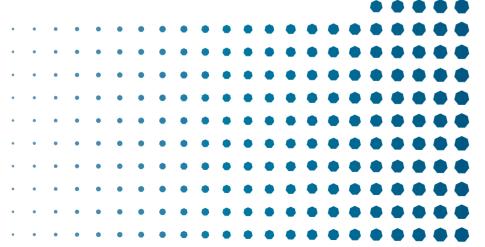National Protective
Security Authority

Personnel Security Maturity Model

Establishing a robust Personnel Security (PerSec) regime strengthens an organisation's resilience to insider risk and wider external threats. The Personnel Security Maturity Model provides a structured framework to support an organisation in developing proportionate PerSec security mitigations.

The benefits of using the NPSA Maturity Model

1 A starting point for developing a measurable PerSec improvement programme using the NPSA tools and guidance appropriate to your organisation's current level of PerSec maturity.

2 A common and consistent benchmark for PerSec performance across the Critical National Infrastructure (CNI), which will enable you to compare your organisations with others in your sector.

7 core elements of effective PerSec:

- Governance and Leadership
- Insider Risk Assessment
- Pre-Employment Screening
- Ongoing Personnel Security
- Monitoring and Assessment of Employees
- Investigation and Disciplinary Practices (Response)
- Security Culture and Behaviour Change

CNI organisations should contact their NPSA Security Advisor for more information on how to engage with the NPSA Maturity Model or visit: **www.npsa.gov.uk/reducing-insider-risk**

4 key areas

The NPSA Maturity Model questionnaire seeks evidence across four key areas:

EXISTENCE
The existence of PerSec policies, processes and procedures.

IMPLEMENTATION
The implementation of the PerSec programme.

CONSISTENCY
The consistency of the PerSec measures in place.

EFFECTIVENESS
The effectiveness of the PerSec policies and procedures that are in place.

For more information on the NPSA Personnel Maturity Model please go to npsa.gov.uk/personnel-security-maturity-model

Overview of PerSec Maturity Model

Innocent
LEVEL 0

Current Behaviours

Organisation functioning at most basic level. No formal PerSec policies, training or procedures. Senior managers unconcerned by people risk with no attempt to engage with NPSA.

Organisation is at very high risk from operational, financial and reputational damage due to PerSec threats.

Developing
LEVEL 2

Current Behaviours

PerSec seen as business risk and effort made to reduce security incidents. Security defined in terms of adherence to rules, procedures and technical controls, and are managed through lagging indicators (number of breaches, alarms). There is acknowledged approach using standardised templates.

Organisation is at moderate risk from operational, financial and reputational damage due to PerSec threats.

Effective
LEVEL 4

Current Behaviours

Board recognises security is important both morally and financially, providing business advantage. Management recognise precursor indicators, with focus on proactive measures to prevent security incidents and statistics collected and analysed. Majority of workers accept personal responsibility for security.

Organisation is at low risk from operational, financial or reputational damage from PerSec threats.

Aware
LEVEL 1

Current Behaviours

PerSec defined in basic terms of technical or procedural solutions. No standardised threat mitigation processes, training or policies. No board level responsibility for PerSec.

Organisation is at high risk from operational, financial and reputational damage due to PerSec threats.

Competent
LEVEL 3

Current Behaviours

Organisation-wide consistent approach to security with defined processes. Managers recognise a wide range of factors influence security and involvement of front line staff is critical. Significant numbers of front line staff willing to work with management to improve security.

Organisation is at some risk from operational, financial and reputational damage from PerSec threats.

Excellent
LEVEL 5

Current Behaviours

Prevention of PerSec incidents is a core company value with assigned board level responsibility. PerSec risk assessment is reviewed at least annually. Organisation uses range of indicators to monitor performance, innovating to improve security control. All workers share personal responsibility for security.

Organisation is at very low risk from operational, financial and reputational damage due to PerSec threats.

Overall level of maturity is dictated by the lowest level of achievement in any one of the seven core elements.