CHECKLIST

SECURITY

- [ ] What does crowdsourced security look like?
- [ ] When do you apply non security related updates?
- [ ] What are the biggest barriers to remediating and mitigating cybersecurity incidents?
- [ ] How are the security measures you use deployed?
- [ ] Do security patches make fewer logical changes than non security bug fixes?
- [ ] What are application security risks?
- [ ] What is the average amount of data you will lose on an annual basis due to security breaches?
- [ ] Is it the responsibility of your organization itself or the IT supplier to implement and inform of critical security updates?
- [ ] What is an on site security assessment?
- [ ] How long does it take to remediate security defects by type?
- [ ] Why is network security an issue?
- [ ] Are there clearly defined criteria for remediation of security risk for products in development?
- [ ] Do security and non security bug fixes always modify source code?
- [ ] How do security devices impact cybersecurity?
- [ ] Is management prepared to react timely if a cybersecurity incident occurred?
- [ ] Do project teams specify security requirements during development?
- [ ] Is there a test plan in place and are tools available to perform security testing?
- [ ] Are project releases audited for appropriate operational security information?
- [ ] How do you incentivize industry to design, implement, maintain effective cybersecurity solutions?
- [ ] Which security activity is most effective in finding vulnerabilities?
- [ ] Have the security controls been implemented or is there a plan in place?
- [ ] Has a security risk assessment and architectural review been performed?

CHECKLIST

- [ ] Which team is more productive in fixing security defects and vulnerabilities?
- [ ] What kind of security regulatory compliance do you meet?
- [ ] Do you really need to understand the fundamentals of security in order to protect your network?
- [ ] Does your organization have a security operations function?
- [ ] Do projects use automation to evaluate security test cases?
- [ ] What is web application security testing?
- [ ] When do you apply security updates?
- [ ] Are all security test requirements being met?
- [ ] What security measurement practices and data does your organization use to assist product planning?
- [ ] Are security patches smaller than non security bug fixes?
- [ ] Do you advertise shared security services with guidance for project teams?
- [ ] Is your application missing the proper security hardening across any part of the application stack?
- [ ] How do you ensure physical security?
- [ ] Why would you want anything less for the security of your networks and systems?
- [ ] Are stakeholders able to pull in security coaches for use on projects?
- [ ] When was the last security or vulnerability assessment conducted?
- [ ] Does a minimum security baseline exist for secure design review results?
- [ ] What is the security patch management criteria used to prioritize vulnerability remediation?
- [ ] What other risks does the security solution cause?
- [ ] What percentage of applications, users and devices has been reviewed for security issues?
- [ ] How will cybersecurity risk be assessed and management during the lifecycle?
- [ ] How do you manage application security?
- [ ] What are changes that are causing problems for IT security and operations teams?
- [ ] Why is application security important?
- [ ] What controls are needed to satisfy the security requirements to mitigate risk?
- [ ] Is your cybersecurity program aligned with your business strategy?

CHECKLIST

- [ ] How does the application maintain security?
- [ ] Why are you spending so much on security vulnerability remediation?
- [ ] Have you performed the proper security hardening across the entire application stack?
- [ ] How numerous are security flaws compared to security bugs?
- [ ] Who is responsible for authorizing flaw remediation security controls?
- [ ] Is cybersecurity your organization risk management issue?
- [ ] Do you have one million dollars to spend on application security?
- [ ] Do you know which processes and/or systems represent the greatest assets from a cybersecurity perspective?
- [ ] Does a minimum security baseline exist for security testing?
- [ ] Does your organization have an assigned security response team?
- [ ] Does the cloud provider have security/data breach protocols?
- [ ] Why do programmers make security errors?
- [ ] Are stakeholders aware of the security test status prior to release?
- [ ] How are security vulnerabilities discovered?
- [ ] Do stakeholders review vendor agreements for security requirements?
- [ ] How are administrators alerted when security risk score rises?
- [ ] What are the critical security controls?
- [ ] Are security related alerts and error conditions documented on a per project basis?
- [ ] Are there clearly defined criteria for remediation of security risk for commercialized product?
- [ ] Who is responsible for assessing, and monitoring flaw remediation security controls?
- [ ] Are you reviewing for security, functionality, maintainability, and/or style?
- [ ] Are security checks placed before processing inputs?
- [ ] How do you know if the CISOs security program has accounted for all the components to be effective?
- [ ] Are some resources more important that others, therefore requiring higher security?
- [ ] How would you characterize your organizations ability to prioritize security vulnerabilities?

