# Vulnerability assessment VUAS

Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.

|  |
| --- |
| **Guidance Notes:**Activities may include, but are not limited to:* cataloguing and classifying information and technology resources (assets and capabilities) to support vulnerability assessment
* assigning quantifiable value, rank order and importance to information and technology resources
* identifying and analysing the vulnerabilities of each resource, manually or using automated tools and information sources
* prioritising, scoring and ranking the risk associated with vulnerabilities
* business impact assessment
* mitigating or eliminating the vulnerabilities.

Vulnerability assessment tools include web application scanners, protocol scanners and network scanners. |

## Level 2

Undertakes low-complexity routine vulnerability assessments using automated and semi-automated tools.
Escalates issues where appropriate.
Contributes to documenting the scope and evaluating the results of vulnerability assessments.

## Level 3

Follows standard approaches to perform basic vulnerability assessments for small information systems.
Supports creation of catalogues of information and technology assets for vulnerability assessment.

## Level 4

Collates and analyses catalogues of information and technology assets for vulnerability assessment.
Performs vulnerability assessments and business impact analysis for medium complexity information systems.
Contributes to selection and deployment of vulnerability assessment tools and techniques.

## Level 5

Plans and manages vulnerability assessment activities within the organisation.
Evaluates, selects, and reviews vulnerability assessment tools and techniques.
Provides expert advice and guidance to support the adoption of agreed approaches.
Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems.