Primary Column	Column2	Column3	Column4
	Contact Information		
ITC	Sample		
Name	Joe Sample		
Email Address	Joe.Sample@sampleitc.org		
	Instructions		
Question #	If this were a real question, the text of the question would appear here...		
Objective	If this were a real question, a description of the objective would appear here...		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
0.01	***The assessment rubric questions appear in this section.***	Three dropdown choices:	For each self assessment question (each row), use this column to describe what you are doing to be in compliance, or conversely, explain why you are deficient. Use as much space as necessary.
0.02	*Use the dropdown to the right to indicate your response ===>*	Fully Meets the Objective	
0.03	*Or you can type the first letter of the response -- try "p" ===>*	Partially Meets the Objective	
0.04	*Try that again -- type "n" ===>*	Need Assistance to Meet the Objective	Again, please respond for each question (each row).
0.05	*Values are restricted -- try to type "x" . ===>*		
0.06			
	Basic		
Question 1	Does your organization keep track of computing devices on your private network and identify unauthorized devices?		
Objective	Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
1.01	Do You Utilize an Active Discovery Tool?		
1.02	Do You Use a Passive Asset Discovery Tool?		
1.03	Do You Use DHCP Logging to Update Asset Inventory?		
1.04	Do You Maintain Detailed Asset Inventory?		
1.05	Do You Maintain Asset Inventory Information?		
1.06	Do You Address Unauthorized Assets?		
1.07	Do You Deploy Port Level Access Control?		
1.08	Do You Utilize Client Certificates to Authenticate Hardware Assets?		
Question 2	Does your organization have a process for validating the security of purchased software products and services; and do you identify the installation of unauthorized software on your private network?		
Objective	Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
2.01	Do You Maintain Inventory of Authorized Software?		
2.02	Do You Ensure Software is Supported by Vendor?		
2.03	Do You Utilize Software Inventory Tools?		
2.04	Do You Track Software Inventory Information?		
2.05	Do You Integrate Software and Hardware Asset Inventories?		
2.06	Do You Address Unapproved Software?		
2.07	Do You Utilize Application Whitelisting?		
2.08	Do You Implement Application Whitelisting of Libraries?		
2.09	Do You Implement Application Whitelisting of Scripts?		
2.10	Do You Physically or Logically Segregate High Risk Applications?		

Question 3	Does your organization perform periodic application and network layer vulnerability testing or penetration testing against critical information systems?		
Objective	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
3.01	Do You Run Automated Vulnerability Scanning Tools?		
3.02	Do You Perform Authenticated Vulnerability Scanning?		
3.03	Do You Protect Dedicated Assessment Accounts?		
3.04	Do You Deploy Automated Operating System Patch Management Tools?		
3.05	Do You Deploy Automated Software Patch Management Tools?		
3.06	Do You Compare Back-to-back Vulnerability Scans?		
3.07	Do You Utilize a Risk-rating Process?		

Question 4	Do you restrict the use of Administrative Rights?		
Objective	The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
4.01	Do You Maintain Inventory of Administrative Accounts?		
4.02	Do You Change Default Passwords?		
4.03	Do You Ensure the Use of Dedicated Administrative Accounts?		
4.04	Do You Use Unique Passwords?		
4.05	Do You Use Multifactor Authentication For All Administrative Access?		
4.06	Do You Use Dedicated Workstations For All Administrative?		
4.07	Do You Limit Access to Scripting Tools?		
4.08	Do You Log and Alert on Changes to Administrative Group Membership?		
4.09	Do You Log and Alert on Unsuccessful Administrative Account Login?		

Question 5	Have you developed secure configuration baselines for hardware and software on mobile devices, laptops, workstations and servers?		
Objective	Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
5.01	Do You Establish Secure Configurations?		
5.02	Do You Maintain Secure Images?		
5.03	Do You Securely Store Master Images?		
5.04	Do You Deploy System Configuration Management Tools?		
5.05	Do You Implement Automated Configuration Monitoring Systems?		

Question 6	Do you maintain, monitor, and analyze Audit Logs?		
Objective	Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
6.01	Do You Utilize Three Synchronized Time Sources?		
6.02	Do You Activate Audit Logging?		
6.03	Do You Enable Detailed Logging?		
6.04	Do You Ensure Adequate Storage for Logs?		
6.05	Do You Centralize Log Management?		
6.06	Do You Deploy SIEM or Log Analytic Tools?		
6.07	Do You Regularly Review Logs?		
6.08	Do You Regularly Tune SIEM?		

Foundational			
Question 7	Do you enable email and web browser protections?		
Objective	Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
7.01	Do You Ensure Use of Only Fully Supported Browsers and Email Clients?		
7.02	Do You Disable Unnecessary or Unauthorized Browser or Email Client Plugins?		
7.03	Do You Limit Use of Scripting Languages in Web Browsers and Email Clients?		
7.04	Do You Maintain and Enforce Network-Based URL Filters?		
7.05	Do You Subscribe to URL-Categorization Service?		
7.06	Do You Log all URL Requests?		
7.07	Do You Use of DNS Filtering Services?		
7.08	Do You Implement DMARC and Enable ReceiverSide Verification Block Unnecessary File Types?		
7.09	Do You Sandbox All Email Attachments?		
Question 8	Have you enabled malware defenses?		
Objective	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
8.01	Do You Utilize Centrally Managed Anti-Malware Software?		
8.02	Do You Ensure Anti-Malware Software and Signatures are Updated?		
8.03	Do You Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies?		
8.04	Do You Configure Anti-Malware Scanning of Removable Devices?		
8.05	Do You Configure Devices to Not Auto-Run Content?		
8.06	Do You Centralize Anti-Malware Logging?		
8.07	Do You Enable DNS Query Logging?		
8.08	Do You Enable Command-Line Audit Logging?		
Question 9	Do you limit and control active network ports, services, and protocols?		
Objective	Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
9.01	Do You Associate Active Ports, Services and Protocols to Asset Inventory?		
9.02	Do You Ensure Only Approved Ports, Protocols and Services Are Running?		
9.03	Do You Perform Regular Automated Port Scans?		
9.04	Do You Apply Host-Based Firewalls or Port Filtering?		
9.05	Do You Implement Application Firewalls?		
Question 10	Describe your data recovery capabilities.		
Objective	The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
10.01	Do You Ensure Regular Automated Backups?		
10.02	Do You Perform Complete System Backups?		
10.03	Do You Test Data on Backup Media?		
10.04	Do You Protect Backups?		
10.05	Do You Ensure Backups Have At least One Non-Continuously Addressable Destination?		
Question 11	Have you developed secure configurations for network devices such as firewalls, routers, and switches?		

Objective	Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
11.01	Do You Maintain Standard Security Configurations for Network Devices?		
11.02	Do You Document Traffic Configuration Rules?		
11.03	Do You Use Automated Tools to Verify Standard Device Configurations and Detect Changes?		
11.04	Do You Install the Latest Stable Version of Any SecurityRelated Updates on All Network Devices?		
11.05	Do You Manage Network Devices Using MultiFactor Authentication and Encrypted Sessions?		
11.06	Do You Use Dedicated Workstations For All Network Administrative Tasks?		
11.07	Do You Manage Network Infrastructure Through a Dedicated Network?		

Question 12	Do you strictly define and defend your perimeter?		
Objective	Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
12.01	Do You Maintain an Inventory of Network Boundaries?		
12.02	Do You Scan for Unauthorized Connections across Trusted Network Boundaries?		
12.03	Do You Deny Communications with Known Malicious IP Addresses?		
12.04	Do You Deny Communication over Unauthorized Ports?		
12.05	Do You Configure Monitoring Systems to Record Network Packets?		
12.06	Do You Deploy Network-Based IDS Sensors?		
12.07	Do You Deploy Network-Based Intrusion Prevention Systems?		
12.08	Do You Deploy NetFlow Collection on Networking Boundary Devices?		
12.09	Do You Deploy Application Layer Filtering Proxy Server?		
12.10	Do You Decrypt Network Traffic at Proxy?		
12.11	Do You Require All Remote Logins to Use MultiFactor Authentication?		
12.12	Do You Manage All Devices Remotely Logging into Internal Network?		

Question 13	Have you defined how data is protected within and outside of your boundary?		
Objective	Deploy the processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
13.01	Do You Maintain an Inventory of Sensitive Information?		
13.02	Do You Remove Sensitive Data or Systems Not Regularly Accessed by Organization?		
13.03	Do You Monitor and Block Unauthorized Network Traffic?		
13.04	Do You Only Allow Access to Authorized Cloud Storage or Email Providers?		
13.05	Do You Monitor and Detect Any Unauthorized Use of Encryption?		
13.06	Do You Encrypt the Hard Drive of All Mobile Devices?		
13.07	Do You Manage USB Devices?		
13.08	Do You Manage System's External Removable Media's Read/Write Configurations?		
13.09	Do You Encrypt Data on USB Storage Devices?		

Question 14	Do you control access to facilities and information based on the need to know?		
Objective	The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***

14.01	Do You Segment the Network Based on Sensitivity?		
14.02	Do You Enable Firewall Filtering Between VLANs?		
14.03	Do You Disable Workstation to Workstation Communication?		
14.04	Do You Encrypt All Sensitive Information in Transit?		
14.05	Do You Utilize an Active Discovery Tool to Identify Sensitive Data?		
14.06	Do You Protect Information through Access Control Lists?		
14.07	Do You Enforce Access Control to Data through Automated Tools?		
14.08	Do You Encrypt Sensitive Information at Rest?		
14.09	Do You Enforce Detail Logging for Access or Changes to Sensitive Data?		