CHECKLIST

- [ ] Do projects document operational environment security requirements?
- [ ] Does your organization have any security related policies for machines?
- [ ] Does the cloud provider have a security policy/statement?
- [ ] How complex are security patches compared to other non security bug fixes?
- [ ] What are the major root causes of security issues?
- [ ] What security mechanisms/controls are you having trouble implementing?
- [ ] Why crowdsourced security testing?
- [ ] When a cybersecurity incident occurs, what is your plan of response?
- [ ] Has the bureau given any thought to cybersecurity, as well as physical security?
- [ ] How to identify and mitigate cybersecurity risks across multiple public and private organizations?
- [ ] Do projects specify security testing based on defined security requirements?
- [ ] How would you define a strong security operations program?
- [ ] Is there a software security assurance program in place?
- [ ] Are you aware of any information security standards that your organization has?
- [ ] Do cybersecurity initiatives receive adequate support and priority?
- [ ] What security vulnerabilities are you having trouble fixing?
- [ ] How do you most effectively communicate information about security problems?
- [ ] Do you evaluate the effectiveness of cybersecurity?
- [ ] Do project teams specify requirements based on feedback from other security activities?
- [ ] Have you evolved your security architecture and associated processes?
- [ ] Is your crowdsourced security testing successful?
- [ ] Is your application security tool designed to keep up?
- [ ] How do you handle security for machines?
- [ ] Why sunbelt network security inspector?
- [ ] Which team is responsible for each stage of the security vulnerability remediation process?
- [ ] How many security issues are found during secure code reviews?

CHECKLIST

- [ ] Are audits performed against the security requirements specified by project teams?
- [ ] Is a discovered security vulnerability a real issue?
- [ ] What role does security play in a network?
- [ ] Which tools are most effective in detecting security vulnerabilities?
- [ ] What kind of security do you provide for your emails?
- [ ] Do project teams check software designs against known security risks?
- [ ] What type of tests do you use to detect security faults in a network and why?
- [ ] Do projects follow a consistent process to evaluate and report on security tests to stakeholders?
- [ ] Do you have at least one security savvy programmer on every critical development project?
- [ ] Does a minimum security baseline exist for code review results?
- [ ] How can security and IT teams collaborate on the remediation process?
- [ ] How does a workforce introduce the security skills to implement a secure code review methodology?
- [ ] Does your organization regularly compare your security spend with that of other organizations?
- [ ] Can the application revert back to normal operation when the security risk score drops to normal levels?
- [ ] What products and services are required to adopt the security development lifecycle process?
- [ ] What is it about human behavior that makes cybersecurity so inherently difficult?
- [ ] Why is cybersecurity so important?
- [ ] What are the threats associated with the security holes, as well as to your business?
- [ ] Does the product interoperate with other security technologies?
- [ ] Do project teams specifically analyze design elements for security mechanisms?
- [ ] How does security fit in your priorities?
- [ ] Can cybersecurity awareness be trained?
- [ ] Do projects have a point of contact for security issues or incidents?
- [ ] Which software security best practices are you familiar with?
- [ ] Are service releases required to adopt the security development lifecycle process?

CHECKLIST

- [ ] Do security patches affect fewer functions than non security bug fixes?
- [ ] Can project teams access automated code analysis tools to find security problems?
- [ ] Are security notes delivered with each software release?
- [ ] Are there any obligations by your supervisor/employer for performing security testing?
- [ ] Does your solution provide auditing, reporting, and alerting for security related events and information?
- [ ] Do security patches change code base sizes less than non security bug fixes?
- [ ] Do you already have IS security hygiene guidelines?
- [ ] Are security features correct and is functional code secure?
- [ ] What is your organization trying to achieve with information security/privacy program?
- [ ] Do security patches affect fewer source code files than non security bug fixes?
- [ ] Who is responsible for planning and implementing flaw remediation security controls?
- [ ] Are there still security holes lurking in your system?
- [ ] Are security test cases comprehensively generated for application specific logic?
- [ ] NOTES: