# Penetration testing PENT

Testing the effectiveness of security controls by emulating the tools and techniques of likely attackers.

|  |
| --- |
| **Guidance Notes:**  Penetration testing may be a stand-alone activity or an aspect of acceptance testing prior to an approval to operate.  Activities include, but are not limited to:   * ethical hacking (using the same tools and techniques as an adversary to safely exploit security weaknesses) * demonstrating how an adversary can subvert security goals or achieve specific adversarial objectives * evaluating the effectiveness of current/planned defences or mitigation controls * assuring the security of networks, systems, and applications * assessing the strength and effectiveness of cryptographic implementations * identifying insights into the business risks of various vulnerabilities * testing network, infrastructure, web and mobile applications for weaknesses * checking patch levels and configurations * social engineering. |

## Level 2

Assists with penetration testing tasks under routine supervision.  
Supports the execution of standard penetration tests on systems, networks, and applications.  
Helps document and report on test results, findings, and potential security risks.

## Level 3

Follows standard approaches to design and execute penetration testing activities.  
Researches and investigates attack techniques and recommends ways to defend against them.   
Analyses and reports on penetration testing activities, results, issues and risks.

## Level 4

Selects appropriate testing approach using in-depth technical analysis of risks and typical vulnerabilities.   
Produces test scripts, materials and test packs and tests new and existing networks, systems or applications. Provides advice on penetration testing to support others.  
Records and analyses actions and results and modifies tests if necessary.   
Provides reports on progress, anomalies, risks and issues associated with the overall project.

## Level 5

Plans and drives penetration testing within a defined area of business activity.   
Delivers objective insights into the existence of vulnerabilities, the effectiveness of defences and mitigating controls.   
Takes responsibility for the integrity of testing activities and coordinates the execution of these activities. Provides authoritative advice and guidance on all aspects of penetration testing.   
Identifies needs and implements new approaches for penetration testing. Contributes to security testing standards.

## Level 6

Determines penetration testing policy, and owns the supporting processes.   
Manages all penetration testing activities within the organisation. Assesses and advises on the practicality of testing process alternatives.   
Establishes capability for continual improvement and invention in penetration testing and leads the implementation of new approaches.   
Assesses suppliers' development and testing capabilities. Manages client relationships with respect to penetration testing.