Primary Column	Column2	Column3	Column4
	Contact Information		
ITC	Sample		
Name	Joe Sample		
Email Address	Joe.Sample@sampleitc.org		

	la samuadi ana		
	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			

	Pania		
Question 1	Basic 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 Objective	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? 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? Do You Implement Application Whitelisting of Libraries?		
2.08	Do You Implement Application Writtelisting of Scripts?		
2.09 2.10	Do You Implement Application Whitelisting of Scripts? Do You Physically or Logically Segregate High Risk Applications?		
2.10	Do Tou Fifysically of Logically Segregate Flight Risk Applications?		

Question 3 Authoritability lesting or penetration lesting against artical information systems? Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. Authoritable Autho		Does your organization perform periodic application and network layer		
Splective continuously acquire, assess, and take action on new information in order to identify with restabilities, remediate, and minimize the window of opportunity for all actions. 5.01 Do You fun Authentiate Vinterability Scorning Test? 5.02 Do You Performance of English Scorning Test? 5.03 Do You Provide Confidence of Spatial Management Tools? 5.04 Do You Congrain Back-Oscade Authentiality Scorning? 5.05 Do You Congrain Back-Oscade Authentiality Scorning? 5.06 Do You Congrain Back-Oscade Authentiality Scorning? 5.07 Do You Congrain Back-Oscade Authentiality Scorning? 5.08 Do You Congrain Back-Oscade Authentiality Scorning? 5.09 Do You Congrain Back-Oscade Authentiality Scorning? 5.00 Do You Congrain Back-Oscade Authentiality Scorning? 5.00 Do You Congrain Back-Oscade Authentiality Scorning? 5.00 Do You Congrain Back-Oscade Authentiality Scorning? 6.00 Do You Congrain Back-Oscade Authentiality Authorities A	Ougstion 3			
Continuously acquire, assess, and take action on new information in operating for attackers. Self Assessment Assess Assess Assessment Assessme	Question 5			
Objective order to lentify violentabilities, remediate, and minimize the window of opportunity for attackers. Soft Assessment Ob You Plan Automated Violentability Scarring Tools? Ob You Plan Automated Violentability Scarring Tools? Ob You Deep Violentability Scarring Tools? Ob You Scarring Automated Coprating System Patch Management Tools? Ob You Deep Violentability Scarring Tools? Ob You Company Interests Assert Violentability Scarring Tools? Ob You Company Interests Assert Violentability Scarring Tools? The processes and tools used to track/control/prevent/connect the use, assignment, and configuration of administrative Rights? The processes and tools used to track/control/prevent/connect the use, assignment, and configuration of administrative Rights? The processes and tools used to track/control/prevent/connect the use, assignment, and configuration of administrative Rights? The processes and tools used to track/control/prevent/connect the use, assignment, and configuration of administrative Rights? The processes and tools used to track/control/prevent/connect the use, assignment, and configuration and minimizative Account? Ob You Control Administrative Account? Ob You Control Processes and tools used to track/control/prevent/connect the use, assignment, and the other of the development of the Administrative Account? Ob You Control Processes Scarrings Good of the Administrative Account? Ob You Control Processes Scarrings Good of the Administrative Account? Ob You Control Processes Scarrings Good Administrative Account Configuration Acco		· · · · · · · · · · · · · · · · · · ·		
Self Assessment Do You Plan Antonized Multiversity Scienting Town 1 Do You Design Antonized Scheme Plan Management Toxis 2 Do You Congree Back-boak Wherlothly Scient 7 Do You Congree Back-boak Wherlothly Scient 7 Do You Congree Back-boak Wherlothly Scient 7 Do You Used Scientific He use of Administrative Rights? The processes and tools used to inackcontrol/preventionment the use, assignment, and configuration of administrative privileges on computers, networks, and applications. The processes and tools used to inackcontrol/preventionment the use, assignment, and configuration of administrative privileges on computers, networks, and applications. Assert Scientific Scientifi	Objective			
Self Assessment One You Ran Automated Vulnerability Scarring Tors? 100	Objective			
Do You Floring Autheritation Visional Residence of Committed Processors of Com			Answer Each Question Below	Describe Compliance or Explain Deficiency for each item
Do You Perform Authenticated Valentality Scenning? Do You Desptoy Authentiand Coperating System Perfor Menagement Tools? Do You Desptoy Authentiand Coperating System Performance of Coperating Systems Performance of Coperating Performance of Coperati	2.01			,,,,
Do You Protect Declared Assessment Accounts? 104 Do You Deploy Automated Spreamy System Patch Management Tools? 105 Do You Deploy Automated Spreamy System Patch Management Tools? 106 Do You Deploy Automated Spreamy Patch Management Tools? 107 Do You Ulties a Relactionary Patch Management Tools? 108 Do You Care Patch Earth Care Management Tools? 108 Do You Care Patch Care Management Patch Management Tools? 109 Do You Ulties a Relactionary Automated Solvers Patch Management Tools? 109 Do You Ulties And Configuration of administrative Patch Patch Patch Visionary Automated Solvers Patch Patch Visionary Automated Solvers Patch Patch Visionary Automated Solvers Patch Patch Visionary Automated Patch Patch Visionary Automated Patch Patch Visionary Automated Patch P				
Do You Deploy Automated Operating System Patch Management Tools? Do You Deploy Automated Scheeper Start Management Tools?				
Do You Corpor Automated Schrave Patch Management Tode? Do You Corpor Back-to-back Valendarially Scare? Ouestion 4 Do you restrict the use of Administrative Rights? The processes and bods used to tradecontrolly event correct the use, astignment, and on Capital Company of Administrative Privileges on Computers, and spiritudes and and s				
Do you Compare Back-chack Valverability Scanar? Question 4 Do you restrict the use of Administrative Rights? The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications. Processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications. Self Assessment Areser Each Question Relea 401 Do You Change Default Pleasurers? 102 Do You Change Default Pleasurers? 103 Do You Change Default Pleasurers? 104 105 Do You Use Unique Passworks? 105 Do You Use Unique Passworks? 106 Do You Use Unique Passworks? 107 Do You Use Unique Passworks? 108 Do You Use Unique Passworks? 109 Do You Use Unique Passworks? 109 Do You Use Default Worksteins For All Administrative Access? 109 Do You Use Unique Passworks? 109 Do You Use Unique Passworks? 109 Do You Use Unique Passworks? 109 Do You Use Only on the Administrative Access? 109 Do You Use Only on the Administrative Access? 109 Do You Use Only on the Administrative Access? 109 Do You Use Only on the Administrative Access? 109 Do You Use Only on the Administrative Croup Membership? 109 Do You Use Only on the Administrative Croup Membership? 109 Do You Use Only on the Administrative Access the Administrative Croup Membership? 109 Do You Use Only on the Administrative Croup Membership? 109 Do You Use Only on the Administrative Croup Membership? 109 Do You Use Only on the Administrative Access the Administrative Process the Adminis				
Do you restrict the use of Administrative Rights? The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications. ***Solf Assessment** **Solf Assessment** **Solf Assessment** **On You Maintain Inventory of Amministrative Accounts? **Do You Change Default Preserved?* **Do You Use Intelligent Authorities of Administrative Accounts?* **Do You Use Multifactor Authorities of Administrative Accounts?* **Do You Use Multifactor Authorities of Administrative Accounts?* **Do You Use Intelligent Authorities of Administrative Account Ligan?* **Do You Use and Alent On Changes to Administrative Account Ligan?* **Do You Use and Alent On Changes to Administrative Account Ligan?* **Do You Use and Alent On Changes to Administrative Account Ligan?* **Do You Use and Alent On Changes to Administrative Account Ligan?* **Do You Use and Alent On Changes Configuration baselines for hardware and solfware on mobile devices, liptops, workstations and servers? **Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, liptops, surveys, and workstations of Intelligent Authorities Account Ligan.** **Do You Use and Alent Changes Configuration Account Ligan.** **Do You Use and Alent Changes Configuration Amministrative Account Ligan.** **Do You Use Account State Intelligent Authorities Account Ligan.** **Do You Use Account State Intelligent Authorities Account Ligan.** **Do You Use Account Account Account Changes Continued Account Ligan.** **Do You Use Account Account Account Changes				
Objective assignment, and configurations of administrative Rights? The processes and look used to track/control/provent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications. Solf Assessment Answer Each Question Below Describe Compitance or Egitan Dedicisory for each item 101 De You Change Default of Administrative Accounts? 102 103 104 105 105 105 105 105 105 105				
Dejective assignment, and configuration of administrative privileges on computers, networks, and applications. Self Assessment An entworks, and applications are serviced as a computer of administrative privileges on computers, and the computers, and applications are serviced as a computer of administrative Accounts? 4.01 Do You User business because the computer of Annew Each Question Below Describe Compilator or Explain Deficiency for each Rem Do You Use Humilar Describes and Security of the Compilator of Explain Deficiency for each Rem Do You Use Multifactor Authoritectation For All Administrative Accousts? 4.02 Do You Use Multifactor Authoritectation For All Administrative Access? 4.03 Do You Use Multifactor Authoritectation For All Administrative Access? 4.04 Do You Use Production Provided Authoritectation For All Administrative Access? 4.05 Do You Use Production Provided Authoritectation For All Administrative Access? 4.06 Do You Use Production Provided Authoritectation For All Administrative Access? 4.07 Do You User Aller for on Unsuccessful Administrative Access? 4.08 Do You User Aller for on Unsuccessful Administrative Access? 4.09 Do You User Aller for on Unsuccessful Administrative Access? 4.09 Do You User Aller for on Unsuccessful Administrative Access? 5.00 Do You Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, services and settings. 5.01 Do You Establish Socruc Foregore Provided Track Forem exploiting vulnerable services and settings. 5.02 Do You Selablish Source Configuration Administrative Access Acces	5.01	Bo Tod Guilzo d Flori Falling F Foodoo.		
Dejective assignment, and configuration of administrative privileges on computers, networks, and applications. Self Assessment An entworks, and applications are serviced as a computer of administrative privileges on computers, and the computers, and applications are serviced as a computer of administrative Accounts? 4.01 Do You User business because the computer of Annew Each Question Below Describe Compilator or Explain Deficiency for each Rem Do You Use Humilar Describes and Security of the Compilator of Explain Deficiency for each Rem Do You Use Multifactor Authoritectation For All Administrative Accousts? 4.02 Do You Use Multifactor Authoritectation For All Administrative Access? 4.03 Do You Use Multifactor Authoritectation For All Administrative Access? 4.04 Do You Use Production Provided Authoritectation For All Administrative Access? 4.05 Do You Use Production Provided Authoritectation For All Administrative Access? 4.06 Do You Use Production Provided Authoritectation For All Administrative Access? 4.07 Do You User Aller for on Unsuccessful Administrative Access? 4.08 Do You User Aller for on Unsuccessful Administrative Access? 4.09 Do You User Aller for on Unsuccessful Administrative Access? 4.09 Do You User Aller for on Unsuccessful Administrative Access? 5.00 Do You Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, services and settings. 5.01 Do You Establish Socruc Foregore Provided Track Forem exploiting vulnerable services and settings. 5.02 Do You Selablish Source Configuration Administrative Access Acces	Question 4	Do you restrict the use of Administrative Rights?		
