National Protective
Security Authority

GUIDANCE

Role-based Protective Security Risk Assessment Guidance

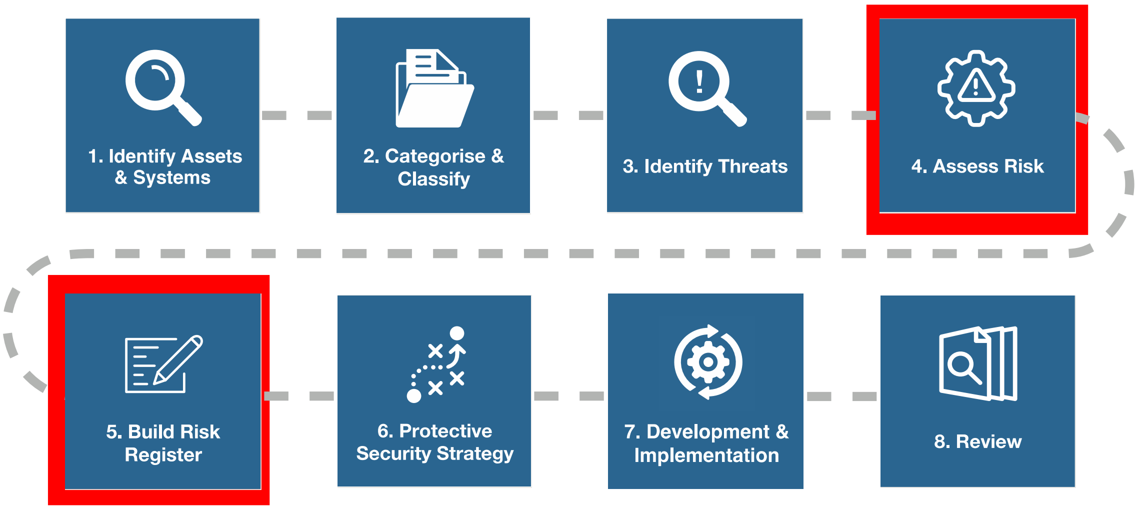
Introduction

Conducting a Role-based Protective Security Risk Assessment that considers the whole workforce will help to identify areas of potential risk, based on the access certain roles have to the assets of an organisation. This process is crucial in understanding the ‘insider’ risk within an organisation, evaluating the effectiveness of any existing countermeasures, and developing a programme of work to mitigate the risk.

It is important terminology is understood in the context of insider risk.   Within this guidance the threat is defined as the *intent* and *capability* of a hostile actor to take adverse action against the organisation - for example, to carry out a terrorist attack, exploit computer networks via cyber means or covertly obtain a piece of intellectual property. And the risk is defined as the *likelihood* and *impact* of such an action.

The NPSA definition of an ‘insider’ is any person who has, or previously had, authorised access to or knowledge of the organisation’s resources, including people, processes, information, technology, and facilities. Please read the NPSA Changes to Insider Risk Definitions document for further information. An insider could be a full time or part-time employee, a contractor or even a business partner. Throughout this guidance we will describe those with legitimate access as the “workforce’.

This guidance follows the NPSA protective security risk management (PSRM) approach, focussing on step 4 and 5 highlighted in red below. It demonstrates a systematic basis for an organisation to develop a proportionate and effective protective security strategy to manage security threats.


1. Identify Assets & Systems
2. Categorise & Classify
3. Identify Threats
4. Assess Risk
5. Build Risk Register
6. Protective Security Strategy
7. Development & Implementation
8. Review

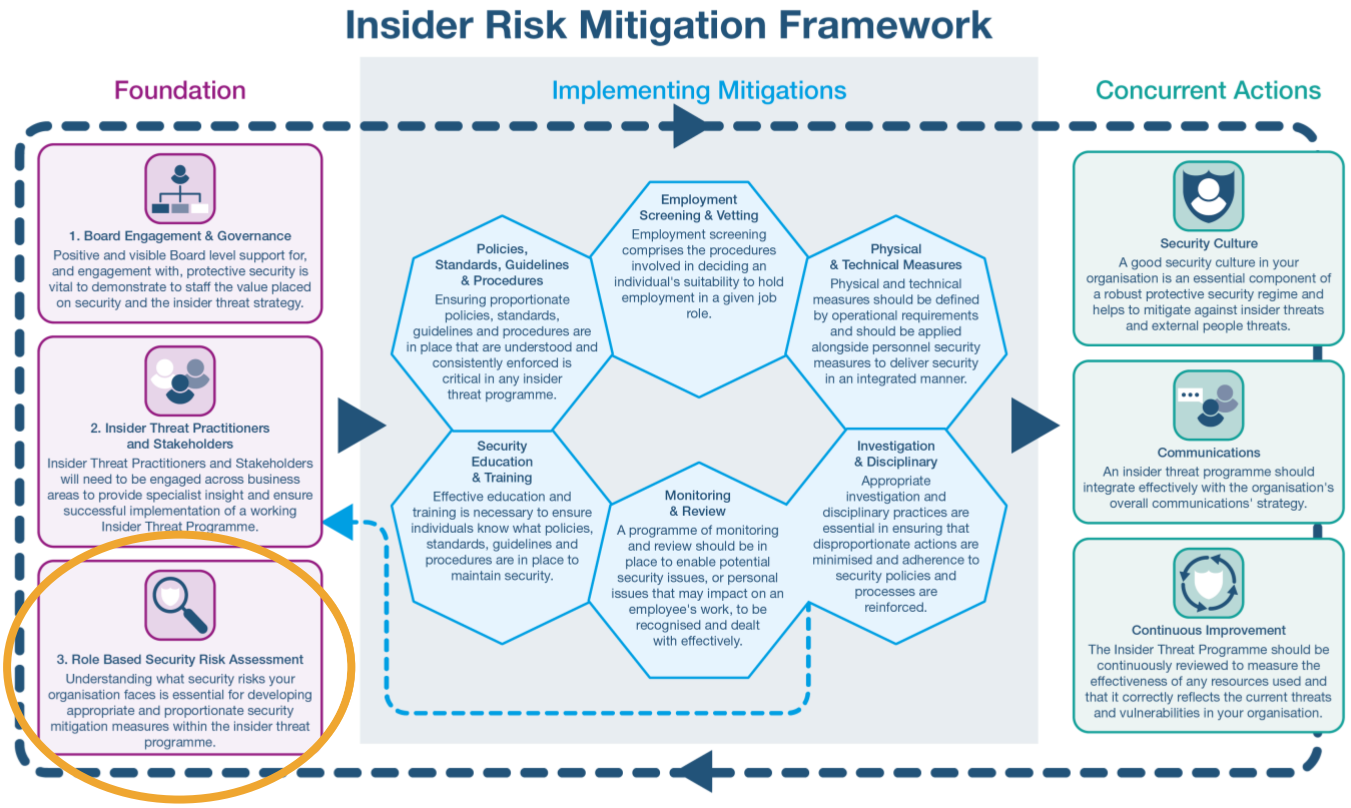
What are the benefits of conducting a Role-based Risk Assessment?

- Developing a Role-based Risk Assessment will help an organisation understand the threat and the risks specific roles may pose, the effectiveness of existing countermeasures (technical/cyber, physical and personnel) and where improvements are required.

- This is a holistic approach, so the benefit of this process comes from the systematic exploration of threats, opportunities and countermeasures, through discussion with the relevant business areas in an organisation, and use of reliable sources of information such as NPSA, NCSC, NaCTSO, regulators and industry bodies.

- This simple, flexible and transparent model can be used alone or as an add-on to existing security or business risk assessment programmes. The outcomes of any Role-based Risk Assessment should be fed back into the strategic security risk register which will ensure a holistic understanding and approach to managing security risks across the whole organisation and avoid knowledge being held in silos.

Developing a Role-based Risk Assessment is essential to support the foundations of any governance of protective security, such as in the Insider Risk Mitigation Framework shown below:



Insider Risk Mitigation Framework

Foundation

1. Board Engagement & Governance

Positive and visible Board level support for, and engagement with, protective security is vital to demonstrate to staff the value placed on security and the insider threat strategy.

2. Insider Threat Practitioners and Stakeholders

Insider Threat Practitioners and Stakeholders will need to be engaged across business areas to provide specialist insight and ensure successful implementation of a working Insider Threat Programme.

3. Role Based Security Risk Assessment

Understanding what security risks your organisation faces is essential for developing appropriate and proportionate security mitigation measures within the insider threat programme.

Implementing Mitigations

Policies, Standards, Guidelines & Procedures

Ensuring proportionate policies, standards, guidelines and procedures are in place that are understood and consistently enforced is critical in any insider threat programme.

Employment Screening & Vetting

Employment screening comprises the procedures involved in deciding an individual's suitability to hold employment in a given job role.

Physical & Technical Measures

Physical and technical measures should be defined by operational requirements and should be applied alongside personnel security measures to deliver security in an integrated manner.

Security Education & Training

Effective education and training is necessary to ensure individuals know what policies, standards, guidelines and procedures are in place to maintain security.

Monitoring & Review

A programme of monitoring and review should be in place to enable potential security issues, or personal issues that may impact on an employee's work, to be recognised and dealt with effectively.

Investigation & Disciplinary

Appropriate investigation and disciplinary practices are essential in ensuring that disproportionate actions are minimised and adherence to security policies and processes are reinforced.

Concurrent Actions

Security Culture

A good security culture in your organisation is an essential component of a robust protective security regime and helps to mitigate against insider threats and external people threats.

Communications

An insider threat programme should integrate effectively with the organisation's overall communications' strategy.

Continuous Improvement

The Insider Threat Programme should be continuously reviewed to measure the effectiveness of any resources used and that it correctly reflects the current threats and vulnerabilities in your organisation.

The Role-based Risk Assessment should be used to:

- provide strategic information to support senior-level decision making
- inform any insider risk strategic stakeholder group (or working group) responsible for implementing an insider risk mitigation programme, https://www.npsa.gov.uk/resources/itsg-tor-template
- provide tactical/operational information for business risk holders responsible for the day-today management of insider risk.

Why focus on insider risk?

- People, processes, information, technology, and facilities are the core elements of all organisations. Employees and colleagues can be the biggest asset for an organisation and are integral to all the other core elements of a business.
- Effective security risk management needs a blend of technological/cyber, physical, and human based approaches, such as, IT controls, physical access controls and the development of effective security culture and behaviour change programmes.

The Role-based Risk Assessment process

Using the information gathered in steps 1-3 of the NPSA PSRM approach, it should be possible to begin a Role-based Risk Assessment. A worked example of the process can be found here (https://www.npsa.gov.uk/resources/illustrative-role-based-risk-assessment-case-study)

Start the Role-based Risk Assessment process with colleagues who have relevant knowledge of critical assets or systems (https://www.npsa.gov.uk/resources/asset-identification-guide) to help inform the assessment. It is vital key representatives from across business areas, who have detailed and specific knowledge of these critical assets and systems, are involved and contribute to this process. The intention should be to work through examples of potential insider activity relating to the critical assets, i.e. to assess the *likelihood* and *impact* of the risks and assess against the organisation's security maturity.

To be effective the identified role-based risks need to provide enough detail to develop appropriate mitigations. Mitigations can reduce both the *likelihood* and the *impact* of the risks by putting measures in place to, for example, deter a hostile act or reduce the potential for harm to be done by a physical attack. In large, complex and multi-national organisations, it may be necessary to repeat the Role-based Assessment process at departmental level rather than attempting to cover all areas of the organisation at once.

Understanding Insider Risk – what does it look like?

To help focus on the assessment process, NPSA research has identified five main strategic types of insider risk.

i. Unauthorised disclosure of sensitive information that belongs to the organisation but is shared with a third party who is not authorised to have it - this can be deliberate (e.g. such as passing a client database to a competitor) or unintentional (e.g. attaching a document by mistake to an email).

ii. Process corruption – for e.g. of a financial process to enable fraud.

iii. Facilitation of third party access to assets – for e.g. allowing physical access to unauthorised personnel by giving a pass to someone or providing a password to allow unauthorised access to IT systems.

iv. Physical sabotage – for e.g. taking a hammer to a IT server.

v. IT or Electronic sabotage – for e.g. introduction of malware to corrupt data.

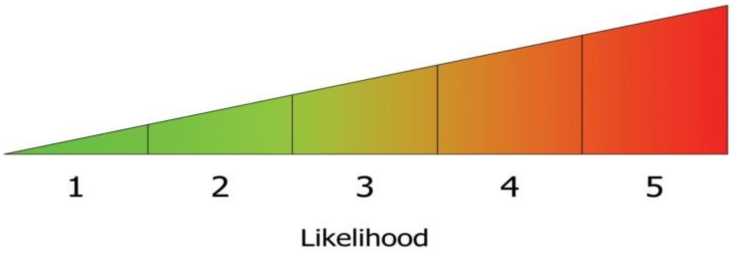
Using these five types of insider risks as broad headings can be a helpful way to structure discussions about the different combinations and methodologies insider risks may occur within the organisation. This thematic structure can be particularly helpful if working at a departmental level where there is a need to develop a consistent approach, ensuring that all departments are using the same process and thinking about the same broad risks. However, organisations should not limit their discussions only to these scenarios and should explore all relevant insider activity.

Assessing Likelihood

NPSA recommends using a using a relative scale ranging from 1 (least likely) to 5 (most likely).

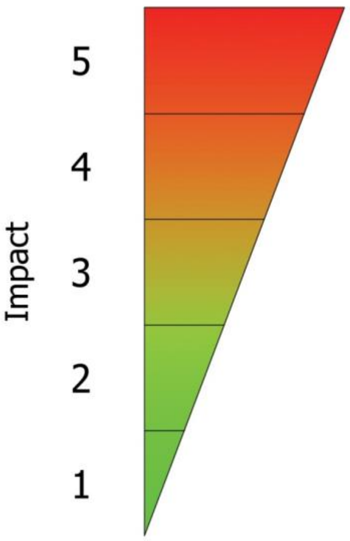
When assessing the likelihood of an insider act taking place, consider:

- **Potential target** – is the organisation a realistic target for a certain type of attack?
- **Precedence** – has other organisations in the same sector been subject to attack?
- **Security culture** – are there lots of security incidents, and how are they dealt with?
- **Countermeasures** – what processes are in place to deter, detect and recover from insider activity and how effective are they i?
- **Ability** – do the workforce have the expertise to carry out the kind of attacks detailed as threats?
- **Access** – do the workforce have the access to carry out the insider attacks identified?



It is important to record and document the detail about any assumptions made to allocate a scenario given a likelihood score. This will ensure any subsequent review of the risks will have a full picture as to how the score was agreed upon.

Assessing Impact



Impact should also be assessed using a relative scale ranging from 1 (lowest impact) to 5 (greatest impact) and should be based on factors that are meaningful to the organisation, such as:

- The number and importance of sites affected
- Potential injuries or fatalities amongst employees or the public
- Financial loss
- Effect to internal and external reputation
- The length of time it would take to resume business as usual
- Adequacy of contingency plans

As with the likelihood scores it is important that assumptions made about the impact scoring are recorded and documented.

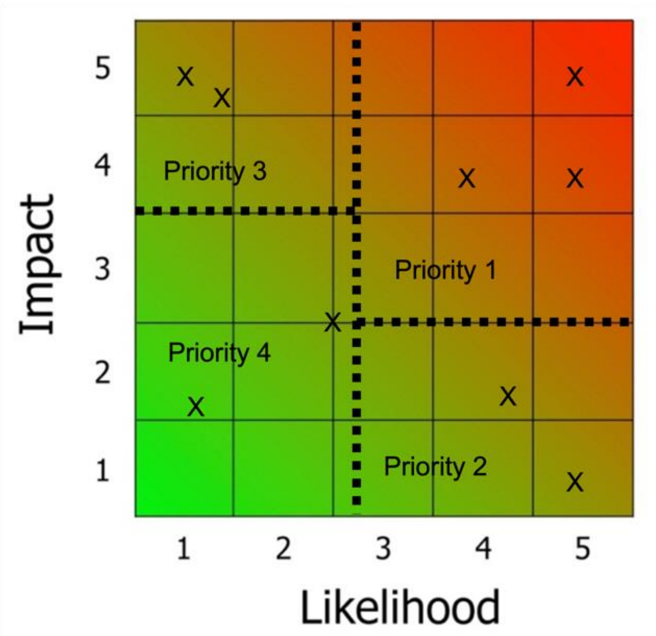
The assumptions provide an evidence-based approach as to why scores were allocated, provide continuity of approach and document thought processes for future reviews. This helps to reduce loss of organisational/corporate knowledge.

The likelihood and impact discussions are likely to have identified specific job roles that enabled the insider risk to manifest – organisations are recommended to make a note of these roles to identify any areas that might need additional security measures to reduce the overall risk.

Prioritising the risks

The next stage of the risk assessment process is to prioritise the risks as this will help focus decision making on the subsequent actions and mitigations to take forward. The simplicity of this approach means that it is easy to map risks onto a matrix.

- Plot each risk on the 5x5 heat grid. For example, a risk with an impact of 2 and a likelihood of 1.
- Once all risks are plotted, carry out a quick review of the grid to see any anomalies/outliers where it might be need to review the scoring and assumptions.
- Natural groups of risks may appear that fit together as an easy and quick way to gauge where the focus of mitigating actions should be.
- Divide the grid up into a number of priorities – for example very high, high, medium or low, would be Priority 1,2,3,4 etc.



- NPSA would recommend the very high impact risks should be in an organisations list of top priorities.

Using a Role-based Risk Register

How the priorities will be taken forward will depend on a number of factors – resource, time, money, readiness of the organisation etc. Any new countermeasures to be implement will need to work holistically with existing (or new) physical, technical and cyber security measures to help deter, detect, and recover from security incidents. This Role-based Risk Assessment should now feed into a protective security strategy and any operational requirements (ORs) for development and implementation.

Once the risk register is completed it should be reviewed on at least an annual basis, but reviewed more frequently if there has been a change in the threat or a major incident within the organisation. A review could also be required as a result of any significant change to the critical assets held or once a mitigation is put in place to assess if the risk has been reduced or displaced the risk to other areas.

Strategic Risk Register

NPSA has identified that many strategic risk registers tend to have a single entry for insider risk, with no granular level of information to assess and manage this risk. The evidence collated through the Role-based Protective Security Assessment can provide evidence to inform this risk, for example if an organisation mapped numerous opportunities for insiders to make unauthorised disclosure but found little opportunity for sabotage. This level of detail in the role-based risk register should be developed into thematic insider risks to sit in the strategic risk register.

Freedom of Information Act (FOIA)
This information is supplied in confidence and may not be disclosed other than to the agreed readership, without prior reference to NPSA. Within the UK, this material is exempt from disclosure under the relevant Freedom of Information Acts and may be subject to exemption under the Environmental Information Regulations and the Data Protection Act 1998.

Disclaimer
The information contained in this document is accurate as at the date it was created. It is intended as general guidance only and you should not rely on it. This information should be adapted for use in the specific circumstances required and you should seek specialist independent professional advice where appropriate before taking any action based on it. To the fullest extent permitted by law, NPSA accept no liability whatsoever for any loss or damage incurred or arising as a result of any error or omission in the guidance or arising from any person acting, relying upon or otherwise using the guidance. Full terms and conditions governing the use of this guidance are available on our website at www.npsa.gov.uk.