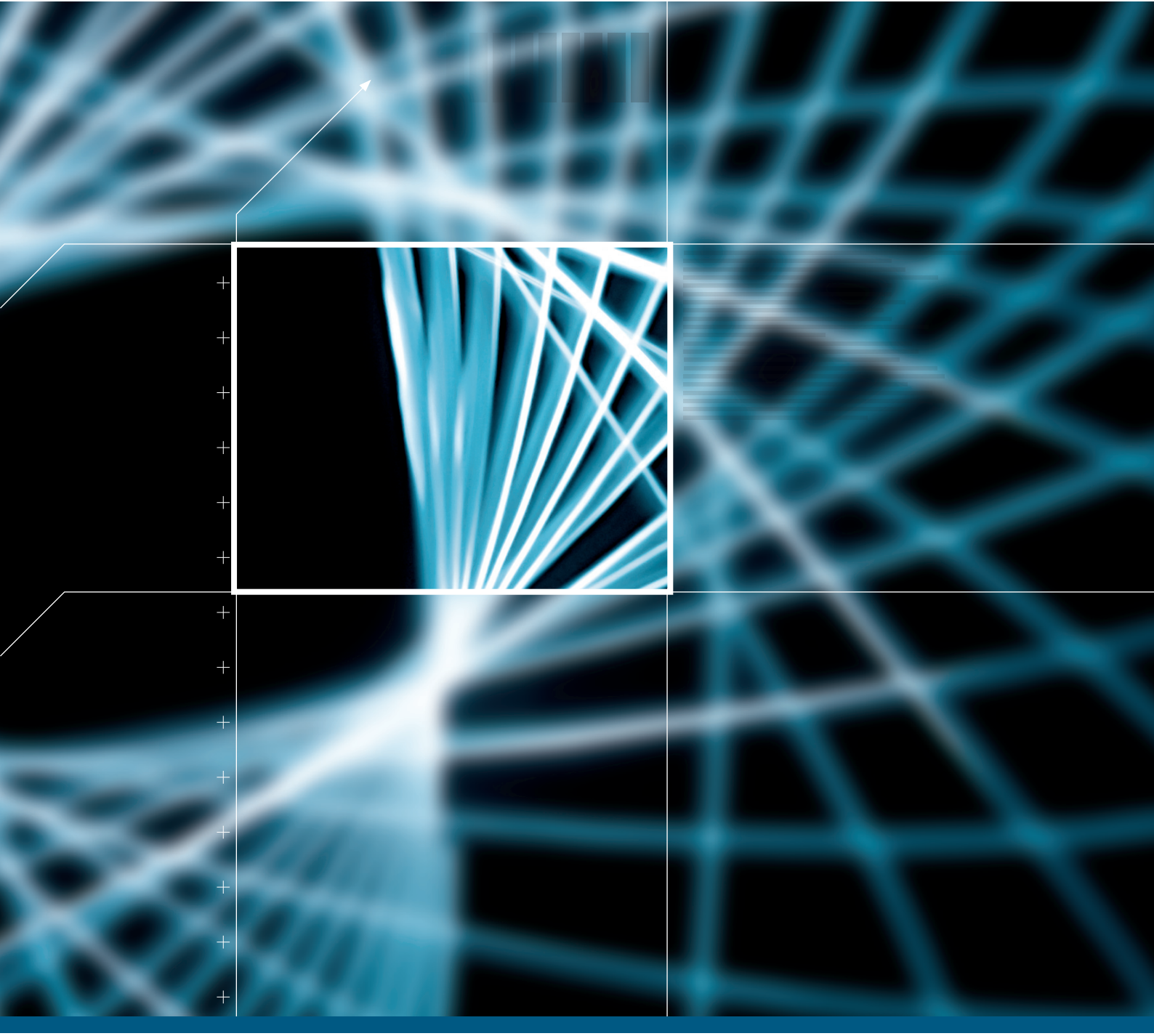


RISK ASSESSMENT FOR PERSONNEL SECURITY

A GUIDE

3RD EDITION

CPNI
Centre for the Protection of National Infrastructure

Contents

Introduction

Centre for the Protection of National Infrastructure

The Centre for the Protection of National Infrastructure (CPNI) is the government authority that provides advice on protecting the country's essential services, facilities and networks from terrorism and other threats.

The National Infrastructure

Nine different sectors form what is known as the national infrastructure. These provide the services which support everyday life:

- Communications
- Emergency Services
- Energy
- Finance
- Food
- Government
- Health
- Transport
- Water

CPNI provides security guidance, training and research from a physical, information and personnel security perspective. It aims specifically to reduce the vulnerabilities within these sectors, with particular emphasis on the most critical elements. Loss or disruption to any of these could cause severe economic or social consequences or even loss of life.

In addition to the nine sectors above, CPNI also provides similar advice to organisations engaged in planning and running the London 2012 Olympics.

A CPNI survey in late 2006 showed that many CNI organisations do not adopt a structured approach to personnel security. Very often, clear rationales for the use of particular personnel security measures are lacking and resources are not targeted in a proportionate way. It is more common for physical and electronic protective security measures to be applied on the basis of systematic risk assessments that promote cost effective security.

Personnel security risk assessment focuses on employees, their access to the organisation's assets, the risks they could pose to the organisation and the sufficiency of countermeasures. It is the foundation of the personnel security management process. It is also crucial in helping Security and Human Resource managers communicate to senior managers the risks to which the organisation is exposed.

This guidance, which is illustrated using a fictional case study, aims to help Security and Human Resource managers to:

- Conduct personnel security risk assessments in a way that balances pragmatism with rigour
- Prioritise the insider risks to an organisation
- Identify appropriate countermeasures to mitigate against those risks
- Allocate personnel security resources in a way that is cost effective and commensurate with the level of risk.

An electronic copy of this guidance is available on the CPNI website www.cpni.gov.uk.

Overview

Personnel security

Personnel security is a system of policies and procedures, which seeks to manage the risk of staff or contractors exploiting their legitimate access to an organisation's assets or premises for unauthorised purposes. Those who seek to exploit their legitimate access are termed 'insiders'.

For the purposes of this guidance, individuals who have legitimate access to an organisation's assets, but who are not staff or contractors – for example, postal delivery workers with temporary site access – fall outside this definition of insiders.

There are many different measures that can be used in a programme of personnel security. Most of them will fall into the following categories:

Pre-Employment personnel security measures	• **Screening** o Pre-employment checks o Assessing insider potential o National Security Vetting[1]
Ongoing personnel security measures	• **Screening** o Pre-employment check updates o Behavioural assessment o National Security Vetting and National Security Vetting aftercare • **Access controls** • **Promoting effective security culture** • **Social Engineering** • **Protective monitoring and intrusion detection** • **Investigations**

These measures are outlined within **Personnel Security: Threats, Challenges and Measures**. Further details are also available in **A Good Practice Guide on Pre-Employment Screening** and **Ongoing Personnel Security: A Good Practice Guide**. All of these publications can be found online at www.cpni.gov.uk.

Risk management in personnel security

The use of appropriate personnel security measures can prevent or deter a wide variety of insider attacks, from staff fraud through to the facilitation or conduct of a terrorist attack. However, these measures can also be labour intensive and costly, and may result in delays to business processes such as recruitment or staff transfers, so it is important that they are implemented in a way that reflects the severity of the risk. Risk management provides a systematic basis for proportionate and efficient personnel security.

1 National security vetting is significantly different to the other controls in this framework; it is a centrally provided service which applies only to particular posts, where the need for vetting has been endorsed by the appropriate Government department.

Risk management is a continuous cycle of:

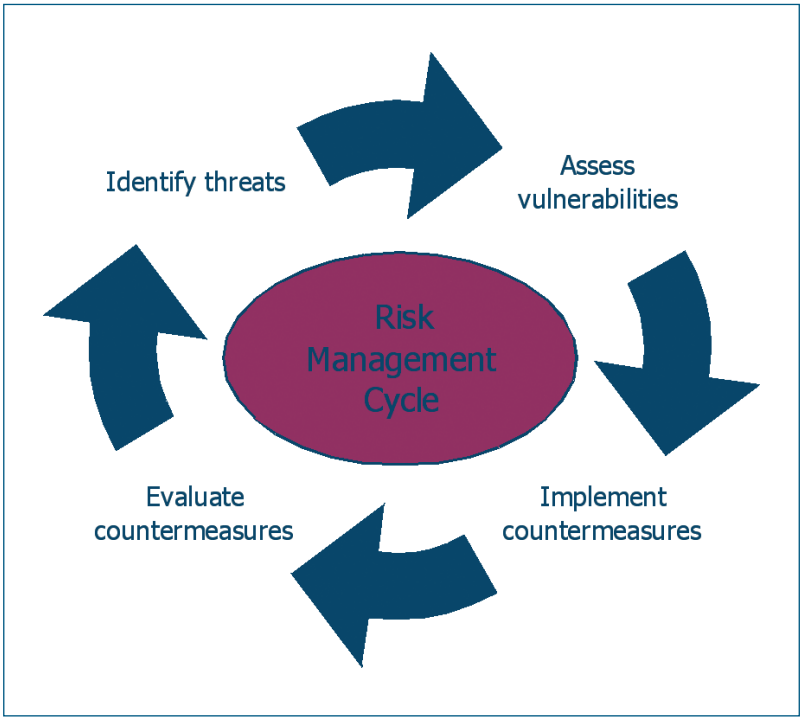
- **Risk assessment** - risks to the organisation are assessed in terms of the likelihood of an undesirable event taking place, and the anticipated consequences

- **Implementation** - security measures are identified and implemented to reduce the likelihood and impact of the undesirable event to an acceptable level

- **Evaluation** - the effectiveness of the countermeasures is assessed and any necessary corrective action is identified.

The cyclical nature of the risk management process ensures that each time a risk assessment is repeated, the implementation and evaluation phases are also reviewed. Much of the value of the risk management process is derived from the systematic exploration of threats, opportunities and countermeasures through engagement with the relevant parties. The discussions involved often produce a level of insight and shared understanding that would not otherwise be achieved.

This document concentrates on risk assessment, the basis for the rest of the risk management process. The guidance is not intended to be prescriptive. Security and human resources professionals will naturally wish to use an approach that best meets the needs of their organisations, bearing in mind the nature of the threat and the resources available to counter it.



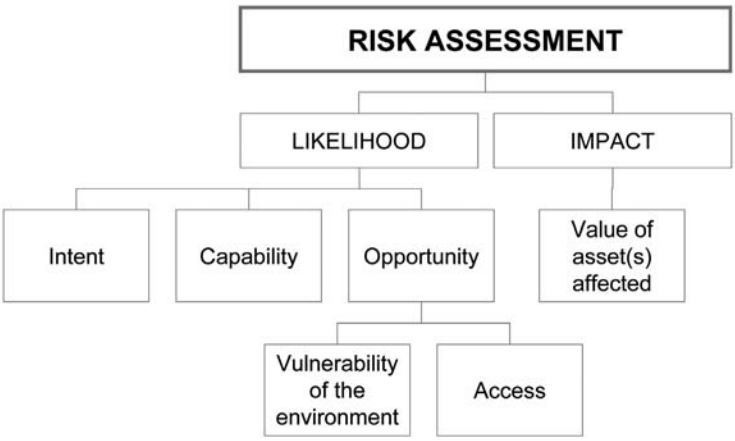
The Risk Assessment process incorporates the **Identify threats** *and* **Assess vulnerabilities** *stages of the Risk Management Cycle.*

Risk assessment: an overview

In this context, risk is usually understood to be the product of two factors: the likelihood of an event occurring, and the impact that the event would have. When each of these has been evaluated, they are combined to provide an overall measure of risk.

Likelihood can be further broken down into three factors: intent, capability and opportunity. Intent is a measure of the insider's determination to carry out the attack, while capability is the degree to which the insider possesses the skills, knowledge and resources to be successful in the attempt. Opportunity is a combination of the access that an insider has to an organisation's assets (by virtue of their role or position), together with the vulnerability of the environment (for example, an environment that is constantly supervised or monitored by CCTV cameras is less vulnerable to some insider threats than an environment which is not subject to these controls).

Impact should be considered in terms of the value of the assets affected and any wider consequences. For example, insider fraud can have both financial and reputational impacts.



Relative and absolute risk assessments

Some risk assessments involve quantitative measures that are absolute, while others use relative judgements. An absolute risk assessment process evaluates an event's likelihood in terms of probability and its impact in terms of numerical measures such as financial cost, or a delay in service delivery. By contrast, in relative risk assessments the likelihood and impact of the risks are simply compared, so that the risks can be listed in rank order.

It is often impossible to produce absolute risk assessments because of the difficulties involved in quantifying likelihood and impact. It is common to adopt semi-quantitative approaches that use scales for likelihood and impact such as 'Very low' to 'Very high'. In these approaches, there is an assumption that everyone involved with the assessment shares an understanding of terms like 'Very high'. The assessors themselves must be able to place the events on the scales in a way that reflects this understanding.

At the other end of the spectrum is an approach that makes no claims to assess the actual likelihood or impact of an event. Relative risk assessments aspire simply to a meaningful ordering of the likelihood, impact and hence risk of different events. This type of assessment will tell you which are the highest risks to the organisation, which are the lowest, and the spread between. This is sufficient for most personnel security risk assessment purposes.

Levels of risk assessment

There are three levels at which personnel security risk assessments can be conducted:

1. Organisation
2. Group
3. Individual.

The first examines and prioritises the types of insider threats that are of concern to the organisation as a whole, the second focuses on groups of employees with differing levels of opportunity to commit the threats, while the third deals with each employee on an individual basis.

Most practitioners will find it helpful to start with the simplest and highest level approach, the organisation level risk assessment, which provides a useful overview of the threats facing the organisation and an opportunity to review countermeasures in general. The group level assessment will require a greater commitment of time and effort, but can yield significant insight into the groups of employees that give most cause for concern and the proportionate application of countermeasures within the organisation. The individual level assessment is the most labour intensive of all, looking at every employee in turn to determine their combined opportunity and insider potential (i.e. threat and susceptibility).

The levels of risk assessment that you use will depend on the threats faced by your organisation and the nature of the workforce. It is important that you understand the way in which the three approaches support different types of decision. For example, if the organisational risk assessment reveals that there is a negligible threat to the organisation from an insider bringing a bomb into the building, this may rule out the need for baggage checks on entry to the site. Alternatively, the group level assessment could reveal that certain employees, due to their role in the organisation, have regular access to highly confidential or sensitive information, and they may therefore require higher levels of supervision in the office. If, at the individual level, a particular employee is considered to have high insider potential and a high level of opportunity, then an individually tailored risk management plan might be required.

Conducting personnel security risk assessments

Personnel security risk assessments are most effective when they are an integral part of a risk management process. This helps to ensure that the assessment actually translates into action.

Best results are achieved when the assessment team comprises:

- Staff from the human resources and security teams.
- Individuals with deep knowledge of particular employee roles (e.g. IT managers for IT roles).
- A trusted external contact to provide an alternative perspective and challenge received wisdom.

Some organisations have found that employees enjoy participating in discussions about the levels of access associated with different posts and the specific actions that post-holders could carry out. These organisations report that their assessments have benefited from this engagement in the organisation and group level assessments.

The risk assessment process should be highly interactive, with significant use of structured group discussions, or workshops. The value of these discussions can be enhanced significantly by a skilled chair or facilitator and by the use of visual aids. Enlarged reproductions of the charts and tables at Annex C, together with sticky notes or marker pens will help you to increase participation, obtain information from participants and to capture that information effectively.

The organisation level risk assessment

The organisation level risk assessment identifies the range of insider threats that an organisation faces and prioritises these in terms of their likelihood and impact. This simple relative risk assessment delivers an agreed, shared understanding of the insider risks to an organisation. As such, it provides a valuable foundation for the implementation of personnel security measures.

The results of the organisation level risk assessment should be recorded in a table with the following column headings:

Insider threat	Likelihood (1-5)	Assumptions (likelihood)	Impact (1-5)	Assumptions (impact)	Risk priority (1-4)	Countermeasures		
						Existing	Sufficient?	New

The table will be populated as the risk assessment progresses, step by step. At the end of the process, the table will provide a record of the insider threats faced by your organisation.

Step one: Identify the potential insider threats

Step 1	Step 2		Step 3	
Insider threat	Likelihood (1-5)	Assumptions (likelihood)	Impact (1-5)	Assumptions (impact)
e.g. Employee introduces a virus into the key IT system				
e.g. Employee brings an explosive device into the building				

The first step is to identify the insider threats that face your organisation, and to record them in the first column of the table. You may find the list of insider threats at annex A helpful. Each threat should take the form of an employee doing something that exploits their access to the organisation for unauthorised purposes.

It is essential that the threats are very carefully defined if the risk assessment is to produce useful results. Consider the following points:

- Range

The threats that you define should include the full range of unauthorised insider activity facing the organisation, including (but not limited to) physical attacks, abuse of intellectual property, and unauthorised disclosure of sensitive information.

- Definition of an insider

Remember that an insider is somebody who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes. It is easy to be distracted by thoughts of accidental damage, or of what could be done by strangers passing your building. These issues might warrant a separate risk assessment, but both fall outside the scope of this exercise.

- Level of detail

The threats should be defined at a level of detail that allows you to consider countermeasures for each one. Very broad threat definitions such as 'bombs' or 'leaks' are insufficient, because they do not contain enough information to make the responses meaningful. On the other hand, very narrow definitions can result in a large, unmanageable number of insider threats from which the added insight gained from each threat then becomes smaller.

Step two: Assess likelihood

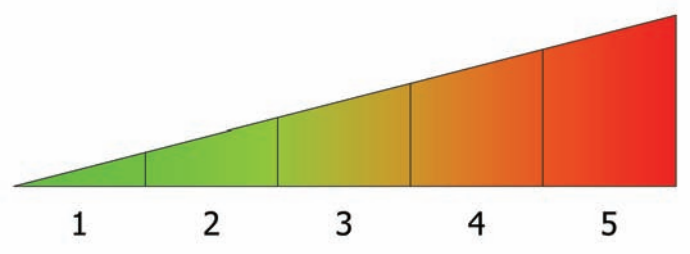
Step 1	Step 2		Step 3	
Insider threat	Likelihood (1-5)	Assumptions (likelihood)	Impact (1-5)	Assumptions (impact)
e.g. Employee introduces a virus into the key IT system	2	System administrator rights required to overcome protection		
e.g. Employee brings an explosive device into the building	1	Device would be carried in a bag		

Once the list of threats is complete and the definitions are clear, the next step is to consider how likely it is that each threat will occur, and to record this under the 'Likelihood' heading in the table.

It is important to focus on likelihood alone - if you are familiar with risk assessment, you may be tempted to consider other factors such as impact. In the CPNI's experience, assessments of impact and likelihood are most effective when they are done independently.

Rather than trying to predict probabilities with great precision, the aim of this part of the assessment is to establish the relative likelihoods of the threats, ranging from 1 (least likely to occur) to 5 (most likely).

It may be helpful to take a look at the list of insider threats, make a rough assessment of which is most likely to occur, and assign it a likelihood of 5; then identify the one that is least likely to occur, and assign it a likelihood of 1. This will provide reference points and help with consistency when evaluating the remaining threats on the same scale.



As you decide on a likelihood value for each new threat, the threats you have already assessed may need to be shuffled up or down the scale, depending on whether they are more or less likely than the new one. This reshuffling will continue until the relative likelihood of all the threats has been agreed.

In deciding the likelihood of each threat, it will be necessary to make some assumptions. For example, if you use recruiting agencies, your assumptions about the agency's compliance with its contractual recruiting agencies will affect your judgments on the likelihood of an insider attack. This assumption, and all others that influence the decision about likelihood, should be recorded in the 'Assumptions (likelihood)' column of the table. This will be useful when considering countermeasures later, and it increases the transparency of the risk assessment process.

Timescales are also important when thinking about likelihood. A threat may not occur within one year, but could occur within three years. If any assumptions are being made with regard to timescales, they should be applied consistently to all threats.

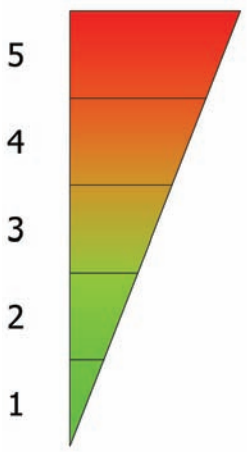
Other points to bear in mind when considering likelihood include:

- How realistic is it that your organisation will be a target for this type of attack?
- Has your organisation been subject to this kind of attack before? This confirms the relevance and feasibility of the threat but not necessarily the future likelihood. Equally, the absence of a threat in the past does not mean that it will not happen in the future.
- What is the current security situation in your industry?
- Do your employees have the kind of expertise required to conduct the attack?
- How effective are your contingency plans and existing countermeasures?

Step three: Assess impact

Step 1	Step 2		Step 3	
Insider threat	Likelihood (1-5)	Assumptions (likelihood)	Impact (1-5)	Assumptions (impact)
e.g. Employee introduces a virus into the key IT system	2	System administrator rights required to overcome protection	2	Loss of service for 24 hours
e.g. Employee brings an explosive device into the building	1	Device would be carried in a bag	5	<50 deaths

Impact is assessed in a similar manner to likelihood, using a relative scale of 1 (lowest impact) to 5 (greatest impact).



Again, make a rough assessment of the insider threat with the lowest impact (1) then assign 5 to the threat with the highest impact.

Although the scale is relative, it should be based on factors that are meaningful to your organisation, such as:

- the number or importance of sites affected
- injuries or fatalities among employees or the public
- financial losses
- reputational damage
- time required for business to recover
- adequacy of contingency plans and existing countermeasures.

The assumptions that you make about these – and other – factors affecting the impact value should be recorded in the ‘Assumptions (impact)’ column of the table.

As with likelihood, determining the impact value is an iterative process. The existing threats will need to be reviewed and reshuffled each time a new threat is considered, until those involved agree on the values assigned. At that point, the relative impact of each threat should be recorded under ‘Impact (1-5)’ in the table.

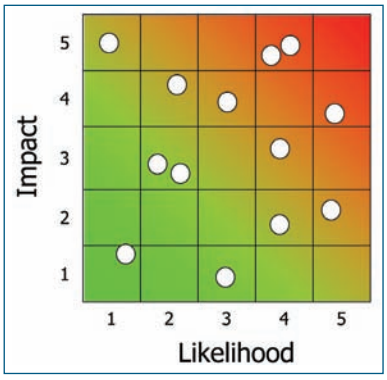
Step four: Determine the risk priority

Step 1	Step 2		Step 3		Step 4
Insider threat	Likelihood (1-5)	Assumptions (likelihood)	Impact (1-5)	Assumptions (impact)	Risk priority
e.g. Employee introduces a virus into the key IT system	2	System administrator rights required to overcome protection	2	Loss of service for 24 hours	2
e.g. Employee brings an explosive device into the building	1	Device would be carried in a bag	5	<50 deaths	4

The likelihood and impact values can now be used to determine the risk priority of each threat.

It may be tempting to do this by multiplying the likelihood and impact values for each threat, giving a value that – if low – can be taken to indicate that the threat is of little concern, and – if high – as an area where countermeasures should most urgently be directed. Unfortunately, this will produce a similar numerical result for a threat with a low likelihood and high impact, as a threat with high likelihood and low impact. Most organisations agree that this is not a sensible result.

The implementation of countermeasures is likely to be swayed more by either likelihood or impact, and the degree to which this applies may even differ for individual threats. The next step is to transfer the threats to a matrix combining the values you have assigned for likelihood and impact.

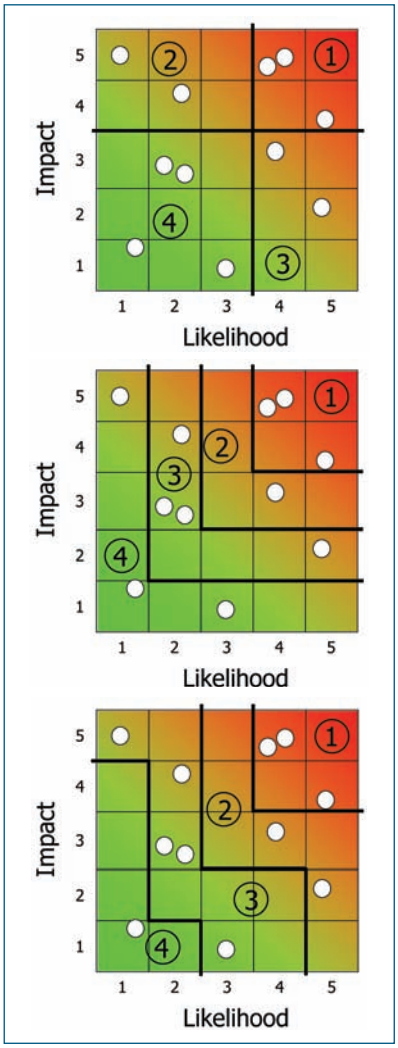


The risk matrix gives a picture of the risk assigned to each threat as a result of the likelihood and impact assessments. This is an important opportunity to look again at each threat and its associated assumptions, to ensure that it appears in the right place on the matrix, relative to the other threats.

It is easier to see in this format that a certain threat may have a slightly greater impact than one that has been placed above it on the matrix - or is less likely than one that appears to the left. In these cases, the threats should be shuffled to a more realistic position, although it would be unusual for any major alterations to be necessary at this stage.

Note that, as the threats are repositioned in the matrix, you should record any new assumptions being made about likelihood or impact, or alter the existing assumptions.

Once the positioning of the threats on the matrix is complete, they can be prioritised. The threats in the top right corner of the chart, with the highest likelihood and the greatest impact, will need to be urgently addressed (i.e. they are priority 1), while those in the bottom left corner, which have the lowest likelihood and least impact, can be addressed as a lower priority (e.g. priority 4, on a 4 point scale).



The prioritisation of threats is a flexible process

In practice, a four point priority scale works well for most organisations, but the scale can be designed to meet particular needs. For instance, it might be more appropriate to use a three point scale, if your organisation is used to a 'traffic light' system, where red signifies an urgent issue, green indicates that there is little to be worried about, and amber is between the two.

Alternatively, dividing the matrix into five or more priority areas will provide greater precision, but may take longer to achieve and result in too much detail for the number of threats involved. You should always bear in mind that the assessment cannot be highly precise; it is important that you do not seek to differentiate risks in a way that assumes greater precision than is actually achievable.

The risk matrix gives a clear graphical representation of the relative severity of the threats facing your organisation. Any method for dividing the matrix is therefore valid, as long as it provides clear priorities for action, which everyone involved in the risk assessment can agree upon. A number of possible prioritisation schemes are shown on the left.

Whatever scale you choose, there is usually no argument about which sectors of the risk matrix should be identified as the highest and lowest risk priorities. It is often much more difficult to prioritise the other sectors. The answer depends on whether you consider likelihood or impact to be the greater driver, and while it may prove very difficult to decide, it is worth persevering because this will help you to make decisions about directing your resources.

Once agreed, the risk priority relating to each threat should be inserted into the appropriate column in the risk assessment table.

Step five: Consider countermeasures

Note: This step is conducted in more detail during a group level risk assessment. If you intend to do a group level assessment then you may not want to complete these steps of the organisation level approach. However, a relatively quick consideration of countermeasures may be worth doing, even if you subsequently increase the level of detail in a group assessment.

Step 5		
Countermeasures		
Existing	Sufficient?	New
Anti-virus protection	• System can be suspended by individual employees • Personal USB disks can be connected to the organisation's computers	• Introduce a two person rule for suspending anti-virus protection • Bar USB ports on computers
Random bag searches conducted during the day	• They are not conducted at night • Compliance with the random bag search system is not audited	• Introduce random bag searches out of hours • Introduce a bag search audit process

Starting with the most urgent threat in risk priority 1, list in the 'Existing' column all countermeasures currently in place that help to mitigate that threat.

As a primary check, look at each countermeasure in turn and decide whether or not it is working sufficiently. For example, if one of your threats is that a bomb could be brought into your building, then one of your countermeasures might be a system for X-ray screening bags at the front door. Questions you might want to ask about this countermeasure include the following:

- Have your security staff had appropriate training to tell suspicious objects from innocent items?
- What is the likely detection failure rate, based on your audits and tests?
- Is there a backup X-ray machine in case the main machine fails?

Use the 'Sufficient?' column to record any doubts and the 'New' column to list the steps required to resolve them.

Finally, review all the countermeasures that you have listed in relation to the threat. Decide whether they work well enough together to contain the risk at an acceptable level, by limiting either the likelihood of the threat or its impact. Once again, record any doubts or gaps in the 'Sufficient?' column, and then use the knowledge of those involved, and the advice of experts, if necessary, to determine what new countermeasures should be implemented. List the new countermeasures in the 'New' column. It is important to ensure that ownership of any new countermeasures is clarified at this stage.

When you have reviewed the countermeasures for all threats in risk priority 1, repeat the process for each of the lower priority threats until all of the threats and countermeasures have been evaluated and the risk assessment is complete.

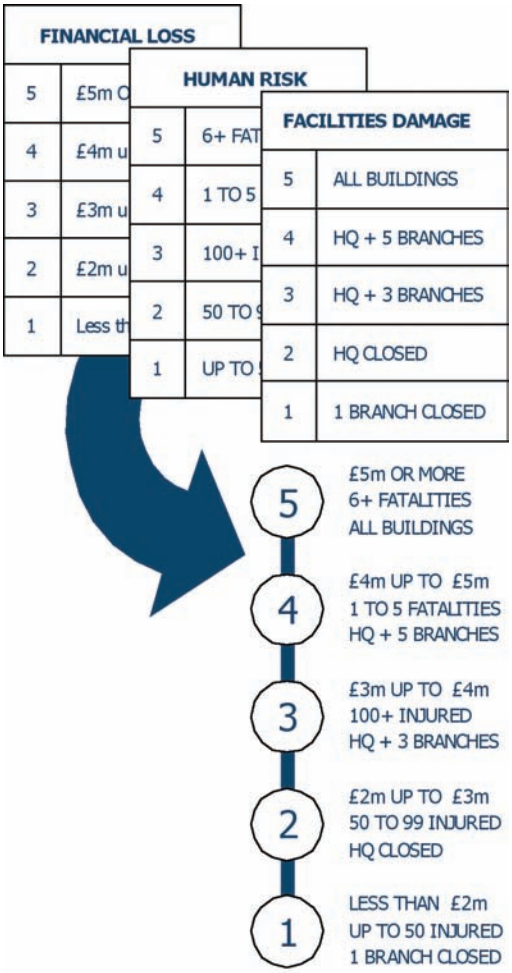
Step six (optional): Creating an absolute scale for impact

For most organisations, this is an optional step, but it is useful if you need further justification or quantification of the cost benefit of personnel security countermeasures.

Using the information recorded in the table, you will be able to review the impact values and assumptions associated with each threat, and by reviewing the factors that have resulted in one threat being assigned a higher or lower impact than another, extract the rules that drove the assessment of impact.

In each case, ask what has caused the threat to be assigned an impact value of 1, 2, 3, 4 or 5? If it is financial loss, then what exactly is the assumed loss? If it is human impact, then what loss of life or how many casualties are involved? If the guiding factor is the damage to your organisation's facilities, find a way to quantify it.

If, for example, you have assigned an impact value of 5 to a threat which you assumed would incur a loss of £500,000, and an impact value of 1 to a threat with an assumed loss of £10,000, you will be able to use this information to derive an absolute scale for threats involving financial losses. Similarly, if you have assumed that one threat will result in no casualties, while in assigning the impact for another you have assumed ten fatalities, then you will have an absolute scale for threats where human life is at risk. Note that the scales need not be linear; they can be exponential, or their values may vary irregularly.



This is a difficult task, particularly if your impact assessments involve many assumptions. It may help to start by reviewing all the threats that have a primarily financial loss, using these to create one absolute impact scale, and then repeating the exercise for threats involving casualties or loss of life to generate a second absolute impact scale. You can repeat this exercise as often as necessary, generating a number of absolute scales for different types of impact, before finally placing them alongside each other to obtain a combined scale of absolute impact. The benefit of this approach is that it removes any requirement to attempt making judgements which equate injury and loss of life with financial loss.

This step has an added benefit of checking the consistency of the judgments contained in your risk assessment. As you review the reasoning behind your impact assessments, you may well decide that, on reflection, some of them should be changed.

Next steps

Risk assessment includes the **identify threats** and **assess vulnerabilities** stages of the Risk Management Cycle. The remaining two stages are **implementation**, which involves putting the new countermeasures identified by the risk assessment into operation, and **evaluation**, during which the effectiveness of the countermeasures is reviewed. The lists of assumptions made during the risk assessment will prove particularly useful during this evaluation.

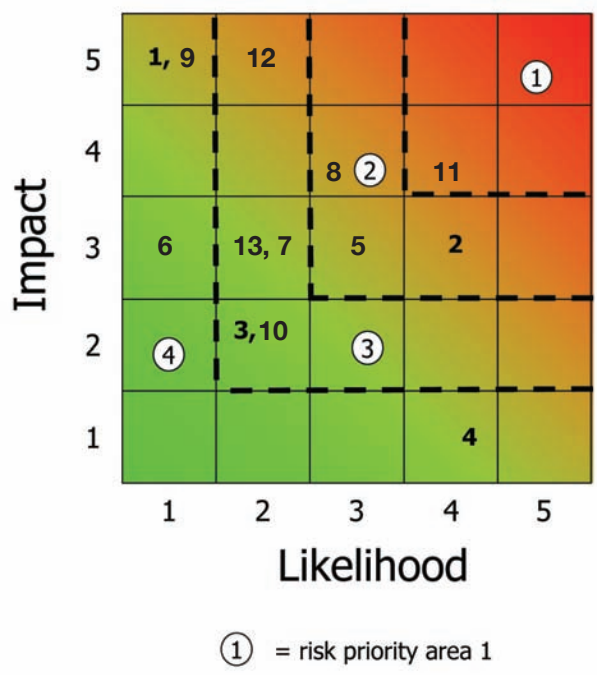
Depending on how much time has passed since the risk assessment, the evaluation stage should also show that the threats identified have moved either further to the left of the risk matrix, indicating a reduced likelihood, or further down the matrix, showing that the impact has been reduced as a result of the countermeasures you have introduced. It is worth bearing in mind, however, that factors outside your control, such as the current threat level, or economic, political and social issues, may also have an influence. The same factors are likely to introduce new threats to be addressed in future risk assessments.

If you are working with relative likelihood and impact scales (i.e. you do not complete Step 6), then your ability to report reductions in risk is more limited. For instance, imagine that you introduce a new control that reduces the likelihood of every threat in your assessment by the same amount. In this case, none of them will move because their relative likelihoods would stay the same. This situation is very unlikely and you will usually be able to record some movement in the relative likelihood or impact of a risk due to your intervention. But, the use of independent scales for assessing opportunity and impact does increase your ability to assess and communicate risk reduction in terms that are meaningful to decision makers (for example, a reduction in anticipated absolute costs).

Organisation level risk assessment case study:

Risk matrix

Threat No.	Threat scenario
1	Employee brings a bomb into the building and it detonates
2	Employee passes information to a third party (facilitation of fraud)
3	Employee introduces a virus into the key IT system
4	Employee (acting alone) transfers a small amount of funds eg. <£10,000 to an unauthorised account
5	Employee helps a third party gain access (obtaining commercially sensitive information with a key logger device)
6	Employee attacks staff (with a knife)
7	Employee reveals the end of year results ahead of schedule (to the press)
8	Employee passes customer details to an individual associated with an extremist organisation or organised crime
9	Employee helps a third party gain entry (brings bomb into the building)
10	Employee carries out a Denial of Service (DoS) attack on an IT system
11	Employee discloses security information, which leads to theft (eg. cash centre/cash in transit)
12	Employee drives a bomb into the organisation's underground car park
13	A group of employees (2+) colluding to authorise illegitimate payment



Risk table

Threat No.	Threat scenario	Likelihood: Scale 1-5	Likelihood Assumptions	Impact Scale: 1-5	Impact Assumptions	Risk priority
1	Employee brings a bomb into the building and it detonates	1	- Random bag searches are conducted	5	- < 50 deaths	4
2	Employee passes information to a third party (facilitation of fraud)	4	- Information passed includes credit card, bank account and customer details for multiple customers - A large number of employees have the opportunity	3	- Facilitation of large level fraud (> £100,000 loss) - High impact on reputation due to the number of customer affected	2
3	Employee introduces a virus in the key IT system	2	- Virus protection mechanisms in place - Sys Admin rights required to circumvent virus protection	2	- Data corruption - System down for 24 hours - Operations are affected - Some reputational damage - Back up systems in place	3
4	Employee (acting alone) transfers a small amount of funds eg. <£10,000 to an unauthorised account	4	- No counter-authorisation requirements in place - Many employees have the opportunity	1	- Loss of < £10,000	4
5	Employee helps a third party gain access (obtaining commercially sensitive information with a 'key logger' device)	3	- Lack of vigilance and inadequate access controls - Significant commercial espionage threat	3	- High reputational damage	2
6	Employee attacks fellow staff with a knife	1	- Historically, this threat has only been external (i.e. not from employees) - Random bag search (not personal search)	3	- Up to five people injured	4
7	Employee reveals end of year results ahead of schedule (to the press)	2	- Restricted personnel know the information - Limited precedent (not happened in years)	3	- High reputational damage - Dent in shareholder value but a short-lived problem	3
8	Employee passes customer details to an individual associated with an extremist organisation or organised crime	3	- Employee unaware of the nature of the organisation they are passing information to, and the severity of their disclosure	4	- Revealed to press/ public - Customers targeted, possibly killed - High reputational damage	2
9	Employee helps a third party gain entry (brings bomb into the building)	1	- Few people have the expertise to construct an improvised explosive device (IED) - No precedent	5	- Same as other person borne improvised explosive devices (PBIEDs), i.e. < 50 dead	4
10	Employee carries out a Denial of Service (DoS) attack on an IT system	2	- Lack of technical knowledge - Historically an external threat - Technical information available to enable this to be carried out - Back up services	2	- System down for 24 hours - Reputational impact - Minimal loss of customers - Loss of customer confidence	3

Threat No.	Threat scenario	Likelihood: Scale 1-5	Likelihood Assumptions	Impact Scale: 1-5	Impact Assumptions	Risk priority
11	Employee discloses security information (which leads to theft, e.g. cash centre/cash in transit)	4	- Precedent - Clear evidence of threat - Easy to do	4	- ≥ £1,000,000 loss - Nobody injured - High reputational damage	1
12	Employee drives a bomb into the organisation's underground car park	2	- Access to car park - Random vehicle searches - Ineffective search procedures	5	- ≤ 200 people killed or injured - Major structural damage resulting in the building being out of use long term and possible relocation of premises	3
13	Group of employees (2+) colluding to authorise illegitimate payment	2	- Dual authorisation required	3	- > £100,000 loss - High reputational damage	3

The group level risk assessment

The group level risk assessment provides a lot more insight into the management of personnel security risks within your organisation. In particular, this assessment shows how countermeasures should be applied to particular roles; it does not assume that measures are applied blanket-fashion across the whole organisation.

