ProtectUK

# Setting the Scene

**ProtectUK publication date**
19/03/2024

This section introduces some of the key components you need to consider before undertaking a risk assessment, including:

- **Organisational Context**

Establishing your internal and external context can help you to set the scene for your risk assessment. This allows you to manage risk in context.

- **Governance**

Setting out a dedicated policy and allocating roles and responsibilities will help you to establish clear direction, ownership and control of the risk management process in your organisation.

- **Risk Appetite**

Establishing the amount of risk that you as an organisation are willing to be exposed to will help ensure that risks are managed in line with your organisational needs and objectives.

- **Scope**

Defining the scope of your risk assessment will enable you to clearly establish what will be captured within your risk assessment.

# Organisational Context

Establishing your internal and external context can help to ensure that risks are understood in relation to your operational environment, business activities and organisational objectives. This is particularly important as certain organisational factors may be a source of risk.

The internal and external context of your organisation should guide the risk management process, helping to inform the choices you make in planning your risk assessment and managing risk.

Your **external** context should take account of:

1. Any social cultural, political, legal, regulatory, financial, technological factors relevant to your organisation
2. Whether these factors are international, national, regional or local
3. Contractual commitments and relationships
4. External stakeholder relationships and expectations
5. Key trends and drivers affecting your organisational objectives

Your **internal** context should take account of:

1. Strategic vision, mission and values
2. Governance and internal organisation
3. Objectives and policies
4. Organisational culture
5. Standards, guidelines, models and best practice adopted by the organisation
6. Available resource and knowledge (including time, people, systems, technologies etc.)
7. Internal stakeholder relationships and expectations

Establishing a clear picture of your organisational context will help you to determine what is important to your business, as well as the resources available to you. It can also help you to consider factors that may increase the likelihood of you being targeted for attack, such as social or political factors.

Throughout this guidance, you will be prompted to consider your organisational context when completing particular activities in the risk management process.

## Governance

Before implementing your risk management approach, it is essential that you establish oversight and accountability of the risk management process within your organisation. This requires the integration

of risk management into your organisational activities at all levels.

Everyone has a responsibility to manage risk and this should be clearly communicated and understood across your organisation. To achieve this, you will need to establish and communicate a security policy and designate key roles and responsibilities to support the risk management process.

**Establishing a policy or statement**

Your commitment to security risk management should be captured through a policy or statement that communicates the purpose for managing security related risk. This policy (or statement) should also clearly outline the roles and responsibilities of key individuals.

You should provide reference to other relevant objectives and policies (e.g. health and safety), in addition to clearly outlining the resources you have made available to support risk management as a programme of work. Typical resources will often include, but are not limited to: people and skills, methods and tools for managing risk, documented processes and procedures, and professional development and training.

Any decisions that you make around the risk assessment process should also be clearly documented. This includes any approaches, methods or techniques you have selected to manage risk in your organisation. Outlining your approach to assessing risk will help to ensure consistency across your organisation, while also enabling others to understand the activities of the RMP and its outcomes.

**Key roles and Responsibilities**

Business owners must be prepared to allocate dedicated resources to risk management to ensure its ongoing effectiveness.

A key part of resource allocation in risk management is the assignment of dedicated roles and responsibilities at appropriate levels within the organisation.

A **responsible person** and a **competent person** are two essential roles that should be assigned to ensure the effective delivery of security risk management in your organisation.

**Responsible Person**

The role of the **responsible person** is to ensure that decisions about risk are implemented and the necessary actions are taken.

A responsible person will set the strategic direction of the RMP and ensure that the necessary resources are allocated to manage risk. Typically, this will be the business owner, but this role may be allocated to any another senior individual in your organisation who has the authority to direct and

control resources.

A responsible person will need to ensure that the importance of managing terrorist risk is clearly communicated and understood at all levels in the organisation. This includes issuing a policy or statement to establish the risk management approach and assigning authority and responsibility at appropriate levels within the organisation. For example, a competent person, senior leadership responsibilities, staff responsibilities etc.