Question 15	How do you protect your wireless network?		
Objective	The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
15.01	Do You Maintain an Inventory of Authorized Wireless Access Points?		
15.02	Do You Detect Wireless Access Points Connected to the Wired Network?		
15.03	Do You Use a Wireless Intrusion Detection System?		
15.04	Do You Disable Wireless Access on Devices if it is Not Required?		
15.05	Do You Limit Wireless Access on Client Devices?		
15.06	Do You Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients?		
15.07	Do You Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data?		
15.08	Do You Use Wireless Authentication Protocols that Require Mutual, Multi-Factor Authentication?		
15.09	Do You Disable Wireless Peripheral Access to Devices?		
15.10	Do You Create Separate Wireless Network for Personal and Untrusted Devices?		

Question 16	Do you monitor and control account administration?		
Objective	Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
16.01	Do You Maintain an Inventory of Authentication Systems?		
16.02	Do You Configure Centralized Point of Authentication?		
16.03	Do You Require Multi-Factor Authentication?		
16.04	Do You Encrypt or Hash all Authentication Credentials?		
16.05	Do You Encrypt Transmittal of Username and Authentication Credentials?		
16.06	Do You Maintain an Inventory of Accounts?		
16.07	Do You Establish Process for Revoking Access?		
16.08	Do You Disable Any Unassociated Accounts?		
16.09	Do You Disable Dormant Accounts?		
16.10	Do You Ensure All Accounts Have An Expiration Date?		
16.11	Do You Lock Workstation Sessions After Inactivity?		
16.12	Do You Monitor Attempts to Access Deactivated Accounts?		
16.13	Do You Alert on Account Login Behavior Deviation?		

	Organizational		
Question 17	Have you implemented a Security Awareness Program?		
Objective	For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
17.01	Do You Perform a Skills Gap Analysis?		
17.02	Do You Deliver Training to Fill the Skills Gap?		

17.03	Do You Implement a Security Awareness Program?		
17.04	Do You Update Awareness Content Frequently?		
17.05	Do You Train Workforce on Secure Authentication?		
17.06	Do You Train Workforce on Identifying Social Engineering Attacks?		
17.07	Do You Train Workforce on Sensitive Data Handling?		
17.08	Do You Train Workforce on Causes of Unintentional Data Exposure?		
17.09	Do You Train Workforce Members on Identifying and Reporting Incidents?		

Question 18	Do you manage in-house developed and acquired software with security in mind?		
Objective	Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
18.01	Do You Establish Secure Coding Practices?		
18.02	Do You Ensure Explicit Error Checking is Performed for All In-House Developed Software?		
18.03	Do You Verify That Acquired Software is Still Supported?		
18.04	Do You Only Use Up-to-Date And Trusted Third-Party Components?		
18.05	Do You Only Standardized and Extensively Reviewed Encryption Algorithms?		
18.06	Do You Ensure Software Development Personnel are Trained in Secure Coding?		
18.07	Do You Apply Static and Dynamic Code Analysis Tools?		
18.08	Do You Establish a Process to Accept and Address Reports of Software Vulnerabilities?		
18.09	Do You Separate Production and Non-Production Systems?		
18.10	Do You Deploy Web Application Firewalls?		
18.11	Do You Use Standard Hardening Configuration Templates for Databases?		

Question 19	Have you developed and tested an incident Response Plan?		
Objective	Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
19.01	Do You Document Incident Response Procedures?		
19.02	Do You Assign Job Titles and Duties for Incident Response?		
19.03	Do You Designate Management Personnel to Support Incident Handling?		
19.04	Do You Devise Organization-wide Standards for Reporting Incidents?		
19.05	Do You Maintain Contact Information For Reporting Security Incidents?		
19.06	Do You Publish Information Regarding Reporting Computer Anomalies and Incidents?		
19.07	Do You Conduct Periodic Incident Scenario Sessions for Personnel?		
19.08	Do You Create Incident Scoring and Prioritization Schema?		

Question 20	Do you conduct penetration testing or red team exercises?		
Objective	Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.		
	Self Assessment	***Answer Each Question Below***	***Describe Compliance or Explain Deficiency for each item***
20.01	Do You Establish a Penetration Testing Program?		
20.02	Do You Conduct Regular External and Internal Penetration Tests?		
20.03	Do You Perform Periodic Red Team Exercises?		
20.04	Do You Include Tests for Presence of Unprotected System Information and Artifacts?		
20.05	Do You Create a Test Bed for Elements Not Typically Tested in Production?		
20.06	Do You Use Vulnerability Scanning and Penetration Testing Tools in Concert?		
20.07	Do You Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards?		
20.08	Do You Control and Monitor Accounts Associated with Penetration Testing?		