#Personnel risk assessment

This guidance is written for departmental and line managers that manage staff. These staff may include, but are not limited to: permanent employees, individuals on attachment or secondment, contractors, consultants, agency and temporary staff.

Personnel security risk assessment focuses on employees and contractors, their access to Ministry of Justice (MoJ) assets, and the risks they could pose. This is set against the adequacy of existing countermeasures. This risk assessment is crucial in helping you communicate to senior managers the risks to which the organisation is exposed.

This guidance aims to help risk management practitioners to:

* Conduct personnel security risk assessments in a robust and transparent way.
* Prioritise the insider risks to an organisation.
* Evaluate existing countermeasures, and identify appropriate countermeasures to mitigate those risks.
* Allocate security resources, which might be personnel, physical or informational in nature, in a way which is cost-effective and proportionate to the risk posed.

**Parent topic:** [Personnel security clearances](personnel-security-clearances.md)

##Personnel security

Personnel security is a system of policies and procedures that seek to manage the risk of people exploiting, or having the intention to exploit, their legitimate access to the organisation’s assets for unauthorised purposes. Those who seek to exploit their legitimate access to systems and data are called “insiders” and they pose an “Insider Risk”.

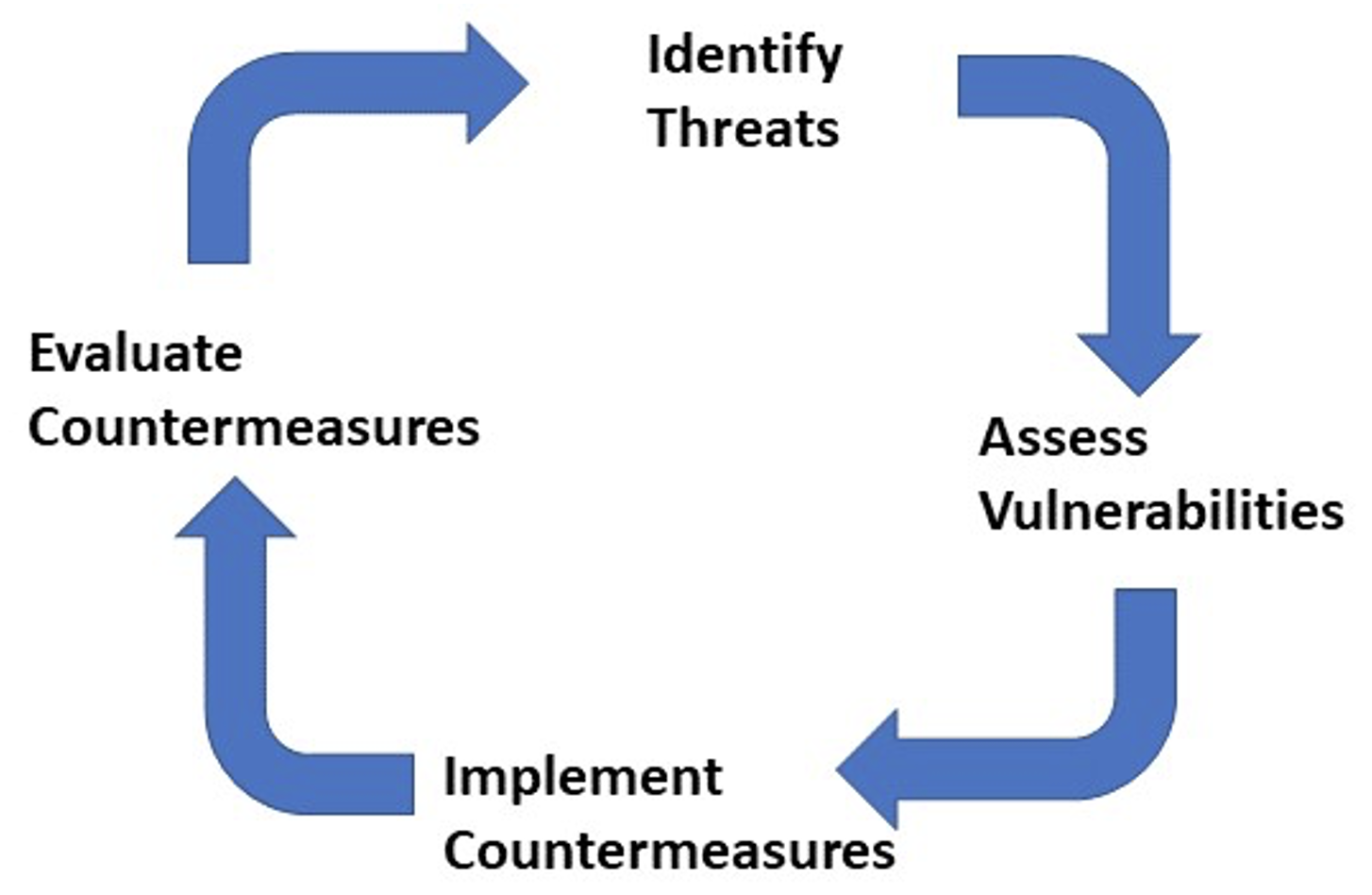
A person who causes harm to the MoJ might have access to assets for one day a month, or every working day. They might be a permanent member of staff, or a contractor. Their access might be in a traditional office, or site setting, or remote. This guidance covers all people who are given legitimate access to MoJ assets and premises.

The guidance for Personnel Risk is not prescriptive. It provides a framework to work with but, to be successful, it requires the MoJ to bring together the right people and information. The more you put into this process, the more worthwhile and useful the results will be.

##Risk management

Risk management is the foundation of the personnel security management process and is a continuous cycle of:

* Identification: identify the risks to the role.
* Risk assessment: assess the risks to the organisation and its assets in terms of the likelihood of a threat taking place, and the impact that such an event might have.
* Implementation: identify and implement security measures to reduce the likelihood and impact of the threat to an acceptable level, bearing in mind that risk can not be completely removed.
* Evaluation: assess the effectiveness of the countermeasures and identifying corrective actions.



A diagram describing a cycle of four stages. The first stage is at the top of the diagram. It is labelled Identify Threats. A large arrow flows out from the right hand side of the top stage, down to the second stage, at the right of the diagram. The second stage is labelled Assess Vulnerabilities. A large arrow flows out from the second stage down to the third stage, at the bottom of the diagram. The third stage is labelled Implement Countermeasures. A large arrow flows out from the third stage up to the fourth and final stage, at the left of the diagram. The fourth and final stage is labelled Evaluate Countermeasures. A large arrow flows out from the fourth and final stage up to the first stage again, at the top of the diagram.

The methodology defines risk as the product of two factors:

* The likelihood of an event occurring.
* The impact that the event would have.

When each of these factors has been evaluated, they are combined and this provides the overall measure of risk.

The cyclical nature of the process ensures that the implementation and evaluation stages are reviewed each time a risk assessment is repeated.

Much of the value of the risk management process comes from the systematic exploration of threats, opportunities, and countermeasures, through engagement with other parties. These differ between departments but can include HR, security, senior management, information specialists, and other technical specialists as appropriate.

##The Risk Management process

The MoJ uses the risk management process developed by the Centre for Protection of National Infrastructure (CPNI). A copy of the CPNI’s guide can be found [here](https://www.cpni.gov.uk/ongoing-personnel-security).

Managers and other risk management professionals **SHALL** follow the process set out in the guide, and maintain detailed records. These **SHOULD** be made available when requested by Audit, Group Security, or HR.

##Downloads

* [Ongoing personnel security: A good practice guide](https://www.cpni.gov.uk/system/files/documents/d0/d2/ongoing-personnel-security-a-good-practice-guide-edition-3.pdf).
* [Personnel security risk assessment](https://www.cpni.gov.uk/system/files/documents/46/06/Personnel-security-risk-assessment-a-guide-4th-edition.pdf).

##Contacts

For any further questions relating to security, contact: [security@justice.gov.uk](mailto:security@justice.gov.uk), or for security advice, contact the [Cyber Assistance Team](mailto:CyberConsultancy@digital.justice.gov.uk).

##Feedback

If you have any questions or comments about this guidance, such as suggestions for improvements, please contact: [IT policy content](mailto:itpolicycontent@digital.justice.gov.uk).