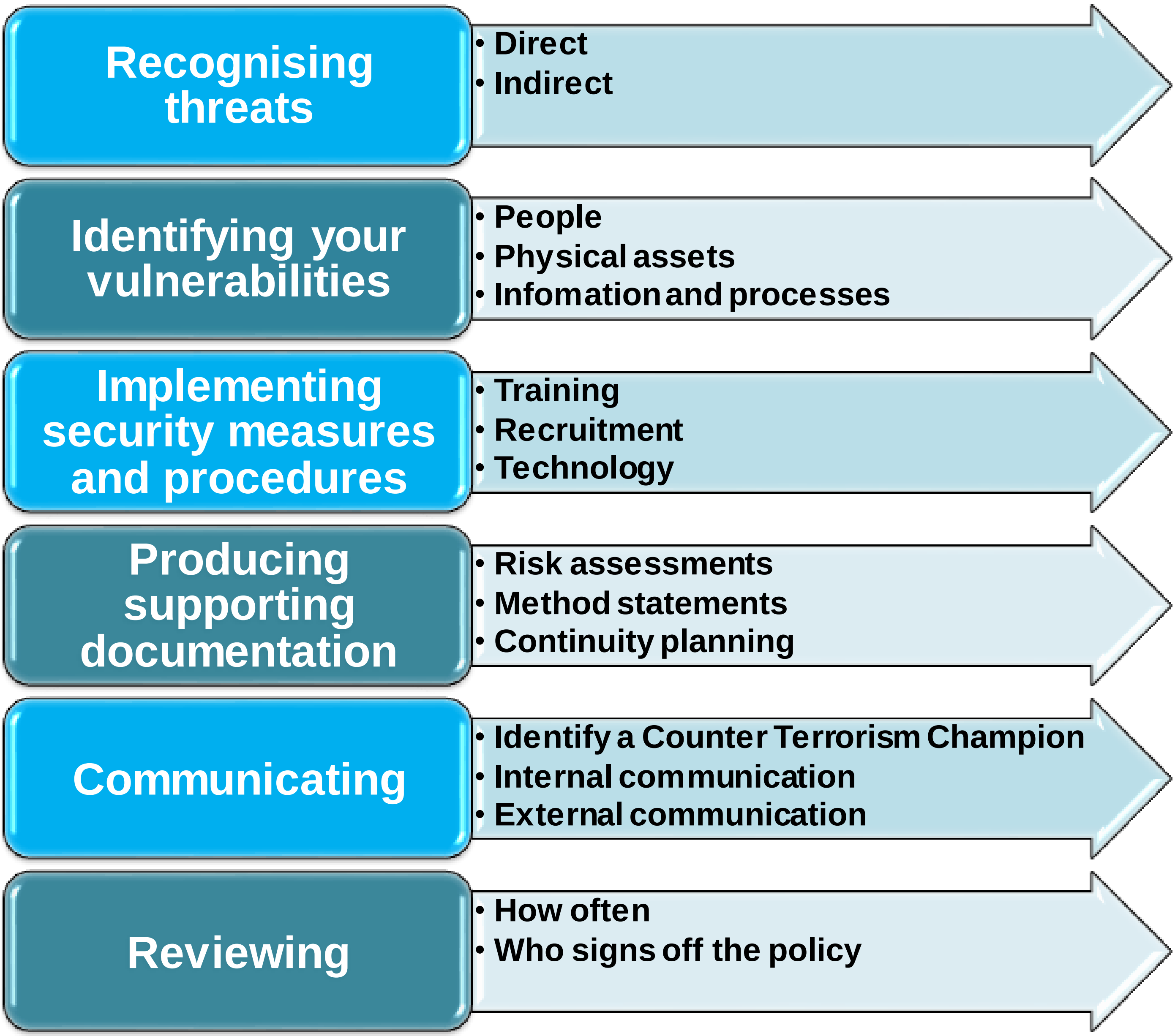
Item	Version 1	Version 1.1	Summary of changes
1.1	Why is counter terrorism now incorporated into the FORS Standard?	Why is counter terrorism now incorporated into the FORS Standard?	Removed mention of current UK threat level

