

---

## The aim of this guidance

Personnel security risk assessment focuses on employees, their access to their organisation's assets, the risks they could pose and the adequacy of existing countermeasures. This risk assessment is crucial in helping security and human resources (HR) managers, and other people involved in strategic risk decisions, 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 (be they personnel, physical or information) in a way which is cost-effective and proportionate to the risk posed.

## 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 an organisation's assets for unauthorised purposes. Those who seek to exploit their legitimate access are termed 'insiders'.

For the purpose of this guidance the person who causes harm to your organisation could be given access to assets for one day a month or every working day, may be a permanent member of staff or a contractor and their access may be in a traditional office or site setting or via a remote means of working. As you work through the risk assessment the term 'individual(s)' and 'personnel' are used to cover *all* people who are given legitimate access to your organisation's assets and premises. This may include, but is not limited to: permanent employees, individuals on attachment or secondment, contractors, consultants, agency staff and temporary staff.

## Personnel security risk assessment

This guidance explains how to use one type of methodology; it is not the only type of risk assessment but it is unique in that it focuses upon the risks posed by the people with legitimate access to the assets in your organisation. It is simple, robust, flexible and transparent. It can be used alone or as an 'add-on' to your existing risk assessment programme. Whilst the guidance explains how to examine the risks that people pose to your valued assets, it does not attempt to indicate which of those assets are the most important or which group of employees might pose the greatest threat. This will require your own expertise and knowledge of your organisation. Each sector has its own risks and each sector knows its business the best.

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

---