The assessment takes as its starting point the threats identified during the organisation's level assessment. Consideration is then given to the groups of employees that have the greatest opportunity to carry them out, concentrating mainly on levels of access to the organisation's assets, including information, materials, systems, buildings and people.

As with the organisation's risk assessment level, the group level should be carried out by a team comprising primarily human resources and security managers, with contributions as appropriate from other experts.

The results of the group level risk assessment should be recorded in a table with the following column headings:

Insider threats in priority order	Group with high opportunity	Reasons	Access	Vulnerability assessment	Countermeasures		
					Existing	Sufficient?	New

As with the organisation's level risk assessment, the table will be populated as each step of the risk assessment is completed, providing a record of the groups of employees in your organisation best placed to carry out the threats, the factors that provide them with that level of opportunity, and the countermeasures required.

Step one: Identify and prioritise the insider threats

Step 1				
Insider threats in priority order				
Employee reveals commercially sensitive information				

The assessment should begin by identifying and prioritising the insider threats facing the organisation, as described in the organisation level risk assessment, and listing them in the first column of the group level risk assessment table in risk priority order.

Step two: Perform initial identification of groups with the most opportunity

Step 1	Step 2			
Insider threats in priority order	Group with high opportunity			
Employee reveals commercially sensitive information	Senior managers			
	IT administrators			

The purpose of this step is to identify the subset of employees on which the risk assessment should concentrate. The assessment should be relatively quick; a more detailed assessment will follow in subsequent stages.

The approach is to look at each threat in turn, and determine which groups of employees in your organisation have the greatest opportunity to carry it out. You should base these judgements on:

1. The extent to which the employees, routinely or potentially, have access to the assets under threat.
2. The vulnerability of the environment to an attack by an employee.

When deciding which groups have opportunity to carry out threats, it is likely that the groupings will to some extent reflect job roles within the organisation. For example, if the threat under consideration concerns the compromise of IT systems, then one group of employees with high opportunity is likely to be the IT Systems Administrators, due to their unsupervised systems access and high level passwords. However, some groupings will not correlate quite so directly to organisational job titles, so it is important to think about all employees carefully, and not be constrained by job titles. Depending on the degree of detail that you wish to pursue, you may find that this stage of the assessment becomes a significant research and analysis exercise, involving the collation of information about the organisation's employees and the roles that they perform. A series of interviews with managers or supervisors may be helpful.

Once you have established which groups have the greatest opportunity, you should record these in the risk assessment table.

Recording the size of the groups

It is useful to make a note of the approximate size of the group – again, this may require some research to establish and the involvement of Human Resources (HR) will be essential. It is reasonable for some groups to be quite small, but if a group is very large, it may mean that there is room to be more precise in how the opportunity of that group is defined.

- Large groups and likelihood

A very large group may affect the likelihood (decided during the organisation level risk assessment) of the threat under consideration. For example, the likelihood that an insider will corrupt a central database might increase if you now find that a very large group of employees has the opportunity to do so. If this is the case, it is worth amending the risk matrix.

- Large groups and impact

A very large group may also affect the impact of a threat. For example, the theft by an employee of a laptop computer may have a low impact on the organisation, but the cumulative effect of a large group of employees doing the same thing may have a significantly greater impact. Once again, it is worth reviewing the organisation level risk assessment to see if this should be reflected in the risk matrix. Generally, it is more likely that your countermeasures will change as a result of increased impact than as a result of increased likelihood.

Step three: Record the nature of the opportunity

Step 1	Step 2	Step 3		
Insider threats in priority order	Group with high opportunity	Reasons		
Employee reveals commercially sensitive information	Senior managers	• Senior managers see the greatest volumes of commercially sensitive information		
	IT administrators	• IT administrators could gain unauthorised access using their IT skills, although it would be hard to achieve undetected		

In the ‘Reasons’ column, record the factors that give the groups a high level of opportunity to carry out the threat under consideration. These reasons will have been discussed in Step 2 but it is important to record them.

The points listed here will help drive the countermeasures that need to be considered to mitigate the threat, so it is important to include enough detail. It would be possible for the reasons in every case to

be ‘knowledge and access’, but this will not provide enough information for meaningful countermeasures to be implemented.

Step four: Score opportunity

Step 1	Step 2	Step 3	Step 4	
Insider threats in priority order	Group with high opportunity	Reasons	Access	Vulnerability assessment
Employee reveals commercially sensitive information	Senior managers	• Senior managers see the greatest volumes of commercially sensitive information	H	H
	IT administrators	• IT administrators could gain unauthorised access using their IT skills, although it would be hard to achieve undetected	M	M

In this step, access and vulnerability are assessed more systematically, and scored using standardised scales for easy comparison. The scores are then used to provide an overall measure of opportunity to carry out a threat.

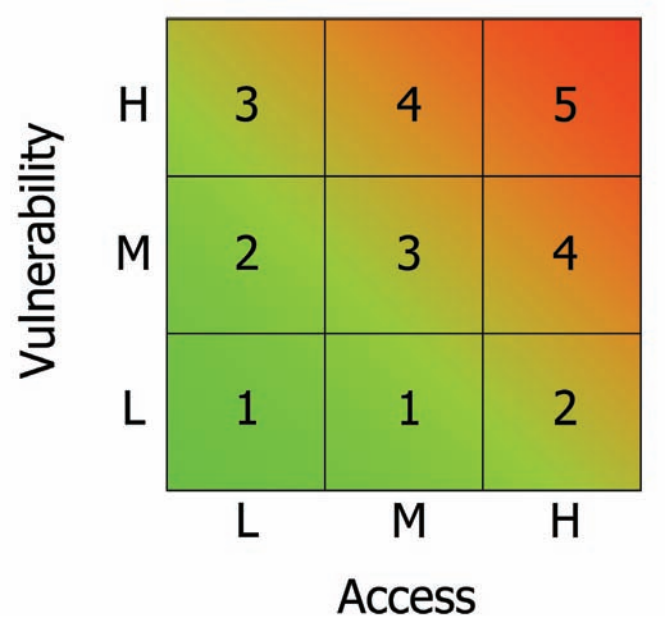
When considering the access of your employees, you will need to decide the extent to which, routinely or potentially, employees in the organisation have access to specific assets. We suggest that you use the simple scale that follows.

Access score (H,M,L)	**Definition**
High	Regular access that is consistent with the role
Medium	Occasional access
Low	Opportunistic access

For the vulnerability assessment, we recommend that you use the vulnerability assessment table at Annex B. Please note that this table is designed to support assessments of overall vulnerability for an organisation; not all of the vulnerability dimensions that it presents will be relevant for assessing the vulnerability of the workplace. Consequently, you will need to decide which dimensions to consider, before using the scales to make your assessments. We recommend that you judge the vulnerability of the workplace on a High, Medium, Low scale.

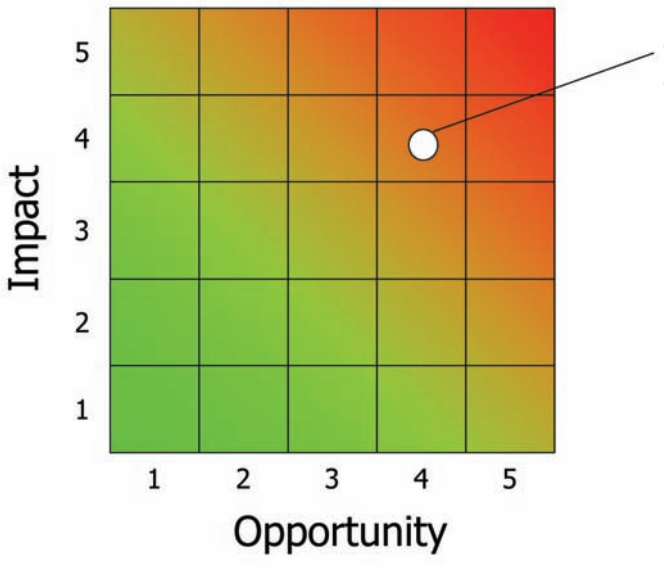
At this stage your employee groups will have been assessed for their access and the vulnerability of their working environments. You now need to combine these scores to produce overall measures of opportunity. We suggest that opportunity is scored on a 1-5 scale.

You will need to decide how you want to translate the access and vulnerability scores into opportunity scores. We suggest that you draw a matrix like the one below and then decide where to place the numbers 1, 2, 3, 4, and 5 based on the combinations of access and vulnerability. The matrix below presents one possible scoring scheme.



The opportunity score associated with each combination of access and vulnerability is shown in each cell.

The scores provide a useful summary of the assessment and help you to rank employee roles in terms of opportunity to carry out specific threats. These scores can also be plotted on a graph against the impact of the threats - see below. The threat-group combinations appearing in the top right hand corner of the chart will be those posing the greatest overall risk to your organisation.



e.g. IT administrator sabotages central database

Step five: Consider countermeasures

Step 3	Step 4	Step 5		
Threat	Group with high opportunity	Countermeasures		
		Existing	Sufficient?	New
Employee reveals commercially sensitive information	Senior managers	• Confidentiality agreements • Protective marking scheme • Numbered copies	• Firewall will not detect transmission of protectively marked documents • Security staff tend to conduct fewer bag searches for senior managers	• Upgrade the firewall to block transmission of protectively marked documents • Audit compliance with the bag search policy
	IT administrators	Computer audit	• The computer audit system will record but not prevent unauthorised access	• Introduce a live alert and warning system to flag unauthorised information access

As with the organisation level risk assessment, start by listing in the 'Existing' column all countermeasures currently in place that help to prevent the groups from carrying out the threat under consideration.