Self Assessment Self Assessment Self Assessment Ansew Each Question Betwoe Self Assessment Ansew Each Question Betwoe Describe Compliance or Equisin Duticisincy Ansex Heart Rem Ansew Each Question Betwoe Ansew Each Question Betwoe Ansew Each Question Betwoe Ansew Each Question Betwoe Describe Compliance or Equisin Duticisincy Ansex Heart Rem Ansew Each Question Betwoe Ansew Each Question Betwoe Describe Compliance or Equisin Duticisincy Ansex Heart Rem Ansew Each Question Betwoe Describe Compliance or Equisin Duticisincy Ansex Heart Rem Ansew Each Question Betwoe Describe Compliance or Equisin Duticisincy Ansex Heart Rem Ansew Each Question Betwoe Describe Compliance or Equisin Duticisincy Ansex Heart Rem Ansew Each Question Betwoe Describe Compliance or Equisin Duticisincy Ansex Heart Rem Describe Compliance or Equisin Duticisincy Ansex Heart Rem Ansew Each Question Betwoe Describe Compliance or Equisin Duticisincy Ansex Heart Question Betwoe Describe Compliance or Equisin Duticisincy Ansex Heart Question Betwoe Describe Compliance or Equisin Duticisincy				
RetWorks, and applications. Solf Assessment Answer Each Question Bolow Describe Compliance or Explain Deficiency for each item 4.01	Objective			
Self Assesment Answer Each Question Below Describe Compliance or Explain Deficiency for each item 1 4.01				
401 Do You Maintain Inventory of Administrative Accounts? 402 Do You Change Default Passwords? 403 Do You Unique Passwords? 404 Do You Use Unlique Passwords? 405 Do You Use Multiflactor Authentication For All Administrative Access? 406 Do You Use Defaulted Workstofann For All Administrative? 407 Do You Use Multiflactor Authentication For All Administrative? 408 Do You Use Defaulted Workstofann For All Administrative? 409 Do You Use Defaulted Workstofann For All Administrative Access? 409 Do You Use and Alet no Changes to Administrative Group Membership? 409 Do You Use and Alet no Insuccessful Administrative Croup Membership? 409 Do You Use and Alet no Insuccessful Administrative Account Login? 409 The You go and Alet no Insuccessful Administrative Account Login? 409 The You developed secure configuration baselines for hardware and Software on mobile devices, laptops, workstations and servers? 400 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. 501 Do You Establish Secure Configuration Management Tools? 502 Do You Walkitain Secure Inages? 503 Do You Securely Storm Master Images? 504 Do You Deploy System Configuration Monitoring Systems? 408 Do You Deploy System Configuration Monitoring Systems? 509 Do You Utilize Three Synchronized Time Sources? 509 Do You Utilize Three Synchronized Time Sources? 601 Do You Utilize Three Synchronized Time Sources? 602 Do You Ackviete Audit Logging? 603 Do You Charlate Logh Management? 605 Do You Deploy System Configuration Management? 606 Do You Deploy System Configuration Management? 607 Do You Deploy System Configuration Management? 608 Do You Deploy System Configuration Management? 609 Do You Deploy Stefan Configuration Management? 609 Do You Deploy Stefan Configuration Management? 609 Do You Deploy Stefan Configuration Man			Answer Each Question Below	Describe Compliance or Explain Deficiency for each item
1	4.01			
10 You Use Unique Passwords? 10 You Use Unique Passwords? 10 You Use Delicated Workstations For All Administrative Access? 10 You Use Delicated Workstations For All Administrative Access? 10 You Log and Alert on Changes to Administrative Group Membership? 10 You Log and Alert on Unsuccessful Administrative Account Login? 10 You Log and Alert on Unsuccessful Administrative Account Login? 10 You Log and Alert on Unsuccessful Administrative Account Login? 10 You Use provided secure configuration baselines for hardware and software on mobile devices, laptops, workstations and servers? 10 Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, saptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. 10 De You Establish Secure Configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. 10 De You Sead Secure Store Nater Images? 10 De You Seaverly Store Nater Images? 10 De You Use Seaverly Store Nater Images? 10 De You Use Seaverly Store Nater Images? 10 De You Uniquement Automated Configuration Management Tools? 10 De You Uniquement Automated Configuration Monitoring Systems? 10 De You Use Three Synchronized Time Sources? 10 De You Utilize Three Synchronized Time Sources? 10 De You Certainize Log Management? 10 De You Deploy Stell Art Log Analytic Tools? 10 De You Deploy Stell Art Log Analytic Tools? 10 De You Deploy Stell Art Log Analytic Tools? 10 De You Deploy Stell Art Log Analytic Tools?	4.02			
