Domain 6: Security Assessment and Testing

6.1 - Design and validate assessment, test, and audit strategies

- Internal
- External
- Third-party

6.2 - Conduct security control testing

- Vulnerability assessment
- Penetration testing
- Log reviews
- Synthetic transactions
- Code review and testing
- Misuse case testing
- Test coverage analysis
- Interface testing
- Breach attack simulations
- Compliance checks

6.3 - Collect security process data (e.g., technical and administrative)

- Account management
- Management review and approval
- Key performance and risk indicators
- Backup verification data
- Training and awareness
- Disaster Recovery (DR) and Business Continuity (BC)

6.4 - Analyze test output and generate report

- Remediation
- Exception handling
- Ethical disclosure

6.5 - Conduct or facilitate security audits

- Internal

- External
- Third-party