Then, look at each countermeasure in turn and decide whether or not it is working sufficiently. If your threat is defined as "Insider introduces virus into primary computer system" and the group with the most opportunity is your IT agency staff, then your existing countermeasures may include the pre-employment screening processes you have specified in the contract between your company and the IT recruitment agency. But without an additional process – auditing the implementation of that screening – it is unlikely that the contract alone will be a sufficient countermeasure.

Use the 'Sufficient?' column to record doubts about any gaps in the countermeasures and the 'New' column to list the steps required to resolve them.

Finally, review all the countermeasures that you have listed in relation to the group having greatest opportunity, and decide whether they work sufficiently well together to limit opportunity and so maintain the risk at an acceptable level. Once again, record any doubts in the 'Sufficient?' column, and then use the knowledge of the group, and the advice of relevant experts if necessary, to determine what new countermeasures should be implemented. List these in the 'New' column.

When you have decided which groups have high opportunity to carry out the threats in risk priority 1, and addressed the issue of countermeasures in each case, repeat the exercise for all remaining risk priorities.

If the time available for the group level risk assessment is limited, you may choose to tackle only the threats in the higher risk priorities, but it is important to remember that there may be some factors that only becomes evident during the group level risk assessment – such as very large group size – which affects the prioritisation of threats, and may be missed if the assessment is not completed.

Group level risk assessment case study:

Assessment of opportunity for selected insider risks

At the group level address the threats in your highest priority areas first. The table below looks at a selection of threat examples from a range of priority areas.

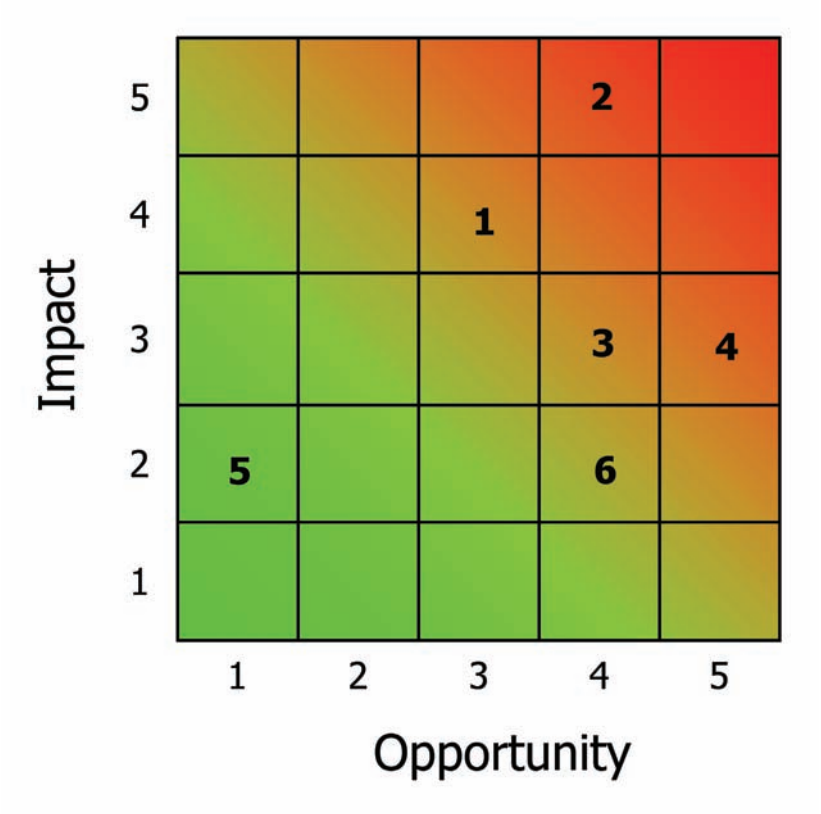
Insider Threat	Risk Priority Area	Which groups have high opportunity?	Reasons	Access (H,M,L)	Vulnerability (H,M,L)
Employee discloses security information (11)	1	Security employees (management) [15]	- These employees are well placed to identify security vulnerabilities that can be exploited	H	M
		Security employees (operational) [15]	- These employees are well placed to identify security vulnerabilities that can be exploited	M	M
Employee reveals end of year results ahead of schedule (to the press) (7)	3	Senior management [20]	- Access to information; limited circulation; existing contacts in media	H	M
		Printing (select group) (internal/ external) [25]	- Access to information that is not widely available	H	H
Employee carries out a Denial of Service (DoS) attack on an IT system (10)	3	IT staff [100] Ex-IT staff in the last two years [75]	- IT staff have the skills and the opportunity. - Knowledge of system - Knowledge of systems' vulnerabilities	M	L
Employee introduces a virus in the key IT system (3)	3	IT staff (with appropriate access and admin rights) [30] IT contractors [10] Ex IT staff in the last 2 years [75]	- These IT staff have the skills and the opportunity (their Sys Admin rights give them the ability to suspend the virus protection mechanisms). - Knowledge of systems' vulnerabilities	H	M
Employee brings a bomb into the building and it detonates. (1)	4	All staff have significant opportunity but the following employee roles have greater opportunity than most: Contractors, IT engineers, Maintenance staff, Cleaning staff [total: 300]	- They work out-of-hours, when security checks are less frequent. - Bag searches are made on a random sample.	M	M
		Security guards [30]	- Opportunity to bypass security measures	M	H

Assessment of countermeasures

Assessment of opportunity for selected insider risks

Threat scenario	Group	COUNTERMEASURES		
		Existing	Sufficient?	New
Employee discloses security information (11)	Security employees (management)	- Security employees are subject to criminal record check - Some access controls - Security culture varies across the organisation	- Poor control over access to sensitive security information	- Refresh training on 'need to know' - Rotate personnel in key security positions - Introduce security culture self-assessment across the organisation
	Security employees (operational)	- Security employees are subject to criminal record check - Some access controls - Security culture varies across the organisation		- Refresh training on 'need to know' - Rotate personnel in key security positions - Introduce security culture self-assessment across the organisation
Employee brings a bomb into the building and it detonates. (1)	Contractors, IT engineers, maintenance staff, cleaning staff	Random bag searches (daytime) Lesser pre-employment screening checks for contractors	- Variable standards - Changed with alert status - Contractor screening insufficient	- Random bag searches at night - Explosives screening - Annual refresher training - Checks that are consistent with those for permanent staff with the same access levels
	Security guards	Random bag searches (daytime)	- Variable standards - Changed with alert status - Some security guards can bypass friends on duty without checks	- Introduce new audit system for random bag searches to increase compliance for security guards
Employee reveals end of year results ahead of schedule to the Press (7)	Senior management	- Documents are numbered and on limited distribution - Audit trail of emails. - Use of protective marking - Clear desk/need-to-know policy	- No restrictions on printing off emails or sending them to an external address	- Encryption of sensitive corporate information to mitigate the risk of external communication by email - Limit disaffected employees' access to sensitive corporate information - Promote an effective security culture - Prohibit cameras or mobile phones within the building
	Printing	- Confidentiality agreement in place - Documents are numbered and on limited distribution - Use of protective marking - Clear desk/Need-to-know policy	- Low compliance with clear desk policy. - No restrictions on printing off emails or sending them to an external address.	- Enforce clear desk policy - Reinforce security aspects of the contract with the printer - Encryption of sensitive corporate information to mitigate the risk of external communication by email

Threat scenario	Group	COUNTERMEASURES		
		Existing	Sufficient?	New
Employee carries out a Denial of Service (DoS) attack on an IT system (10)	IT staff	- CCTV - Supervision and natural surveillance by colleagues - Back up system in place	- CCTV does not give effective coverage of some key locations - No annual security appraisals or whistle-blowing systems to flag concerns	- Introduce a rule whereby no employee can be in the IT Server room unaccompanied. - Introduce a system to allow employees to raise concerns about co-workers
	Ex-IT staff	Automatic removal of IT privileges on return of staff ID card	Staff directory not updated immediately, increasing potential for social engineering attacks.	Brief staff on the need to extend personnel security to ex-IT personnel. Automate the process whereby staff details are removed from the staff database when they return their staff ID badge
Employee introduces a virus in to the key IT system (3)	IT staff (with appropriate access and admin rights)	- Anti-virus software - Software alerts from outside - Virus checking policies - CCTV	- Anti-virus software may be turned off by an employee with Sys admin rights - Auditing is retrospective and does not provide timely alerts and warnings	- Require counter-authorisation before anti-virus software can be suspended - Restrict the use of communication devices (e.g. USB sticks or CD ROMs) - Live monitoring of IT systems and warning of irregular activity
	IT contractors (with admin rights)	- Anti-virus software - Software alerts from outside - Virus checking policies - CCTV	- IT contractors sometimes employed prior to completion of pre-employment screening checks - Anti-virus software may be turned off by an employee with Sys admin rights - Auditing is retrospective and does not provide timely alerts and warnings	- Ensure that any IT contractor employed prior to completion of pre-employment checks is accompanied at all times. - Require counter-authorisation before anti-virus software can be suspended - Restrict the use of communication devices (e.g. USB sticks or CD ROMs) - Live monitoring of IT systems and warning of irregular activity



1. Security employee (operational) discloses security information
2. Security guard brings a bomb into the building
3. A member of the senior management reveals the end of year results ahead of schedule
4. A printing department employee reveals the end of year results ahead of schedule
5. A member of the IT staff carries out a Denial of Service (DoS) attack on the IT system
6. An IT contractor introduces a virus in the key IT system

Producing risk scores for employee roles

The group level approach starts with the insider threats to the organisation and then assesses the opportunity that employees have to commit those acts. The relationships between job roles and threats are therefore considered in detail. One major benefit of this is that countermeasures can be applied to job roles in a way that takes into account the types of threat that different employees might pose. However, the approach is very qualitative and makes no attempt to quantify the level of risk presented by particular job roles.

It is possible to conduct a more quantitative approach, instead of, or alongside the approach described above. This entails scoring the opportunity provided by a given job role and also the impact that could be achieved by an employee in that role. By combining these scores you can arrive at an overall assessment of the level of risk associated with a job role. The benefit of this approach is that job roles can be prioritised on the basis of these scores and countermeasures can be linked to thresholds in the scoring system. For instance, you might decide that any role scoring in the top ten warrants a criminal record check.

Many practitioners will find the results of this approach presentationally appealing and it can provide a relatively simple framework for decision making. However, there are two drawbacks:

1. It does not encourage detailed consideration of insider threats and the way in which the opportunity for these threats varies between roles. The impact that could be achieved in a given job role is usually based on an assumption as to the reasonable worst-case threat. For instance, it might be assumed that the reasonable worst-case threat posed by a financial controller is fraud, in which case the opportunity for the controller to facilitate, say a physical attack, would not be considered. The allocation of countermeasures is less precise and comprehensive using this approach.

2. In order to score opportunity and impact it is necessary to devise numerical scales that apply to the full range of job roles and threats under consideration. This is a significant challenge.

The individual level risk assessment

At the individual level, personnel security risk assessment seeks to examine the insider potential (i.e. malicious and susceptibility) of individual employees. Individual risk is the combination of an assessment of insider potential and the level of opportunity which exists for that individual, based on their role and access.

The process of carrying out an individual level risk assessment is considerably more complex than at the organisational or group level, most notably because it is technically much more difficult to assess intent and susceptibility and as yet there is no agreed or tried and tested method of doing this. In addition, seeking to conduct individual risk assessments across an organisation will be substantially more resource intensive. For these reasons, it is likely that relatively few organisations will employ this approach, although some may use individual level assessment for the small proportion of employees that fall in the highest risk group(s) or as a means of assessing the risk posed by an employee of concern.

CPNI is currently working on research into the behaviours and vulnerabilities associated with insider activity. The ultimate aim of this research is to assist with decision making with regards the insider risk at an individual level.

Glossary of terms

Asset	Any element, service, function or event that supports the Critical National Infrastructure. Assets can be physical entities such as people or equipment and non-physical entities such as networks and systems.
Critical National Infrastructure (CNI)	Those key assets of the national infrastructure, the failure or loss of which could cause severe economic or social damage and/or large scale loss of life. The national infrastructure is the underlying framework of facilities, systems, sites and networks necessary for the functioning of the United Kingdom and the delivery of the essential services upon which the UK relies.
Impact	The level of negative effect upon the UK's public health and safety, its economy, the essential services upon which it relies, public and commercial confidence, and the functioning of government, that can be expected to arise directly or indirectly if an asset is damaged, destroyed or disrupted by a terrorist attack or other malicious incident. The degree to which there are alternatives to the asset (i.e. the resilience of the CNI) will affect the level of impact.
Insider	An employee or contractor who seeks to exploit their legitimate access to an organisation for unauthorised purposes.
Insider opportunity	The feasibility of an employee conducting an insider attack on the basis of the access afforded by their organisational role and the vulnerability of the working environment.
Motivation	A combination of proven intent to attack and the attractiveness of the target in meeting the aspirations and aims of the adversary.
Personnel security	A system of policies and procedures, which seeks to manage the risk of staff or contractors exploiting their legitimate access to an organisation's assets or premises for unauthorised purposes.
Risk	The potential for loss, damage, disruption, death or injury, following an assessment of: • the likelihood (the combination of threat and vulnerability) that a malicious attack will occur affecting an asset; and • the impact of the malicious attack
Threat	The assessment of a terrorist or other malicious attacker's motivation and capability to attack an asset. The manifestation of the threat could take the form of one or more attacks or attempted attacks, either concurrent or simultaneous.
Vulnerability	Vulnerability is a characteristic of, or flaw in, an asset's design, location, protective security measures, process, or operation that renders it susceptible to, or offers the opportunity for, disruption or destruction, incapacitation, or exploitation by terrorists or other malicious actors. These characteristics may be found in infrastructure on which the asset is dependent.

Annex A – List of insider threats

This list is not intended to be exhaustive, but may be useful in generating discussion of threats relevant to the organisation.

ACCESS TO INFORMATION

Theft of information / intelligence

Disclose sensitive information

Disclose sensitive information to specific parties

Disclose sensitive information to the public

Existing data

Sabotage organisation data - falsify

Sabotage organisation data - destroy / remove

Misuse of information

Distribution to unauthorised eyes inside / outside the organisation

ACCESS TO IT SYSTEMS

Disclose IT system details

Disclose IT systems used and their capabilities to specific parties

Disclose source

Disclose the organisation's confidential sources to specific parties

Hack IT systems

Hack in to IT systems to copy information stored for further use

Hack in to IT systems to monitor use

Sabotage existing systems / data

Sabotage of existing systems - affect systems e.g. with viruses

Sabotage of existing systems - destroy systems

Sabotage of existing data - falsify

Sabotage of existing data - destroy / remove (e.g. with USB stick)

Bug telephone systems

Bug telephone systems to monitor use

Bug telephone systems to eavesdrop

Misuse of systems

Facilitating access of a third party to an IT system [record assumed impact in impact assumptions column]

Access forthcoming systems and developments

Access forthcoming systems and developments - destroy

Access forthcoming systems and developments - sabotage

Access forthcoming systems and developments - disclose to the public

Access forthcoming systems and developments - disclose to specific parties

ACCESS TO SITES, BUILDINGS, MATERIALS AND MECHANICAL SYSTEMS

Facilitate access of a third party to the building

Facilitate access of a third party to areas of the building e.g. through Fire Exits [record assumed impact in impact assumptions column]

Forge security passes

Give security pass to others

Facilitate access of a third party to information

Facilitate access of a third party to information [record assumed impact in impact assumptions column]

Theft of goods / materials

Theft/distribution of harmful materials (e.g. radiological material/weapons)

Theft and distribution of non-harmful materials (e.g. passports, driving licences, clean criminal records certificates).

Sabotage of goods / materials / building

Sabotage access points - to create weak areas

Sabotage storage facilities - to disrupt working practice

Sabotage storage facilities - to allow others access

Sabotage air conditioning units - to disrupt working practice

Sabotage air conditioning units - to cause casualties

Sabotage food and drink - to cause casualties

Sabotage walkways / lifts etc - to cause casualties

Sabotage post delivery system - to disrupt working practice

Disclose information about the premises and security systems

Disclose information about the building e.g. weaknesses (to specific parties)

Disclose information about the building e.g. weaknesses (to the public)

Disclose information about the security systems and measures in place (to the public)

Disclose information about the security systems and measures in place (to specific parties)

Direct attack on the building (e.g. explosives)

Direct attack on mechanical systems

Physical destruction of systems / files

Physically destroy systems (e.g. IT centre)

Physically destroy files (e.g. by fire)

Access to developed / developing technology

Access to developed / developing technology - destroy

Access to developed / developing technology - sabotage

Access to developed / developing technology - disclose to specific parties

Access to developed / developing technology - disclose to the public

Use of recording devices

Bring in and use recording devices / scanners / phreaking devices - disclosure of information

ACCESS TO PERSONNEL

Disclose sensitive information

Disclose info gathered verbally through informal discussion - to the public

Disclose info gathered verbally through informal discussion - to specific parties

Disclose information from potentially sensitive meetings - to the public

Disclose information from potentially sensitive meetings - to specific parties

Persuade others to gather / pass information (short term)

Build specific relationships with an aim to acquire specific knowledge (long term)

Force individuals to gather / pass information

Force individuals to gather / pass information under duress

Force individuals to gather / pass information through bribery

Recruitment of others – commercial espionage

Attack / threaten individuals / groups of personnel

Physically attack individuals

Physically attack groups of personnel

Conduct a mass casualty attack on employees

Violate the liberty of individuals / groups (e.g. hostage taking)

Threaten personnel

Annex B – Vulnerability scale

A vulnerability scale for protective security risk assessments is presented overleaf. The scale is normally accompanied by a scoring system. However, this method provides scores of overall vulnerability for an organisation. For personnel security, the relevance of the different dimensions of vulnerability will vary depending on the nature of the role and the organisation. Consequently, the scale is offered without the scoring system and we suggest that you use it qualitatively to inform your judgements about the vulnerability of the workplace.

Physical vulnerability

	A	B	C	D	E	F
Type of physical vulnerability **Fields A-F**	**Nature of site & perimeter (mainly related to vehicle threats)**	**Construction of building (mainly related to vehicle threats)**	**CBR – vulnerability to ingress & spread of CBR materials**	**Perimeter security systems (e.g. access control, intruder detection and CCTV systems)**	**Extent of control over building – public access & shared occupancy**	**Security & screening of visitors, mail, deliveries etc**
Potential indicators of HIGH vulnerability (Indicators likely to be supported by little evidence of strong security governance, policy and procedures)	• Single layer perimeter (e.g. external skin of building) • Proximity to public roads • High vulnerability to vehicle borne threats (e.g. traversable adjoining land), uncontrolled access and insufficient or permeable physical standoff measures • Critical components located near perimeter (i.e. minimal stand-off protection)	• Building design susceptible to progressive collapse or lack of structural redundancy • Heritage buildings – planning restrictions may limit possible enhancements • Significant use of glass • Exposed key structural elements	• Accessible air Intakes • Exterior shell of building relatively permeable: windows often open or poorly fitting; poor design of entrances	• Systems installed and/ or operated in an *ad hoc* manner, without clear concept of use • Inconsistent application, obvious gaps in coverage • Single layer and weak perimeter • Proximity to public ways • Critical components located near perimeter	• Multiple entrances - people and/or vehicles • Building for which public access is essential • Multiple occupancy • Many and frequent visitors • Un-zoned, i.e. unrestricted movement within building	• Visitor reception within body of building • Poor staff awareness re postal threats • Post-room in heart of building • Mail opened at desks without screening • *Ad hoc* visitors and deliveries accepted without question
Medium						
Potential indicators of LOW Vulnerability (Indicators likely to be supported by clear evidence of strong security governance, policy and procedures)	• Multi-layer perimeter • Significant stand-off between exterior of perimeter and critical components of site/building • Additional crash-proof measures (e.g. bollards, traffic restrictions) keeping unscreened vehicles at a distance; such continuous measures designed with a clear control strategy	• Building design not susceptible to progressive collapse • Glazing and cladding systems specifically designed to withstand blast and minimise fragmentation	• Inaccessible air intakes • Good HV AC (Heating, ventilation & air-conditioning system) system design, e.g. zoned, with advantageous pressure gradients, limiting spread of contaminants • Building relatively impermeable: e.g. windows sealed shut	• Robust systems providing capability that reflects concept of use • Security staff seen as key element of overall perimeter security system • Multi-layered perimeter and entrance arrangements Full height robust entry barrier	• Building controlled by occupying organisation • Unrestricted access limited to staff and trusted contractors • Visitors by appointment only; sponsored and escorted by staff; photo id checked • Building zoned to restrict movement	• Clear concept of operation; all screening systems meet clear requirements • Staff involved in screening trained and well motivated • All visitors screened at site perimeter; mail and deliveries screened off-site. • Visitors & deliveries always expected • Good staff awareness re postal threats

Personnel vulnerability

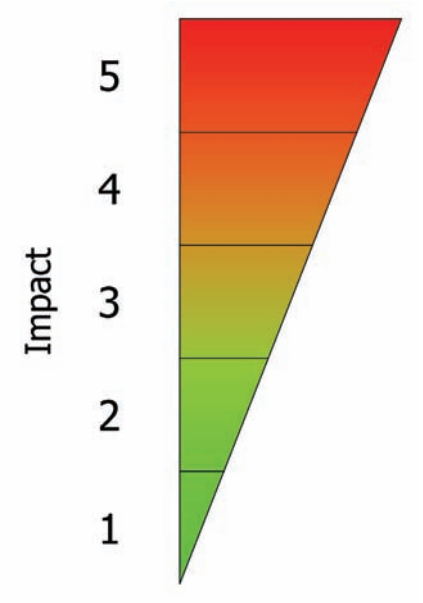
	A	B	C	D	E	F
Type of personnel vulnerability **Fields A-F**	**Personnel security risk assessment and audit**	**Pre-employment screening**	**Security culture**	**Monitoring and assessment of employees**	**Investigation practices and disciplinary procedures**	**Governance of personnel security**
Potential indicators of HIGH vulnerability	• A lack of routine personnel security risk assessment - poor understanding of which roles create the greatest exposure to risk across the organisation. • Personnel security measures are not always applied proportionately • No regular auditing of personnel security, measures against role requirements and standards	• Pre-employment screening practices are *ad hoc*. • Pre-employment screening for contractors and overseas staff are particular weaknesses • There is no effective auditing of those pre-employment screening checks performed by third parties. • There is no explicit risk-based justification for the use of national security vetting checks, which are carried out in isolation not as part of a managed personnel security regime.	• Good protective security is a low priority for management and staff. • Poor appreciation of the threats to the organisation. • Personnel security is not viewed as the responsibility of all staff • A lack of effective communication mechanisms by which staff can raise security concerns • A lack of effective briefing on security practices	• Formalised monitoring and assessment procedures are absent or *ad hoc* • Behavioural assessment either absent or is not evidence based • Procedures fail to identify insider threats (including threats to national security) in a timely fashion or produce an unacceptable number of false positives	• Disciplinary procedures are not appropriate for the full range of insider threats (including threats to national security) • Investigative practices do not enable effective legal defence of dismissal decisions that are taken to appeal	• HR and Security departments do not collaborate effectively and there is confusion about the division of their responsibilities for personnel security • There are no clear lines of accountability for personnel security
Medium						
Potential indicators of LOW vulnerability	• Personnel security risk assessment is routine and integrated within a risk management process • The assessment considers the opportunity of employee groups to commit threats and the impacts that these threats would have • Personnel security practices are regularly audited for compliance with requirements per role	• Standards are documented, understood and, where necessary, mandated through regulations • Practice is consistent with these standards across the organisation • Employees and contractors do not commence work prior to successful completion of all checks (or they are escorted at all times)	• Protective security is a very high priority for management and staff • Security is seen as the responsibility of all staff • Staff are vigilant • Staff have a good understanding of the security risks to the organisation • Security culture is assessed using validated tools and weaknesses are addressed through targeted communications	• Computer audit systems, regular (e.g. annual) staff security appraisals, whistle-blowing systems and behavioural assessment techniques are all used to detect suspicious or anomalous employee behaviour	• Investigative/ disciplinary procedures are robust, appropriate for the range of potential insider threats, and enshrined in formal and fully communicated policies • Arrangements allow the organisation to defend itself robustly in response to legal appeals from staff who are dismissed	• HR and Security collaborate very closely, but with a clear division of responsibility • There is a clearly identifiable senior responsible owner for personnel security

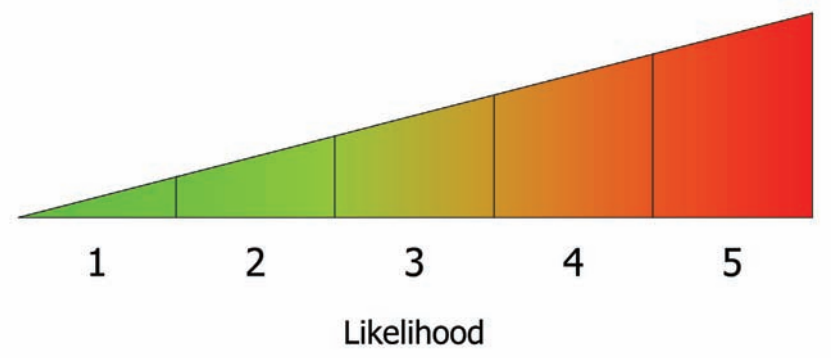
Electronic vulnerability

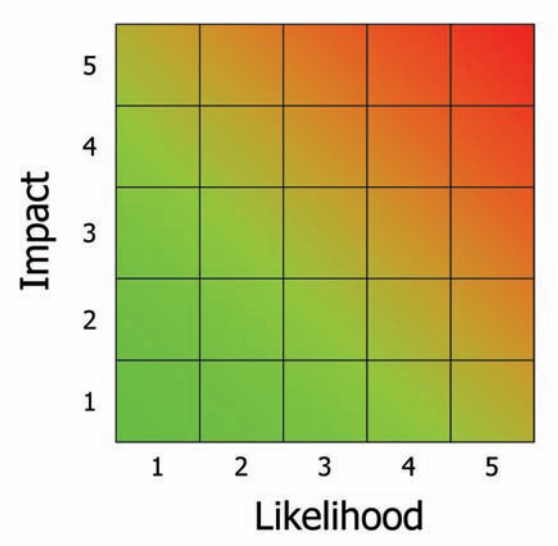
	A	B	C	D	E	F
Type of Electronic vulnerability **Fields A-F**	**Information Security management & audit**	**Risk management**	**Technical control policies**	**Technical control procedures**	**System acquisition, development & maintenance**	**System's physical environment, outsourcing and off-shoring**
Potential indicators of HIGH vulnerability (Indicators likely to be supported by little evidence of strong security governance, policy and procedures)	• Information security not discussed at board level, and no method of reporting to board level • No security policy • No management system for IT generally or information security in particular • Audit of IT systems is inadequate	• Information risks not assessed, or assessed only within the IT department • No management structure for management of information security risks • No Business Continuity Management (BCM) • No Information Asset Inventory	• Lack of coherent policies or lack of awareness of policies such as: - Client security, including laptops, remote access - Network security, including access control, user management, network services, IDS and pen tests • Anti-virus software • System patching	• Lack of adequate procedures, with ineffective audit, such as: - Client security, including laptops, remote access - Network security, including access control, user management, network services, IDS and pen tests • Anti-virus software • System patching	• Security issues are not included in the acquisition, development and maintenance process • No change control processes	• Critical systems development and/or operation are outsourced and/or off-shored with no security issues in the contract • Outsource/off-shore issues not included in risk assessments or audits • Critical systems have poor physical security
Medium						
Potential indicators of LOW vulnerability (Indicators likely to be supported by clear evidence of strong security governance, policy and procedures)	• Board level ownership of Information Security • IS policy implements board strategy within industry standards • IT systems managed to industry standards (e.g. ITIL) • Critical systems certified to 27001	• Corporate risk management system includes information security risks and reports to Board level • Up to date Information Asset Inventory forms the basis for threat assessment and BCM • Comprehensive and well rehearsed BCM plans	• Policies are coherent and integrated • All staff are aware of the policies to the extent that they need to be • Breaches of policy are investigated and remedial action taken	• Procedures are comprehensive • Effectiveness is audited regularly • Security incidents are investigated and remedial action taken	• Security issues dealt with at all stages • Change control processes operating effectively	• No critical systems are outsourced • All critical systems have good physical security

Annex C: Diagrams for use in risk workshops

The following diagrams and tables can be copied, enlarged and printed onto laminates for use in brainstorm sessions.







Disclaimer
Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining form acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

March 2009