4.05 Do You Use Multifactor Authentication For All Administrative Access? 4.07 Do You Limit Access to Scripting Tools? 4.08 Do You Limit Access to Scripting Tools? 4.09 Do You Log and Aller on Changes to Administrative Group Membership? 4.09 Do You Log and Aller on Changes to Administrative Group Membership? 4.09 Do You Log and Aller on Changes to Administrative Account Login? 4.09 Do You Log and Aller on Changes to Administrative Account Login? 4.09 Do You Log and Aller on Changes to Administrative Account Login? 4.09 Do You Log and Aller on Changes to Administrative Account Login? 4.09 Do You Log and Aller on Changes to Administrative Account Login? 4.09 Do You Log and Aller on Changes to Administrative Account Login? 4.00 Do You Log and Aller on Changes to Administrative Account Login? 5.00 Do You Ministrative Crue To revent attackers from exploiting vulnerable services and settings. 5.01 Do You Establish Secure Configuration Management and change control process in order to prevent attackers from exploiting vulnerable services and settings. 5.01 Do You Establish Secure Configurations? 5.02 Do You Ministrati Secure Configurations? 5.03 Do You Securely Store Master Images? 5.04 Do You Ministrative Count Configuration Management Tools? 5.05 Do You Implement Automated Configuration Monitoring Systems? 6.06 Do You Utilize Three Synctroized Time Sources? 6.07 Do You Deptoy Steller Or Configuration Monitoring Systems? 6.08 Do You Centralize Log Management? 6.09 Do You Ensure Adequate Storage for Login? 6.00 Do You Deptoy Steller or Log Analytic Tools? 6.01 Do You Deptoy Steller or Log Analytic Tools? 6.07 Do You Deptoy Steller or Log Analytic Tools?	4.03	Do You Ensure the Use of Dedicated Administrative Accounts?		
4.06 Do You Use Decicated Workstations For All Administrative? 4.07 Do You Limit Access to Septinging Tools? 4.08 Do You Log and Alert on Changes to Administrative Account Login? 4.08 Do You Log and Alert on Unsuccessful Administrative Account Login? 4.09 Have you developed secure configuration baselines for hardware and software on mobile devices, laptops, workstations and servers? 5.5 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** 5.01 Do You Establish Secure Configurations? 5.02 Do You Maintain Secure langues? 5.03 Do You Securely Store Master Images? 5.04 Do You Deptoy System Configuration Management Tools? 5.05 Do You Implement Automated Configuration Menitoring Systems? **Question 6 **Do You Implement Automated Configuration Menitoring Systems?** **Self Assessment** **Answer Each Question Below** **Describe Compilance or Explain Deficiency for each item** **Describe Compilance or Explain De	4.04			
4.07	4.05	Do You Use Multifactor Authentication For All Administrative Access?		
4.09 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 Software on mobile devices, laptops, workstations and servers? Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration anagement and change control process in order to prevent attackers from exploiting vulnerable services and settings. Self Assessment Do You Establish Secure Configurations? 5.01 Do You Scarely Store Master Images? 5.03 Do You Scarely Store Master Images? 5.04 Do You Deploy System Configuration Management 1 Tools? 5.05 Do You unjenent Automated Configuration Management 7 Tools? 5.06 Do You unjenent Automated Configuration Monitoring Systems? Question 6 Do You Unitiat, monitor, 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 Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Describe Compliance or Explain Deficiency for each item Answer Each Question Belo	4.06	Do You Use Dedicated Workstations For All Administrative?		
Augustion 5 Answer Each Question 6 Bo You Log and Alert on Unsuccessful Administrative Account Login? Have you developed secure configuration baselines for hardware and software on mobile devices, laptops, workstations and servers? Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and settings. Belf Assessment Answer Each Question Below Describe Compliance or Explain Deficiency for each item Self Assessment Answer Each Question Below Describe Compliance or Explain Deficiency for each item Sol De You Securely Store Master Images? Do You Use Secure Configuration Management Tools? Do You Use Secure Vote Mater Images? Answer Each Question Below Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficiency for each item Describe Compliance or Explain Deficiency for each item Answer Each Question Below Describe Compliance or Explain Deficie	4.07	Do You Limit Access to Scripting Tools?		
Have you developed secure configuration baselines for hardware and software on mobile devices, laptops, workstations and servers? 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 Bellow 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 Umplement Automated Configuration Monitoring Systems? Question 6 Do You maintain, monitor, and analyze Audit Logs? Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack. Self Assessment Answer Each Question Bellow 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 Deploy SiEM or Log Analytic Tools? 6.06 Do You Deploy SiEM or Log Analytic Tools? 6.07 Do You Regularly Review Logs?	4.08	Do You Log and Alert on Changes to Administrative Group Membership?		
Objective scarring of the devices, laptops, workstations and servers? Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and Objective workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. ***Self Assessment** Self Assessment** ***Self Assessment** ***Solice** ***Device** **Device** ***Device** ***Device** ***Device** ***Device** **Device** ***Device** ***Device** ***Device** ***Device** **Device** ***Device** **Device** **Dev	4.09	Do You Log and Alert on Unsuccessful Administrative Account Login?		
Objective scarring of the devices, laptops, workstations and servers? Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and Objective workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. ***Self Assessment** Self Assessment** ***Self Assessment** ***Solice** ***Device** **Device** ***Device** ***Device** ***Device** ***Device** **Device** ***Device** ***Device** ***Device** ***Device** **Device** ***Device** **Device** **Dev				
Objective or mobile devices, laptops, workstations and servers? 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 Umplement 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? 6.03 Do You Cathale Audit Logging? 6.04 Do You Enable Detailed Logging? 6.05 Do You Cantralize Log Management? 6.06 Do You Centralize Log Management? 6.07 Do You Regularly Review Logs?				
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 Uniperment Automated Configuration Monitoring Systems? Question 6 Do you maintain, monitor, and analyze Audit Logs? Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack. 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 Enable Detailed Logging? 6.05 Do You Centralize Log Management? 6.06 Do You Centralize Log Management? 6.07 Do You Deploy SIEM or Log Analytic Tools? 6.08 Do You Centralize Log Management? 6.09 Tool Regularly Review Logs?	Question 5			
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 Self Assessment Sol Do You Establish Secure Configurations? Do You Maintain Secure Images? 5.02 Do You Maintain Secure Images? 5.03 Do You Deploy System Configuration Management Tools? 5.04 Do You Deploy System Configuration Monitoring Systems? Question 6 Do you maintain, monitor, and analyze Audit Logs? 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 Do You Utilize Three Synchronized Time Sources? 6.01 Do You Enable Detailed Logging? 6.03 Do You Enable Detailed Logging? 6.04 Do You Enable Detailed Logging? 6.05 Do You Centralize Log Management? 6.06 Do You Centralize Log Management? 6.07 Do You Replay Review Logs?				
Objective 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? 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 Enable Detailed Logging? 6.05 Do You Centralize Log Management? 6.06 Do You Centralize Log Management? 6.07 Do You Reploy SIEM or Log Analytic Tools? 6.07 Do You Reploy SIEM or Log Analytic Tools? 6.07 Do You Reploy Review Logs?				
control process in order to prevent attackers from exploiting vulnerable services and settings. Self Assesment Solf Answer Each Question Below Do You Establish Secure Configurations? 5.01 Do You Securely Store Master 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? 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 Enable Detailed Logging? 6.05 Do You Centralize Log Management? 6.06 Do You Deploy SilEM or Log Analytic Tools? 6.07 Do You Replay Review Logs?				
Self Assesment Answer Each Question Below Describe Compiliance 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? 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 Compiliance or Explain Deficiency for each item 6.01 Do You Utilize Three Synchronized Time Sources? 6.02 Do You Activate Audit Logging? 6.04 Do You Enable Detailed Logging? 6.05 Do You Centralize Log Management? 6.06 Do You Deploy SIEM or Log Analytic Tools? 6.07 Do You Deploy SIEM or Log Analytic Tools? 6.07 Do You Regularly Review Logs?	Objective			
Self Assesment 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 Objective Occllect, manage, and analyze Audit Logs? 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 Enable Detailed Logging? 6.05 Do You Centralize Log Management? 6.06 Do You Deploy SiEM or Log Analytic Tools? 6.07 Do You Regularly Review Logs?				
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? 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 Enable Detailed Logging? 6.05 Do You Centralize Log Management? 6.06 Do You Deploy SIEM or Log Analytic Tools? 6.07 Do You Regularly Review Logs?		<u> </u>		
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? 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 Enable Detailed Logging? 6.05 Do You Deploy SIEM or Log Analytic Tools? 6.06 Do You Deploy SIEM or Log Analytic Tools? 6.07 Do You Regularly Review Logs?			Answer Each Question Below	Describe Compliance or Explain Deficiency for each item
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? 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 Deploy SIEM or Log Analytic Tools? 6.06 Do You Deploy SIEM or Log Analytic Tools? 6.07 Do You Regularly Review Logs?		•		
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? 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 Ensure Adequate Storage for Logs? 6.04 Do You Ensure Adequate Storage for Logs? 6.05 Do You Centralize Log Management? 6.06 Do You Deploy SISEM or Log Analytic Tools? 6.07 Do You Regularly Review Logs?				
Do You Implement Automated Configuration Monitoring Systems? Question 6 Do you maintain, monitor, and analyze Audit Logs? 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?		· · · · · · · · · · · · · · · · · · ·		
Question 6 Objective Objec				
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?	5.05	Do You Implement Automated Configuration Monitoring Systems?		
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?	Ougstion 6	Do you maintain, manitar, and analyze Audit Logo?		
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?	Question 6			
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?	Objective			
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?		,	Answer Each Question Below	Describe Compliance or Explain Deficiency for each item
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?	0.04			
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?				
6.04 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?		88 8		
6.05 Do You Centralize Log Management? 6.06 Do You Deploy SIEM or Log Analytic Tools? 6.07 Do You Regularly Review Logs?		77.7		
6.06 Do You Deploy SIEM or Log Analytic Tools? 6.07 Do You Regularly Review Logs?				
6.07 Do You Regularly Review Logs?				
2- 1- 1- Garay Land State.				
	0.00			

	Foundational		
Question 7	Do you enable email and web browser protections?		
Quodilon .	Minimize the attack surface and the opportunities for attackers to		
Objective	manipulate human behavior though their interaction with web browsers		
Objective	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		
7.06	File Types?		
7.09	Do You Sandbox All Email Attachments?		
0 " 0			
Question 8	Have you enabled malware defenses?		
	Control the installation, spread, and execution of malicious code at		
Objective	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
0.01	Do You Utilize Centrally Managed Anti-Malware Software?		
8.01 8.02	Do You Ensure Anti-Malware Software and Signatures are Updated?		
0.02	Do You Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit		
8.03	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?		
	Manage (track/control/correct) the ongoing operational use of ports,		
Objective	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?		
Ougstion 10	Deparities your data recovery canabilities		
Question 10	Describe your data recovery capabilities. The processes and tools used to properly back up critical information		
Objective			
	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?		
10.01 10.02	Do You Perform Complete System Backups?		
10.02	Do You Test Data on Backup Media?		
10.03	Do You Protect Backups?		
	Do You Ensure Backups Have At least One Non-Continuously Addressable		
10.05	Destination?		
	Have you developed secure configurations for network devices such as		
Question 11	firewalls, routers, and switches?		

	Establish, implement, and actively manage (track, report on, correct) the		
01.1 "	security configuration of network infrastructure devices using a rigorous		
Objective	configuration management and change control process in order to		
	prevent attackers from exploiting vulnerable services and settings.		
	O. W. Assessment	Answer Each Question Below	Describe Compliance or Explain Deficiency for each item
44.04	Self Assessment Do You Maintain Standard Security Configurations for Network Devices?	Answer Lach Question Delow	Describe compliance of Explain Dencioney for each item
11.01	to the state of th		
11.02	Do You Document Traffic Configuration Rules?		
11.03	Do You Use Automated Tools to Verify Standard Device Configurations and Detect Changes?		
	Do You Install the Latest Stable Version of Any SecurityRelated Updates on All Network		
11.04	Devices?		
44.05	Do You Manage Network Devices Using MultiFactor Authentication and Encrypted		
11.05	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		
02,000	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 12.10	Do You Deploy Application Layer Filtering Proxy Server? Do You Decrypt Network Traffic at Proxy?		
12.10	Do You Require All Remote Logins to Use MultiFactor Authentication?		
12.12	Do You Manage All Devices Remotely Logging into Internal Network?		
12.12	20 You manago / in 20 hose remotely 20 ggmg into internal rections.		
0 " 10	Have you defined how data is protected within and outside of your		
Question 13	boundary?		
	Deploy the processes and tools used to prevent data exfiltration, mitigate		
Objective	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 13.08	Do You Manage USB Devices? Do You Manage System's External Removable Media's Read/Write Configurations?		
	Do You Encrypt Data on USB Storage Devices?		
13.09	DO TOU LINGSPIL DAILA OIT COD STOTAGE DEVICES!		
	Do you control access to facilities and information based on the need to		
Question 14	know?		
	The processes and tools used to track/control/prevent/correct secure		
	access to critical assets (e.g., information, resources, systems)		
Objective	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?		
14.03	Bo Four Enterior Botali Edgging for Adocad of Changes to Constitute Bata.		
Question 15	How do you protect your wireless network?		
Question 15			
OLL C	The processes and tools used to track/control/prevent/correct the		
Objective	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?		
45.07	Do You Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data?		
15.07			
15.08	Do You Use Wireless Authentication Protocols that Require Mutual, Multi-Factor		
13.06	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?		
	Actively manage the life cycle of system and application accounts - their		
Objective	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?		
	Do You Encrypt or Hash all Authentication Credentials?		
16.04	**		
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		
Objective	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		
16.02	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?		
	Do You Establish a Process to Accept and Address Reports of Software Vulnerabilities?		
18.08			
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?		
	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)		
Objective			
	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.	Annual Fact Overting Below	Describe Committees on Francisco Deficiency for each item
	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?		
	Test the overall strength of an organization's defense (the technology,		
Objective	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?		
20.02	Do You Perform Periodic Red Team Exercises?		
	Do You Include Tests for Presence of Unprotected System Information and Artifacts?		
20.04	20 Tod mode Tosts for Freschice of Onprotected Cystem monifolion and Attracts?		
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?		
	Do You Ensure Results from Penetration Test are Documented Using Open, Machine-		
20.07	readable Standards?		
20.07 20.08			