

1. For Developers:

- Do you follow secure coding guidelines during the development phase? (Yes/No)
- Is input validation and output encoding implemented to prevent injection attacks? (Yes/No)
- Are authentication and authorization mechanisms built into the application? (Yes/No)
- Have vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF) been mitigated? (Yes/No)
- Is user data encrypted and are passwords hashed securely? (Yes/No)
- Do you conduct code reviews with a focus on identifying security flaws? (Yes/No)
- Are security patches for third-party libraries applied regularly? (Yes/No)
- Are automated security tools integrated into the CI/CD pipeline? (Yes/No)
- Do you track and respond to security vulnerabilities reported by external sources? (Yes/No)

2. For IT Team:

- Are servers and infrastructure protected by firewalls and security controls? (Yes/No)
- Is the antivirus or IDS/IPS system updated and running? (Yes/No)
- Do you monitor the network for any abnormal activities or security breaches regularly? (Yes/No)
- Is regular vulnerability scanning and penetration testing performed? (Yes/No)
- Is access to sensitive data restricted by user roles or privileges? (Yes/No)
- Are system and data backups taken regularly and stored securely? (Yes/No)
- Is there an incident response plan in place for security threats? (Yes/No)
- Do you enforce multi-factor authentication for administrative access? (Yes/No)
- Is logging and auditing enabled for tracking changes and anomalies? (Yes/No)

3. For Management:

- Do you have an organization-wide security policy in place? (Yes/No)
- Are regular security audits and assessments conducted? (Yes/No)
- Does the organization comply with data protection regulations (GDPR, HIPAA)? (Yes/No)
- Is there a protocol for handling and reporting security incidents? (Yes/No)
- Is security awareness training provided to all employees regularly? (Yes/No)
- Is there a defined budget for enhancing the security infrastructure? (Yes/No)
- Are third-party vendors' security policies reviewed before integration? (Yes/No)
- Do you have a business continuity plan in place in case of a major security incident? (Yes/No)

•