CHECKLIST

ORGANIZATION

- [ ] Who has responsibility for vulnerability management currently within your organization?
- [ ] Are all your employees working in your organization of own free will?
- [ ] Do you disseminate patch update information throughout organizations local systems administrators?
- [ ] How is cti data and information being utilized in your organization?
- [ ] Does your organization have a standard desktop configuration and software standards?
- [ ] Have any major data breach caused your organization to change its mode of operations?
- [ ] Does your organization or systems requiring remediation face numerous and/or significant threats?
- [ ] What is involved with your recently announced reorganization?
- [ ] Have new facilities been added or removed from your organization?
- [ ] Do you feel vulnerability management is important for your organization like yours?
- [ ] How closely do other organizations track to the average?
- [ ] Why would your organization fix the least important vulnerabilities the most often?
- [ ] Which environmental actions has your organization introduced or supported within the last year, if any?
- [ ] Has remediation of all known weaknesses been performed in a timely manner on each of your organizations systems?
- [ ] What defines your organizations sphere of influence?
- [ ] What updates are most important to your organization?
- [ ] What parts of your organization do you remediate quickly and what parts will take longer?
- [ ] Where are cti team members drawn from within your organization?
- [ ] Does your organization evaluate your own suppliers on environmental issues?
- [ ] How big are cyber risks for your organization and your organizations you do business with?

CHECKLIST

- [ ] Will it fit with the culture of your own organization?
- [ ] What are the requirements for software delivered to your organization from a vendor?
- [ ] How can technologists become forces for the public interest within own organizations?
- [ ] Do you feel your organization devotes the adequate amount of resources to vulnerability management?
- [ ] How do other organizations plan to improve the vulnerability risk management program next year?
- [ ] What organizations and departments work with young people?
- [ ] Does your organization know about what is required based on risk ratings?
- [ ] Do governance processes and your organizational culture enable effective cyber risk management?
- [ ] Are your top people leaving you and your organization?
- [ ] What are the issues organizations should be aware of?
- [ ] How much influence does your organization have?
- [ ] Are the applications running on the endpoint critical for your organization?
- [ ] Has your organization ever been breached as a result of a vulnerability being left unpatched?
- [ ] How are cti data and information being utilized in your organization?
- [ ] Are cti requirements clearly defined in your organization?
- [ ] Does your organization systematically use audits to collect and control compliance evidence?
- [ ] Which main environmental targets has your organization worked towards during the last year?
- [ ] Is your organization routinely targeted and face attempts of attack?
- [ ] Does your organization perform vulnerability scanning?
- [ ] What organizations and departments work with older people?
- [ ] How to build a compliance communication within your organization?
- [ ] Do the business stakeholders understand your organizations risk profile?
- [ ] Has your organization established formal governance and controls to protect the sensitive data?
- [ ] Has your organization ever stopped using a product due to vulnerability disclosure?
- [ ] What are the legal, regulatory, and contractual requirements your organization must meet?

CHECKLIST

- [ ] Is your organization response team ready?
- [ ] Has your organization had to make investment in IT hardware and/or software?
- [ ] Has your organization acquired any other organizations?
- [ ] What does success look like for your organization?
- [ ] How mature are your organizations processes for incident handling?
- [ ] Is your organization experiencing compliance fatigue?
- [ ] Does your organization periodically assess risk using the criteria set forth in the control requirement?
- [ ] Has your organization established a continuous monitoring of impacts?
- [ ] What data types are currently stored by your organization?
- [ ] What is the total population of your organization?
- [ ] How are other organizations performing in reality?
- [ ] Is your organization environment getting complex day by day?
- [ ] How large is your organization that you work for?
- [ ] What is the industry of your organization that you work for?
- [ ] Is your organizations vulnerability management program winning?
- [ ] Is the vulnerability pertinent to your organizations operations?
- [ ] Are you and your organization ready to deal with a cyber crisis?
- [ ] Are solutions driven by your own or organization policy?
- [ ] Does the vulnerability affect systems within your organizations network?
- [ ] Does your organization have a good handle on its asset inventory?
- [ ] Will your organization work to secure an agreement?
- [ ] Do you guess how many times your organization has been hacked?
- [ ] What updates are most important to your organization and why?
- [ ] Does your organization utilize a set of policies and standards to control software development?
- [ ] Does organization project estimation allot time for code reviews?
- [ ] Is responsibility for the working environment clearly defined at all levels in your organization?

CHECKLIST

- [ ] Are vulnerabilities analyzed to determine relevance to your organization?
- [ ] How long does it take to detect new hardware and software added to your organizations network?
- [ ] Does your organization have an environmental management system or programme?
- [ ] What updates are least important to your organization?
- [ ] Does your organization duty to protect mostly just require more regulation?
- [ ] What is your organizations involvement in vulnerability management?
- [ ] Has your organization kept pace?
- [ ] Which human rights issues may arise within your organizations sphere of influence?
- [ ] What is the main purpose of your organization you work for?
- [ ] Does your organization share the cost risk identification measures with suppliers?
- [ ] Does your organization utilize a consistent process for incident reporting and handling?
- [ ] What is a fourth of your organizations capitalization?
- [ ] Who in your organization is responsible for vulnerability management?
- [ ] Who has access to your organizations most valuable information?
- [ ] Does your organization run vulnerability scans?
- [ ] Has new technology been introduced to your organization?
- [ ] Does your organization have a vulnerability management program?
- [ ] How mature are your organizations processes for incident detection and analysis?
- [ ] Does your organization understand and document the types of attackers it faces?
- [ ] Do you feel your organization can take on additional responsibilities in vulnerability management?
- [ ] How does your organizational policy influence how you manage updates if at all?
- [ ] Does the plan acknowledge the role that local organizations can play in representing local communities?
- [ ] Do projects in your organization consider and document likely threats?
- [ ] What are the environmental impacts of your organizations activities?
- [ ] What is your organizational structure for sharing information?
- [ ] Can organizations remediate vulnerabilities before exploitation?

CHECKLIST

- [ ] How does your threat model change by doing business with a partner organization?
- [ ] How many employees did your organization hire?
- [ ] Does your organization have any policies on software updates for machines?
- [ ] NOTES: