CodeVertex Penetration Test Readiness Checklist

Before kickoff:
- Define business objectives and success criteria
- Confirm in-scope assets (domains, IPs, apps, APIs, cloud accounts)
- Identify out-of-scope systems and critical constraints
- Establish testing windows and escalation contacts
- Provide access details and test accounts
- Confirm MFA and SSO behavior for testing
- Share architecture diagrams and data flow maps (if available)

Security and legal:
- Signed NDA and authorization letter
- Rules of engagement and safe testing boundaries
- Data handling requirements (PII, PHI, PCI)
- Logging and monitoring expectations

Operational readiness:
- Identify change freeze windows
- Ensure incident response team is informed
- Confirm point-of-contact for daily updates
- Prepare remediation owners and timelines

Post-test:
- Schedule debrief for findings and priorities
- Define retest window
- Assign owners to remediation items

Contact: contact@codevertex.io