The responsible person should closely monitor the progress of the RMP on a regular basis to ensure that risks remain at an acceptable level to the organisation, and that any controls measures implemented are working effectively to control risk.

At an operational level, a responsible person may choose to undertake the risk assessment process, or allocate this to a **competent person** to carry out this task on their behalf.

A competent person may also be instructed to provide assistance to the responsible person at different stages during the risk assessment. For example, when identifying vulnerabilities or verifying the effectiveness of control measures.

The overall responsibility for controlling terrorist risks will always remain with the **responsible person**.

**Competent Person**

It is important that the risk management process is supported by sufficiently competent people. A **competent person** or persons should be identified to help ensure the safety of employees, customers, volunteers and other visitors. Some employers may have already done this for other purposes but a suitable person should also be identified to help with the management of terrorist security risks.

**When identifying a competent person or persons, it is important to consider the following:**

- What will you require the competent person to do?
- What qualifications or training does your competent person need to perform their role effectively?
- Who can you designate as a competent person?
- When and how should you use an external competent person?
- Sources of competent persons

**What is the role of a competent person?**

A competent person may perform the following roles in your organisation:

- The first is to help an organisation **identify risk** and **put in place suitable controls.**

To perform this role, a competent person should have the skills, knowledge and experience to be able to recognise the risks facing the organisation. They should be capable of identifying the control measures best suited to protect the organisation, customers, staff and others in light of these threats, and be able to assist with the implementation of any selected controls. They may also be responsible for completing a risk assessment on behalf of a responsible person.

- The second is to **sense check or validate control measures**.

To perform this role, a competent person should have access to any relevant documentation, reports or sources of knowledge concerning the control(s) in question. They should be capable of establishing whether each control is working effectively to control risk based on the information that is made available to them. They may perform this role in addition to the above role.

Although the same person could undertake the role of a responsible person and a competent person, in most organisations these roles will be undertaken by different people. This is because the role of the competent person and responsible person are different.

As the strategic lead, the responsible person must be able to make decisions, commit resources and provide budgets to support any required actions resulting from the RMP. They must ensure that decisions about risk are implemented. To do this, they must be able to allocate dedicated resources and assign actions to relevant individuals.

**What qualifications or training does a competent person need to do the role effectively?**

Ideally, a competent person should have a thorough understanding of security and risk management. However, there are currently no legal requirements for a competent person to have formal security qualifications or formal training in managing risk.

Given the above, you may choose to seek out individuals in your organisation that have experience managing risk in other areas. For example, individuals that have responsibilities for health and safety or security. These individuals are likely to have some formally recognised qualification from places such as:

- The Institution of Occupational Safety and Health (IOSH)
- The National Examination Board in Occupational Safety and Health (NEBOSH)
- Security Institute
- International Security Management Institute (ISMI)

or

- Be a Certified Security Management Professional (CSMP) if they have undergone security training.

They may have also undertaken some counter-terrorism related training, such as the ACT Awareness e-learning programme offered by NaCTSO, or the SCaN training offered by NPSA.

This training makes these individuals best placed to take on the role of a competent person as they should have a good understanding of

risk management and some practical experience managing risk in the context of your organisation.

**Who can you designate as a competent person?**

You could assign one or a combination of:

- yourself
- one or more of your workers
- someone from outside your organisation

The person(s) chosen should be security minded, have knowledge of previous terrorist attacks and the different attack types, and knowledge of the control measures which can be used to protect against or respond to the different attack types.

If there is one or more competent persons within your organisation, it makes sense to use them rather than a competent person from outside the organisation because they will have a better understanding of the organisation’s needs. However, you may not think that your internal staff have the level of competence required to completely fulfil the role of a competent person, or you may simply prefer to have an independent evaluation of your arrangements.

**When and how to use a competent person from outside your organisation**

Although it is acceptable to appoint an internal competent person, there are various circumstances where appointing an external competent person is desirable. For example, there may be no suitably competent person available internally, or some aspect of the organisation’s premises or operations may require some specialised security expertise.

When appointing a competent person from outside your organisation, research suppliers carefully. Make sure that the skills, experience and knowledge they offer match your requirements, are up-to-date, and that you are clear about the extent and limitations of their expertise.

**Where to find competent persons and specialist advice**

You may already know such individuals or how to find them but, if not, there are a number of sources to which you can refer:

- The Register of Security Engineers and Specialists (RSES) which NPSA (formerly CPNI) sponsors and which encompasses Generalist Security Advisors (GSA) and Specialist Security Advisors (SSA)
- The Register of Chartered Security Professionals which is managed by The Security Institute
- The UK Register of Independent Security Consultants managed by the Association of Security Consultants (ASC)
- The National Cyber Security Centre (NCSC) has its own certification of industry expertise for cyber security
- Other sources may become available once the Protect Duty legislation is in place and other registration schemes are developed.

## Community and support networks

**You are not alone.** There will be many other organisations or businesses that are as concerned as you are about securing the sites in your neighbourhood against terrorist attack. It is ineffective to think about protecting your own site in isolation, as working with your neighbouring organisations and businesses not only makes things easier for you, but you will learn from each other and can plan a co-ordinated response.

Also, you do not need to do everything yourself – not even if you have appointed a competent person. Make the best use of the knowledge, experience and expertise around you. Consider which other organisations or stakeholders are involved in managing terrorist threats both locally and nationally with whom it would be beneficial to liaise, network or collaborate:

- Local resilience forums
- Police
- Other Emergency Services (Fire Service, NHS, etc.)
- Local authorities
- Civil contingency units
- Neighbouring businesses and organisations
- Landlords and site owners
- Parent organisations and other stakeholders
- Business Improvement Districts
- Franchisees
- Voluntary organisations

## Risk Appetite

Risk appetite is the amount of risk that you as an organisation are willing to be exposed to and are willing to take in order to achieve your objectives. This enables you to make informed decisions about when you should accept and treat risk.

Before undertaking a risk assessment, you should think carefully about your appetite for risk and outline your position clearly.

Different organisations will have different attitudes toward risk depending on their sectors, activities, culture and objectives. Different risk appetites may also exist across different types of risk. For example, you may less of an appetite for life and safety risks than operational risks. These variations will be discussed in more detail later in this guidance. For now, it is important for you to consider setting an overarching risk appetite. This will help you to clearly establish your general attitude and approach toward risk.

Typically, risk appetites may be defined as follows:

- **Averse**

Avoidance of risk and uncertainty in the achievement of key objectives.

- **Minimalist**

Preference for very safe options that have a low degree of inherent risk.

- **Cautious**

Preference for safe options that have low degree of residual risk.

- **Open**

Willing to consider all options and choose one most likely to result in successful delivery.

- **Eager**

Eager to be innovative and choose options based on maximising opportunities even if those activities carry very high residual risk.

When determining your position i.e. how much risk you are willing to be exposed to, you should consider your finances and resources, legal and regulatory environment, the expectations of your stakeholders, and your business aims and objectives.

Essentially, you are looking to answer the following question: at what level is the organisation comfortable with risk being taken?

Some organisations choose to approach the setting of risk appetite by producing a risk appetite statement that formally acknowledges the position they have adopted from the five appetites listed above. Others may apply the concept of risk appetite to their risk management approach without formally acknowledging this in such a statement.  Whether you choose to produce a formal risk appetite statement or not, you will still need to clearly communicate your expectations around risk in order to direct decision-making and ensure consistent practice.

The UK Government's Orange Book and additional guidance note on Risk Appetite provide further information on risk appetite and developing risk appetite statements. This includes a number of example risk statements that may help you develop your own statements.

Your risk appetite will help guide your decision-making throughout the risk management process, helping to ensure that you manage risk in ways that reflect your organisational needs and the expectations of your stakeholders.

## Scope

Before undertaking any risk assessment, it is essential that you define the scope of what you are assessing. This should clearly set out the boundaries of your assessment and what your assessment will capture.

The scope of a security risk assessment will typically capture an organisation's business as usual activities. However, some organisation may choose to undertake separate risk assessments for particular events or new systems.

**KEYWORDS**
RISK MANAGEMENT
RISK ASSESSMENT
RISK
RESPONSE