CPNI
Centre for the Protection of National Infrastructure

Insider Risk Mitigation Framework

Physical & Technical Measures

The need to apply any physical or technical security measures in mitigating the insider threat should be identified in the role based risk assessment. It is essential that clear Operational Requirements (OR) are produced.

The OR process helps organisations make smarter investments in security measures. It enables them to protect assets from compromise by implementing measures that are in proportion to the risks they face: Maintaining confidentiality, integrity, and/or availability (CIA).

By following this process, security managers and practitioners are able to assess, develop and justify the actions their organisation needs to take, and the investments they need to make to protect critical assets against security threats. At the end of the process they will have a clear statement of need based on the issues that need addressing and the solutions that should help. This systematic and thorough assessment will help to support their business case.

The use of the OR process should enable the delivery of personnel, physical and technical/cyber security measures in an integrated manner, multiplying the effectiveness of all measures and using different measures to fill gaps that others cannot plug (a Defence in Depth approach).

Existing Products

Operational Requirements
Access Control & Locks (Physical)
CCTV (Physical)
Secure Working Areas (Physical)
Security Control Rooms (Physical)
Protection of Sensitive Information & Assets (Physical)
Password guidance (NCSC)
Cloud Security Guidance (NCSC)
Protecting Bulk Personal Data (NCSC)
10 Steps to Cyber Security (NCSC)
Cyber Resilience (NCSC)
The Trouble with Phishing (NCSC)
Phishing, Spear Phishing and Whaling (NCSC)