



4.0 Reporting and Communication

4.1 Explain the importance of vulnerability management reporting and communication.

- **Vulnerability management reporting**
 - Vulnerabilities
 - Affected hosts
 - Risk score
 - Mitigation
 - Recurrence
 - Prioritization
- **Comppliance reports**
- **Action plans**
 - Configuration management
 - Patching
- Compensating controls
- Awareness, education, and training
- Changing business requirements
- **Inhibitors to remediation**
 - Memorandum of understanding (MOU)
 - Service-level agreement (SLA)
 - Organizational governance
 - Business process interruption
 - Degrading functionality
 - Legacy systems
- Proprietary systems
- **Metrics and key performance indicators (KPIs)**
 - Trends
 - Top 10
 - Critical vulnerabilities and zero-days
 - SLOs
- **Stakeholder identification and communication**

4.2 Explain the importance of incident response reporting and communication.

- **Stakeholder identification and communication**
- **Incident declaration and escalation**
- **Incident response reporting**
 - Executive summary
 - Who, what, when, where, and why
 - Recommendations
 - Timeline
- Impact
- Scope
- Evidence
- **Communications**
 - Legal
 - Public relations
 - Customer communication
 - Media
 - Regulatory reporting
 - Law enforcement
- **Root cause analysis**
- **Lessons learned**
- **Metrics and KPIs**
 - Mean time to detect
 - Mean time to respond
 - Mean time to remediate
 - Alert volume