Contents

1. Introduction

In version 5 of the FORS Standard, under Bronze requirement 'O7 Counter terrorism', an organisation must have a policy and supporting procedures in place to help safeguard against potential security and terrorist threats. FORS has produced this document which, used in conjunction with the FORS Standard, will help you to write an effective counter terrorism policy and supporting procedures. In addition, the document provides guidance on communicating your policy and keeping your organisation up to date with any new vulnerabilities or threats that have been identified. The process can be broken down into the following steps:

Tip: You must read the Demonstration of Bronze requirement 'O7 Counter terrorism'



Recognising threats
- Direct
- Indirect

Identifying your vulnerabilities
- People
- Physical assets
- Infomation and processes

Implementing security measures and procedures
- Training
- Recruitment
- Technology

Producing supporting documentation
- Risk assessments
- Method statements
- Continuity planning

Communicating
- Identify a Counter Terrorism Champion
- Internal communication
- External communication

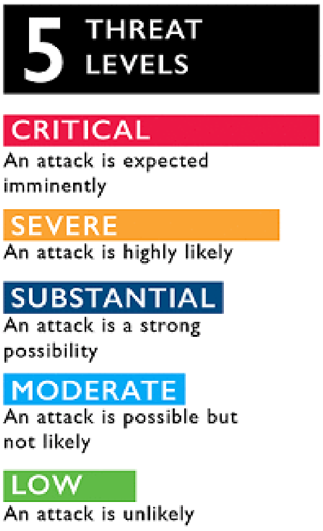
Reviewing
- How often
- Who signs off the policy

Certain language is used within this document indicating what is mandatory when creating a counter terrorism policy and procedures and how it must be cascaded and reviewed. 'Must' indicates an element that is mandatory to demonstrate a requirement has been met. 'Should' indicates an element that is recommended as good practice.

At the end of the document, there are two checklists. The first (section 12), will ensure you have met the requirements of Bronze requirement ‘O7 Counter terrorism’. The second (section 13), will ensure your counter terrorism policy complies with other requirements in the FORS standard.

1.1. Why is counter terrorism now incorporated into the FORS Standard?

The importance for organisations to have a counter terrorism policy follows the disturbing rise in the use of commercial vehicles in terrorist-related incidents. In 2017, 14 people were killed in London in three separate attacks where a commercial vehicle was used as a ramming device, otherwise known as a Vehicle as Weapon attack. Across Europe, Vehicle as a Weapon attacks have had an even greater impact. Between 2016 and 2017, four attacks resulted in the deaths of 126 people.



5 THREAT LEVELS

CRITICAL
An attack is expected imminently

SEVERE
An attack is highly likely

SUBSTANTIAL
An attack is a strong possibility

MODERATE
An attack is possible but not likely

LOW
An attack is unlikely

The 5 UK threat levels

1.2. What is a counter terrorism policy?

A policy is the overarching commitment of the organisation. The policy should apply to all staff in your organisation, including senior management. Your counter terrorism policy does not have to be a large document (around 2-4 pages is sufficient), although it does have to be specific to your operation and must cover everything that your organisation considers may be ‘at risk’ from a potential terrorist threat(s). The policy must always be supported by procedures. These are a series of steps for employees to follow as a consistent approach to accomplish an end result.

You can attend FORS Practitioner workshop 1- Developing fleet management policy for guidance on writing and structuring your transport policy

1.3. Combining vehicle security and counter terrorism policy

Operational security (Bronze requirement O6) and Counter terrorism (Bronze requirement O7) policy share many overlapping principles, such as vehicle security. Therefore, you can incorporate both into one single policy to meet both requirements. If you choose to do this, you must state clearly that your policy covers both requirements.

1.4. Small operators

Small operators are organisations with fewer than five vehicles and fewer than five employees.

Although all operators are encouraged to produce and maintain documented evidence of meeting the FORS Standard, in accordance with section 2.12 of the FORS Standard, small operators may demonstrate verbally that they meet certain Bronze requirements, including Bronze requirement ‘O7 Counter terrorism’.

2. Policy statement

Your policy must begin with a policy statement. This is an overarching statement of what your organisation intends to do to address the issue of terrorism. For a counter terrorism policy, this will almost always centre around identifying security threats and the use of procedures to minimise potential threats.

3. Recognising potential threats

Before considering how to mitigate risks, you need to understand the range of threats your organisation could face. Threats can be both direct, where your organisation itself is the target, and indirect, where your organisation itself was not the target but finds itself dealing with the consequences. Threats can range from comparatively low-key to critical events.

3.1. Direct threats (your organisation is the target)

For direct threats, you need to consider what elements, or circumstances, within your operations could put your employees or assets directly in harm’s way. For example:

- Does your organisation deal with chemicals, explosives, gases or other hazardous substances that could be used by terrorists?
- What information about your organisation is readily available to the public?
- How careful are employees with assets that might contain sensitive information i.e. mobile phones?
- Is your organisation associated with a high profile individual(s), through visitors, sponsors, contractors or a contentious area of work?
- How aware is your organisation about the current terror risk in the area(s) you operate?
- Do all areas of the business undertake consistent recruitment checks?
- How vulnerable are your vehicles to being stolen or exploited to aid terrorist objectives?

3.2. Indirect threats (your organisation is not the target but you are dealing with the consequences)

Your organisation may also be indirectly impacted by terrorism:

- Do you operate in high risk areas which are likely to be targeted?
- Could your IT networks react to the sudden emergence of a new virus or hackers?

More information on how to recognise terrorist threats can be found here

4. Identifying vulnerabilities

Once threats have been identified you need to decide who or what in your organisation is vulnerable and needs safeguarding, so you can put procedures in place to protect them. For this you might want to group vulnerabilities into the following categories:

1. **People** - staff, customers and contractors
2. **Physical assets** - buildings, vehicles and equipment
3. **Information and processes** - IT systems, data, supply chains

Additional information on identifying vulnerabilities can be found here

Tip: You do not have to use all of these if you feel they are not specific to your organisation. You can add other vulnerabilities within your organisation which are not listed above.

5. Implementing security measures and procedures

Having acknowledged what assets in your organisation could be vulnerable, you need to devise appropriate security measures or procedures to protect them. It is important to remember that no single security measure/procedure or level of investment will provide 'total' protection to your organisation. However, there are a range of measures and procedures you can use to minimise the possibility of terrorist threats.

Tip: You must create a procedure for any other elements specific to your business which may be affected by terrorism

As part of this exercise, you also need to identify where your existing security measures need improving. You must create a procedure to cover your training and another procedure to cover recruitment or ensure your existing procedures include these elements. You should also consider creating a procedure to cover technology.

5.1. Technology

It is not practical for a business to invest in every technology available on the market. However, technical solutions such as remote door locks, ignition locks and other safeguards could help prevent vehicles from being stolen. Moreover, telematics systems which track the vehicle and load can be helpful with route planning and geo-fencing as well as allowing for fleet operators to know exactly where a vehicle is in an emergency.

5.2. Training

Ongoing training for all staff is key for communicating and reminding staff of new and existing security measures and mitigating any bad habits which may have developed. In addition, and in line with Bronze requirement 'D4 Professional development', drivers of all vehicle types must complete the mandatory FORS Professional Security and Counter Terrorism eLearning module (or a FORS approved counter terrorism awareness training course or eLearning module). In accordance with 'Annex 1' of the FORS Standard, this training must be completed every 24 months as a minimum.

Further awareness information and training can also be utilised by visiting the national police counter terrorism website

5.3. Recruitment

In line with Bronze requirement 'M4 Staff resources', you must have checks in place for recruiting staff. These checks are in place to minimise the chances of employing someone who is not who they say they are. Checks you must carry out include:

- Employment history (usually five to ten years)
- Fitness to drive
- Qualifications and licensing
- Ability or eligibility to work

Further information on additional recruitment checks can be found here

You should also check if the applicant has any prosecutions pending or is waiting for sentencing by a court.

6. Documentation

Risk assessments, method statements and continuity plans are an effective way to document how you have identified threats and vulnerabilities and employed the appropriate protective procedures to reduce risk to as low as reasonably practicable. Risk assessments and method statements must be used to support counter terrorism policy and procedures to meet Bronze requirement ‘M1 FORS documentation’.

Tip: The methods used for documentation do not have to be included in your policy (but do need to be readily available at time of audit). You just need to demonstrate that you have used them when identifying threats/ vulnerabilities and creating procedures.

6.1. Risk assessments

A good way to formulate procedures to mitigate risk(s) from threats of terrorism is to produce a risk assessment(s). This will help you to understand where your risks are and how you can minimise these. A risk assessment is a document in which you identify elements within your work environment (such as situations, processes, etc.) that may cause harm, particularly to people. Once you have identified these, you analyse and evaluate how likely and severe the risk is. Then decide what measures must be in place to reduce or control the harm as far as reasonably practicable.

More information can be found about writing effective risk assessments for counter terrorism here

6.2. Method statements

A method statement sometimes called a ‘safe system of work’, is a document that details the way a work task or process is to be completed. The method statement must outline the hazards involved and include a step by step guide on how to do the job safely. The method statement must also detail which control measures have been introduced to ensure the safety of anyone who is affected by the task or process.

6.3. Emergency and business continuity plan

Unlike risk assessments and method statements, emergency and business continuity plans are not mandatory to comply with Bronze requirement ‘M1 FORS documentation’ in the FORS Standard. However, they are an effective document to use for identifying threats and vulnerabilities and employing the appropriate protective procedures to reduce risk. Emergency and business continuity plans can be used to document systems of prevention and recovery to deal with threats and risks facing a company, to ensure that personnel and assets are protected and able to function in the event of a disaster. A continuity plan must detail the immediate steps that must be taken by management and employees in an emergency and must, where possible, account for ways to enable your organisation to return to 'business as usual' as soon as possible.

Click here for further information on writing continuity plans

7. Counter Terrorism Champion

In line with Bronze requirement 'M4 Staff resources', a Counter Terrorism Champion must be appointed and identified in the organisation chart. You will need to appoint someone who you feel is competent to fill the role and explain to them what their roles and responsibilities will be. Their roles and responsibilities should encompass:

- The creation and implementation of your organisation's emergency response plan(s) (formed as part of the risk assessments, method statements and continuity plans)
- Ensuring the counter terrorism policy is reviewed, signed off and communicated, with any alterations also effectively communicated to all staff
- Ensuring staff feel confident in performing their duties set out in the policy
- Ensuring that your emergency and business continuity plan is followed through in the event of an emergency to allow for a quick response and a swift return to 'business as usual'
- Ensuring any relevant information or evidence is collected and reported to the emergency services and senior management, promptly, in accordance with your counter terrorism reporting procedure

8. Reporting

Your organisation must decide who your employees are expected to report an incident or suspicious activity to i.e. managers and/or your Counter Terrorism Champion as well as who, when required, will be expected to report the incident or suspicious activity externally (for example to the emergency services). Incidents that have an immediate threat to life and/or property will need to be reported externally first.

8.1. External reporting

Organisations must distinguish how they expect all staff to report a potential incident and how it is assessed as being substantial enough to inform the relevant authorities. The report should include the following information:

- Who and/or what was witnessed
- When it was seen
- Where it occurred
- Why it is suspicious

Should a security or terrorist incident need escalating to the emergency services, the following telephone numbers and hyperlinks direct your enquiry to the relevant authority:

- Call 999 – Speak to the police and report your suspicions
- Call 101- For crimes which do not require an emergency response
- Call the police anti-terrorist hotline on 0800 789 321 to report an immediate threat to life or property
- Report your suspicions to the Metropolitan Police online
- Report suspicious activity to MI5
- Report online terrorist material

8.2. Internal reporting

All staff must be aware of who their point of contact is (usually a line manager) and who their organisation’s Counter Terrorism Champion is, as well as their contact details. It is important that staff are aware of all the different channels of communication to reach their point of contact/Champion in the event of an incident or should they see something suspicious. Common methods of communication are:

- Phone
- Text
- Email
- Internal intranet

In an emergency, it is best to contact someone via the phone as this is the quickest method of communication.

Tip: Flash cards are a useful way of ensuring staff have the appropriate contact details for their point of contact. You should also provide employees with a cascading contact list i.e. if they can’t get in contact with their point of contact, who they would be expected to contact next

9. Acknowledgement of your counter terrorism policy

The policy must be approved and signed by senior management, in accordance with Bronze requirement 'M1 FORS documentation'. This is to acknowledge the policy and that they understand and agree with the policy being introduced. It is important to remember that this policy will contain some of the most sensitive information about your organisation so you need to be clear about how it is distributed.

10. Review and communication process

Outdated policies can leave your organisation at risk. Regular policy reviews and procedures keep your organisation up to date with any new vulnerabilities or threats that have been identified. Policy reviews also ensure that all your policies remain consistent and effective, especially in response to organisational changes. The policy, procedures and risk assessment relevant to counter terrorism must be documented, reviewed (a minimum of every 12 months in accordance with Bronze requirement 'M1 FORS documentation') and communicated to all transport-related staff, with any update or amendment also circulated (see Bronze requirement 'M5 Communication' for details). Moreover, the policy procedures and risk assessments must be retained until your next FORS audit in a legible condition as they will be required for inspection.

Tip: You should ensure everyone signs to demonstrate they are aware and have knowledge of the policy and procedures

When documenting how often you intend to review your policy, you should think about what circumstances would cause you to review your policy sooner than expected and include this in your policy document. For example, if the UK’s threat level is increased from its current level.

Any changes made to the policy after a review must always be communicated to all relevant employees. In accordance with Bronze requirement 'M5 Communication', communication must include the responsibilities relevant to drivers and staff involved in the fleet operation. New policy or changes to policy must be communicated using supporting documentation such as:

- Toolbox talks
- Driver handbook
- Staff briefings or training sessions
- Handouts to all staff
- High visibility coverage
- Staff notice boards
- Office intranet

All FORS Professional Toolbox Talks, which are aligned to version 5 of the FORS Standard, can be found here

11. Further guidance

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf

https://www.gov.uk/government/publications/stay-safe-film

https://act.campaign.gov.uk/

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/374657/expecting_the_unexpected_reviewed.pdf

https://www.gov.uk/government/publications/recognising-the-terrorist-threat/recognising-the-terrorist-threat

https://www.cpni.gov.uk/system/files/documents/5a/c9/Protecting-Against-Terrorism.pdf

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62327/secure-in-the-knowledge.pdf

12. Checklist for meeting Bronze requirement ‘O7 Counter terrorism’

Completing this checklist correctly will aid you in writing your policy and procedures and will help you to meet Bronze requirement ‘O7 Counter terrorism’.

No.	ACTION	COMPLETED
1.	**Have you created an overarching policy statement?**	
2.	**Have you assessed the different threats to your business?**	
3.	**Have you identified the vulnerable assets (people, physical assets and information) to your organisation?**	
4.	**Have you included procedures to reduce the risk of threats to those that are vulnerable?**	
5.	**Have you documented the assessment in writing through risk assessment, method statements and continuity plans?**	
6.	**Have you nominated a Counter Terrorism Champion within your organisation and are they fully aware of their roles and responsibilities?**	
7.	**Are all staff aware of how to report a potential incident to authorities, who their point of contact is within the organisation and what is the preferred method of communication?**	
8.	**Are managers aware of the procedure of how to handle incidents when they are reported to them, both internally and externally?**	
9.	**Have you incorporated all mandatory training relevant to counter terrorism into employees' personal development plans and planned for how it will be kept up to date?**	
10.	**Have background checks for new employees been implemented in the recruitment process?**	
11.	**Has the policy been reviewed and signed off by senior management?**	
12.	**Have you cascaded the policy and procedures to staff in a manner whereby they understand what is required of them and have they signed to say they do so?**	
13.	**Has a process been put in place to ensure your counter terrorism policy is reviewed a minimum of annually?**	

13. Checklist for related requirements

This checklist will help to ensure that you comply with other supporting requirements within the FORS Standard.

No.	ACTION	COMPLETED
1.	**The policy, procedures and risk assessment relevant to security and counter terrorism must be documented and reviewed in accordance with Bronze requirement 'M1 FORS documentation'**	
2.	**The policy, procedures and risk assessment relevant to security and counter terrorism must be retained in accordance with Bronze requirement 'M2 Records'**	
3.	**The policy, procedures and risk assessment relevant to security and counter terrorism must be communicated in accordance with Bronze requirement 'M5 Communication'**	
4.	**The policy, procedures and risk assessment relevant to security and counter terrorism must be consistent with requirement O6 (if not combined with O7)**	
5.	**FORS Professional Security and Counter Terrorism eLearning must be included in your Professional Development Plans in accordance with Bronze requirement 'D4 Professional development'**	
6.	**The Counter Terrorism Champion must be identified in the organisation chart in accordance with Bronze requirement 'M4 Staff resources'**	

FORS
FLEET OPERATOR
RECOGNITION SCHEME

08448 09 09 44
enquiries@fors-online.org.uk
www.fors-online.org.uk

@FORS_online