

## Overview

This standard is about managing vulnerability assessment activities.

This involves developing and delivering a comprehensive vulnerability management capability.

It includes defining effective strategies, policies and procedures for identifying, reporting and mitigating vulnerabilities impacting the organisation. It also includes identifying and recommending measures to manage and remediate vulnerabilities, establishing a vulnerability toolset to scan and report findings, and providing metrics and reporting on system vulnerabilities, patch management status, and trend analysis for management stakeholders.

This standard is for those who need to manage vulnerability assessment activities as part of their duties.

## Performance criteria

*You must be able to:*

1.  
Create, implement and maintain vulnerability management policies and procedures in line with organisational standards
2.  
Define the organisational vulnerability scanning infrastructure, tools and techniques to deliver vulnerability assessments
3.  
Specify organisational hardening policies to minimise operating system vulnerabilities
4.  
Lead the identification of new processes to improve vulnerability assessments
5.  
Implement training and development plans for all vulnerability assessment staff to maintain required capabilities
6.  
Lead vulnerability assessment and patch management capabilities to determine the security posture of the target system
7.  
Manage the master patch record and ensure all technology stacks are patched regularly to ensure vulnerabilities are proactively handled
8.  
Develop metrics to provide status updates on vulnerability management activities
9.  
Track progress of vulnerability remediation activities through formal change processes to verify closure
10.  
Produce and communicate vulnerability reports to inform stakeholders on capabilities, trends and performance metrics

## Knowledge and understanding

### *You need to know and understand:*

1. How to design and implement an organisational vulnerability management strategy
2. That vulnerability management is an essential component of an information security management system
3. That the regular identification and mitigation of vulnerabilities is a key element of risk governance
4. How to take responsibility for the budgetary control process for vulnerability management activities
5. That the vulnerability assessment policy defines who can perform vulnerability assessments and how often they should occur
6. The process of vulnerability assessment provides visibility of vulnerabilities and mitigations across an organisation's information systems
7. How to manage vulnerability management capabilities to deliver organisational requirements
8. How to analyse complex vulnerability problems
9. How to manage and resolve mitigations for complex vulnerabilities
10. The steps involved in infrastructure configuration hardening informed through vulnerability assessment
11. The importance of identifying and reviewing new tools and techniques to improve vulnerability assessment capabilities
12. The importance of providing ongoing training and guidance to all vulnerability assessment employees
13. The use of automated tools to support improvements to efficiency and effectiveness of vulnerability assessment activities
14. How to measure the effectiveness of vulnerability management through reporting and metrics

TECDT61151



Manage vulnerability assessment activities

---

<b>Developed by</b>	e-skills
<b>Version Number</b>	1
<b>Date Approved</b>	30 Mar 2022
<b>Indicative Review Date</b>	30 Mar 2025
<b>Validity</b>	Current
<b>Status</b>	Original
<b>Originating Organisation</b>	ODAG Consultants Ltd.
<b>Original URN</b>	TECDT61151
<b>Relevant Occupations</b>	Information and Communication Technology Professionals
<b>Suite</b>	IT and Telecoms Professional (procom)
<b>Keywords</b>	cyber security, vulnerability

---