Initial	Submitter Details

Welcome to the Cybersecurity Questionnaire (Ref:EX01)

This questionnaire has been developed for the purpose of measuring your cybersecurity capability. Your company has been asked to complete this questionnaire by one or more of the Exostar partners. The information you provide will be used to manage your cybersecurity risk.

By responding to this questionnaire, you represent that you have appropriate authority to complete the questionnaire on behalf of your company. The Exostar partners may separately use the information for risk assessment. Your answers to the questionnaire will be treated as your company's Proprietary information by Exostar or the Exostar partners and can only be changed by your company. Please do not include any Competitively Sensitive information or Proprietary information of any customer including any Subscriber Company in your answers in the questionnaire. The questionnaire may be amended without notice.

Guidance

CSC v5.1

Initial	Submitter Details

Introduction (Ref:EX01a)

The recommended steps to complete this questionnaire are as follows:

For scoping purposes, this questionnaire must cover your company’s entire Enterprise IT infrastructure as long as all elements are governed by the same security policies. If multiple networks are governed by differing security policies, separate questionnaires may be required. In that case, please contact your Point of Contact at the Exostar Partner with whom you have a business relationship for additional guidance.

Guidance

CSC v5.1

Initial	Submitter Details

Instructions (Ref:EX01b)

The Cybersecurity Questionnaire was built upon the foundation of the Critical Controls, a recommended set of actions for cyber defense that provide specific and actionable ways to thwart the most pervasive attacks. (Refer to links provided in Guidance box for more information and history on the Critical Controls).

The questionnaire is structured upon 22 "Control Families". Within each Control Family, there are several Control Activities to which one of the following responses is required:

- A tick mark indicates the control has been fully implemented
- No tick mark indicates the control has NOT been fully implemented

You may download a blank questionnaire to assist your team in formulating your responses prior to input in this questionnaire. (see the dropdown list in the Reports button on the left side of summary of the form). If at anytime you need to exit the questionnaire, please click on Save & Exit button to ensure that your responses are saved in the system. Upon return, the system will return you to the last page visited.

Once your questionnaire has been completed and submitted, a Capability Level result will be calculated based upon the responses provided. A report will then be made available that provides the determination of your overall Capability Level, the capability level achieved for each Control Family and a set of recommended control activities that are needed to achieve a higher capability level.

Capability Levels are defined as follows:

- Level 0 - Indicates no or minimal cyber risk management program; significant cyber protections are lacking; additional risk mitigations must be implemented
- Level 1 - Indicates a basic level cyber risk management program; some protections in place but additional risk mitigations must be implemented
- Level 2 - Indicates a moderate level cyber risk management program; good protections in place but additional risk mitigations are required to protect sensitive information
- Level 3 - Indicates a solid performing cyber risk management program; strong protections have been implemented; Advanced threats are understood and taking steps to address with specific controls; Additional risk mitigations are likely needed to protect against advanced attacks
- Level 4 - Indicates a cyber risk management program that can detect, protect against, and respond to advanced threats; Specific advanced controls are implemented
- Level 5 - Indicates a cyber risk management program that can detect, protect against, and respond to advanced threats; Specific advanced controls are implemented and optimized on an ongoing basis

Your company must have implemented all control activities contained within a capability level to attain that capability level and prior to being able to meet the next capability level. Refer to Control Activity to Capability Level Matrix in Guidance Section to the right.

A minimum Capability Level of 3 is encouraged to ensure a solid performing cyber risk management program is in place. It is recognized that not all companies will be able to immediately attain Capability Level 3. That said, the results should be used to prioritize and implement additional controls that may be needed to improve the health of your company's cybersecurity posture.

The Exostar Partners may use your company's resulting Capability score as an indicator to formulate business risk decisions. Some Exostar Partners may require different minimum Capability Levels (higher or lower) be attained depending upon the nature and sensitivity of work that is performed. In addition, some Exostar Partners may leverage your responses to conduct further

Guidance

CSC = Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ – provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

Control Activity to Capability Level Matrix:
www.myexostar.com/downloadasset.aspx

CSC v5.1

assessment and/or audit reviews of your controls.

It is imperative that you keep this questionnaire updated as additional controls are implemented and improvements are made to your cybersecurity posture.

Initial	**Submitter Details**	1.Device Inventory

Q Who in your organization is responsible for providing the answers to this cybersecurity questionnaire? (Ref:EX002)

Name :

Job Title :

Email :

Name :

Job Title :

Email :

Name :

Job Title :

Email :

Guidance

System/Technical Issues Questions:
PIM Website:www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ – provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

Submitter Details	1.Device Inventory	2.Software Inventory

Q In relation to Inventory Of Authorized and Unauthorized Devices, which of the following Capability Level 1 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX03)

□ Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to an organization's public and private network(s). Both active tools that scan through network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed. (CSC 1-1)

□ Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network. (CSC 1-4)

□ Deploy dynamic host configuration protocol (DHCP) server logging, and utilize a system to improve the asset inventory and help detect unknown systems through this DHCP information. (CSC 1-2)

Guidance

Control 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.

The following are Capability Level 2 controls:

- CSC 1-1
- CSC 1-4

The following are Capability Level 3 controls:

- CSC 1-2

There are no Capability Level 1 controls for this control family.

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

Submitter Details	1.Device Inventory	2.Software Inventory

Q In relation to Inventory Of Authorized and Unauthorized Devices, which of the following Capability Level 4 to 5 controls has your organization implemented? Please check all that apply. (Ref:EX05)

□ Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network. (CSC 1-3)

□ Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems. (CSC 1-5)

□ Deploy network access control (NAC) to monitor authorized systems so if attacks occur, the impact can be remediated by moving the untrusted system to a virtual local area network that has minimal access. (CSC 1-6)

□ Utilize client certificates to validate and authenticate systems prior to connecting to the private network. (CSC 1-7)

Q Please provide any additional information on your implementation of the Inventory Of Authorized and Unauthorized Devices controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX06)

Guidance

Control 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.

The following are Capability Level 4 controls:

- CSC 1-3
- CSC 1-5

The following are Capability Level 5 controls:

- CSC 1-6
- CSC 1-7

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

In relation to Inventory Of Authorized and Unauthorized Software, which of the following Capability Level 1 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX07)

□ Dangerous file types (e.g., .exe, .zip, .msi) should be closely monitored and/or blocked. (CSC 2-6)

□ Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified. (CSC 2-2)

□ Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. Furthermore, the tool should record not only the type of software installed on each system, but also its version number and patch level. (CSC 2-4)

Guidance

Control 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.

The following are Capability Level 2 controls:

- CSC 2-6

The following are Capability Level 3 controls:

- CSC 2-2
- CSC 2-4

There are no Capability Level 1 controls for this control family.

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

1.Device Inventory	**2.Software Inventory**	3.Secure Configurations

In relation to Inventory Of Authorized and Unauthorized Software, which of the following Capability Level 4 to 5 controls has your organization implemented? Please check all that apply. (Ref:EX09)

□ Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow. When protecting systems with customized software that may be seen as difficult to whitelist, use item 8 below (ref: CSC 2-8) (isolating the custom software in a virtual operating system that does not retain infections). (CSC 2-1)

□ The software inventory systems must be integrated with the hardware asset inventory so that all devices and associated software are tracked from a single location. (CSC 2-5)

□ Configure client workstations with non-persistent, virtualized operating environments that can be quickly and easily restored to a trusted snapshot on a periodic basis. (CSC 2-8)

□ Deploy software that only provides signed software ID tags. A software identification tag is an XML file that is installed alongside software and uniquely identifies the software, providing data for software inventory and asset management. (CSC 2-9)

□ Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system. A strict change-control process should also be implemented to control any changes or installation of software to any systems on the network. This includes alerting when unrecognized binaries (executable files, DLL's and other libraries, etc.) are found on a system, even inside of compressed archives. This includes checking for unrecognized or altered versions of software by comparing file hash values (attackers often utilize altered versions of known software to perpetrate attacks, and file hash comparisons will reveal the compromised software components). (CSC 2-3)

□ Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment. (CSC 2-7)

Please provide any additional information on your implementation of the Inventory Of Authorized and Unauthorized Software controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX010)

□

Guidance

Control 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.

The following are Capability Level 4 controls:

- CSC 2-1

The following are Capability Level 5 controls:

- CSC 2-5
- CSC 2-8
- CSC 2-9
- CSC 2-3
- CSC 2-7

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

2.Software Inventory	3.Secure Configurations	4.Assess/Remediation

Q In relation to Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers, which of the following Capability Level 1 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX011)

□ Implement automated patching tools and processes for both applications and for operating system software. When outdated systems can no longer be patched, update to the latest version of application software. Remove outdated, older, and unused software from the system. (CSC 3-2)

□ Limit administrative privileges to very few users who have both the knowledge necessary to administer the operating system and a business need to modify the configuration of the underlying operating system. This will help prevent installation of unauthorized software and other abuses of administrator privileges. (CSC 3-3)

□ Establish and ensure the use of standard secure configurations of your operating systems. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. Hardening typically includes: removal of unnecessary accounts (including service accounts), disabling or removal of unnecessary services, configuring non-executable stacks and heaps, applying patches, closing open and unused network ports, implementing intrusion detection systems and/or intrusion prevention systems, and use of host-based firewalls. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors. (CSC 3-1)

□ Do all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL or IPSEC. (CSC 3-7)

Guidance

Control Objective: Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

The following are Capability Level 1 controls:

- CSC 3-2
- CSC 3-3

The following are Capability Level 2 controls:

- CSC 3-1

The following are Capability Level 3 controls:

- CSC 3-7

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

In relation to Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers, which of the following Capability Level 4 to 5 controls has your organization implemented? Please check all that apply. (Ref:EX013)

□ Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization's change management processes. Images should be created for workstations, servers, and other system types used by the organization. (CSC 3-4)

□ Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis. (CSC 3-10)

□ Negotiate contracts to buy systems configured securely out of the box using standardized images, which should be devised to avoid extraneous software that would increase their attack surface and susceptibility to vulnerabilities. (CSC 3-6)

□ Utilize file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. All alterations to such files should be automatically reported security personnel. The reporting system should have the ability to account for routine and expected changes, highlighting unusual or unexpected alterations. For investigative support, the reporting system should be able to show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should also identify suspicious system alterations such as owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; as well as detecting the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes). (CSC 3-8)

□ Implement and test an automated configuration monitoring system that measures all secure configuration elements that can be measured through remote testing using features such as those included with tools compliant with Security Content Automation Protocol (SCAP), and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects, (where applicable), and new services running on a system. (CSC 3-9)

□ Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network. (CSC 3-5)

Please provide any additional information on your implementation of the Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX014)

Guidance

Control Objective: Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

The following are Capability Level 4 controls:

- CSC 3-4
- CSC 3-10

The following are Capability Level 5 controls:

- CSC 3-5
- CSC 3-6
- CSC 3-8
- CSC 3-9

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

3.Secure Configurations	**4.Assess/Remediation**	5.Malware Defenses

In relation to Continuous Vulnerability Assessment and Remediation, which of the following Capability Level 1 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX015)

□ Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped. (CSC 4-5)

□ Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project). (CSC 4-1)

□ Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested. Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses. Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user. (CSC 4-3)

□ Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk. (CSC 4-7)

Guidance

Control Objective: Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

The following are Capability Level 1 controls:

- CSC 4-5

The following are Capability Level 2 controls:

- CSC 4-1
- CSC 4-3

The following are Capability Level 3 controls:

- CSC 4-7

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

3.Secure Configurations	**4.Assess/Remediation**	5.Malware Defenses

Q In relation to Continuous Vulnerability Assessment and Remediation, which of the following Capability Level 4 to 5 controls has your organization implemented? Please check all that apply. (Ref:EX017)

□ Carefully monitor logs associated with any scanning activity and associated administrator accounts to ensure that all scanning activity and associated access via the privileged account is limited to the timeframes of legitimate scans. (CSC 4-6)

□ Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level. (CSC 4-10)

□ Correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools themselves is logged. Second, personnel should be able to correlate attack detection events with earlier vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable. (CSC 4-2)

□ Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis. Alternatively, ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities. (CSC 4-4)

□ Measure the delay in patching new vulnerabilities and ensure that the delay is equal to or less than the benchmarks set forth by the organization. Alternative countermeasures should be considered if patches are not available. (CSC 4-8)

□ Evaluate critical patches in a test environment before pushing them into production on enterprise systems. If such patches break critical business applications on test machines, the organization must devise other mitigating controls that block exploitation on systems where the patch cannot be deployed because of its impact on business functionality. (CSC 4-9)

Q Please provide any additional information on your implementation of the Continuous Vulnerability Assessment and Remediation controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX018)

Guidance

Control Objective: Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

The following are Capability Level 4 controls:

- CSC 4-6
- CSC 4-10

The following are Capability Level 5 controls:

- CSC 4-2
- CSC 4-4
- CSC 4-8
- CSC 4-9

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

4.Assess/Remediation	**5.Malware Defenses**	6.In-house SW Security

Q In relation to Malware Defenses, which of the following Capability Level 1 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX019)

- □ Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers. (CSC 5-1)
- □ Employ anti-malware software that offers a remote, cloud-based centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update. (CSC 5-2)
- □ Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares. (CSC 5-3)
- □ Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted. (CSC 5-4)
- □ Scan and block all e-mail attachments entering the organization's e-mail gateway if they contain malicious code or file types that are unnecessary for the organization's business. This scanning should be done before the e-mail is placed in the user's inbox. This includes e-mail content filtering and web content filtering. (CSC 5-5)
- □ Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables. (CSC 5-6)

Guidance

Control 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.

The following are Capability Level 1 controls:

- CSC 5-1
- CSC 5-2
- CSC 5-3
- CSC 5-4

The following are Capability Level 2 controls:

- CSC 5-5

The following are Capability Level 3 controls:

- CSC 5-6

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

© 2015 CIS

4.Assess/Remediation	**5.Malware Defenses**	6.In-house SW Security

Q In relation to Malware Defenses, which of the following Capability Level 4 to 5 controls has your organization implemented? Please check all that apply. (Ref:EX021)

- □ Ensure that automated monitoring tools use behavior-based anomaly detection to complement traditional signature-based detection. (CSC 5-8)
- □ Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains. (CSC 5-11)
- □ Limit use of external devices to those that have a business need. Monitor for use and attempted use of external devices. (CSC 5-7)
- □ Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint. (CSC 5-9)
- □ Implement an incident response process that allows the IT support organization to supply the security team with samples of malware running on corporate systems that do not appear to be recognized by the enterprise's anti-malware software. Samples should be provided to the security vendor for "out-of-band" signature creation and later deployed to the enterprise by system administrators. (CSC 5-10)

Q Please provide any additional information on your implementation of the Malware Defenses controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX022)

Guidance

Control 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.

The following are Capability Level 4 controls:

- CSC 5-8
- CSC 5-11
- CSC 5-7

The following are Capability Level 5 controls:

- CSC 5-9
- CSC 5-10

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

5.Malware Defenses	6.In-house SW Security	6a.Purchased SW Security

Does your organization develop any software that your organization uses in house? (Ref:EX016)

○ Yes

○ No

Guidance

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

5.Malware Defenses	**6.In-house SW Security**	6a.Purchased SW Security

Q In relation to Application Software Security - Inhouse Developed Software, which of the following Capability Level 1 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX023)

- □ For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. (CSC 6-3)
- □ Test in-house-developed web and other application software for coding errors and potential vulnerabilities prior to deployment using automated static code analysis software, as well as manual testing and inspection. In particular, input validation and output encoding routines of application software should be reviewed and tested. (CSC 6-7)
- □ For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested. (CSC 6-9)
- □ Ensure that all software development personnel receive training in writing secure code for their specific development environment. (CSC 6-10)
- □ For in-house developed applications, ensure that development artifacts (sample data and scripts; unused libraries, components, debug code; or tools) are not included in the deployed software, or accessible in the production environment. (CSC 6-11)
- □ Test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, whenever updates are made to the application, and on a regular recurring basis. Include tests for application behavior under denial-of-service or resource exhaustion attacks. (CSC 6-4)
- □ Do not display system error messages to end-users (output sanitization). (CSC 6-5)
- □ Maintain separate environments for production and nonproduction systems. Developers should not typically have unmonitored access to production environments. (CSC 6-6)
- □ Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, SQL injection, command injection, and directory traversal attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed. (CSC 6-2)

Q Please provide any additional information on your implementation of the Application Software Security - Inhouse Developed Software controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX024)

Guidance

Control Objective: Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

The following are Capability Level 1 controls:

- CSC 6-3
- CSC 6-7
- CSC 6-9
- CSC 6-10
- CSC 6-11

The following are Capability Level 2 controls:

- CSC 6-4
- CSC 6-5
- CSC 6-6

The following are Capability Level 3 controls:

- CSC 6-2

There are no Capability Levels 4 & 5 controls for this control family.

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

6.In-house SW Security	6a.Purchased SW Security	7.Wireless Access

Q In relation to Application Software Security - Purchased Software, which of the following Capability Level 1 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX025)

□ For all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations. (CSC 6-1)

□ For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested. (CSC 6-9)

□ Test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, whenever updates are made to the application, and on a regular recurring basis. Include tests for application behavior under denial-of-service or resource exhaustion attacks. (CSC 6-4)

Guidance

Control Objective: Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

The following are Capability Level 1 controls:

- CSC 6-1

The following are Capability Level 2 controls:

- CSC 6-9

The following are Capability Level 3 controls:

- CSC 6-4

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

6.In-house SW Security	6a.Purchased SW Security	7.Wireless Access

Q In relation to Application Software Security - Purchased Software, which of the following Capability Level 4 to 5 controls has your organization implemented? Please check all that apply. (Ref:EX027)

□ Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, SQL injection, command injection, and directory traversal attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed. (CSC 6-2)

□ For acquired application software, examine the product security process of the vendor (history of vulnerabilities, customer notification, patching/remediation) as part of the overall enterprise risk management process. (CSC 6-8)

Q Please provide any additional information on your implementation of the Application Software Security - Purchased Software controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX028)

Guidance

Control Objective: Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

The following are Capability Level 4 controls:

- CSC 6-2

The following are Capability Level 5 controls:

- CSC 6-8

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

6a.Purchased SW Security	7.Wireless Access	8.Data Recovery

Q Does your organization support Wireless Access Controls? (Ref:EX240)

○ Yes
○ No

Guidance

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

6a.Purchased SW Security	**7.Wireless Access**	8.Data Recovery

Q In relation to Wireless Access Control, which of the following Capability Level 1 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX029)

□ Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection. (CSC 7-6)

□ Disable peer-to-peer wireless network capabilities on wireless clients, unless such functionality meets a documented business need. (CSC 7-8)

□ Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need. (CSC 7-9)

□ Configure network vulnerability scanning tools to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points should be deactivated. (CSC 7-2)

Guidance

Control Objective: The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

The following are Capability Level 1 controls:

- CSC 7-6

The following are Capability Level 2 controls:

- CSC 7-8
- CSC 7-9

The following are Capability Level 3 controls:

- CSC 7-2

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

6a.Purchased SW Security	7.Wireless Access	8.Data Recovery

Q In relation to Wireless Access Control, which of the following Capability Level 4 to 5 controls has your organization implemented? Please check all that apply. (Ref:EX031)

- □ Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which provide credential protection and mutual authentication. (CSC 7-7)
- □ Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks. (CSC 7-4)
- □ For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible firmware interface), with password protections to lower the possibility that the user will override such configurations. (CSC 7-5)
- □ Ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Organizations should deny access to those wireless devices that do not have such a configuration and profile. (CSC 7-1)
- □ Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises. In addition to WIDS, all wireless traffic should be monitored by WIDS as traffic passes into the wired network. (CSC 7-3)
- □ Create separate virtual local area networks (VLANs) for BYOD systems or other untrusted devices. Internet access from this VLAN should go through at least the same border as corporate traffic. Enterprise access from this VLAN should be treated as untrusted and filtered and audited accordingly. (CSC 7-10)

Q Please provide any additional information on your implementation of the Wireless Access Control controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX032)

□

Guidance

Control Objective: The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

The following are Capability Level 4 controls:

- CSC 7-7

The following are Capability Level 5 controls:

- CSC 7-4
- CSC 7-5
- CSC 7-1
- CSC 7-3
- CSC 7-10

Tools for Automating Critical Security Controls

CSC v5.1

7.Wireless Access	8.Data Recovery	9.Skills/Tranining

Q In relation to Data Recovery Capability, which of the following Capability Level 2 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX033)

□ Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services. (CSC 8-3)

□ Ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information. To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or use the same backup software. There should be multiple backups over time, so that in the event of malware infection, restoration can be from a version that is believed to predate the original infection. All backup policies should be compliant with any regulatory or official requirements. (CSC 8-1)

Guidance

Control Objective: The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

The following are Capability Level 2 controls:

- CSC 8-3

The following are Capability Level 3 controls:

- CSC 8-1

There are no Capability Level 1 controls for this control family.

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

7.Wireless Access	8.Data Recovery	9.Skills/Tranining

Q In relation to Data Recovery Capability, which of the following Capability Level 4 to 5 controls has your organization implemented? Please check all that apply. (Ref:EX035)

□ Test data on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working. (CSC 8-2)

□ Ensure that key systems have at least one backup destination that is not continuously addressable through operating system calls. This will mitigate the risk of attacks like CryptoLocker which seek to encrypt or damage data on all addressable data shares, including backup destinations. (CSC 8-4)

Q Please provide any additional information on your implementation of the Data Recovery Capability controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX036)

Guidance

Control Objective: The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

The following are Capability Level 4 controls:

- CSC 8-2

The following are Capability Level 5 controls:

- CSC 8-4

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

8.Data Recovery	9.Skills/Tranining	10.Network Devices

Q In relation to Security Skills Assessment & Appropriate Training, which of the following Capability Level 2 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX037)

□ Perform gap analysis to see which skills employees need and which behaviors employees are not adhering to, using this information to build a baseline training and awareness roadmap for all employees. (CSC 9-1)

□ Deliver training to fill the skills gap. If possible, use more senior staff to deliver the training. A second option is to have outside teachers provide training onsite so the examples used will be directly relevant. If you have small numbers of people to train, use training conferences or online training to fill the gaps. (CSC 9-2)

□ Implement an online security awareness program that (1) focuses only on the methods commonly used in intrusions that can be blocked through individual action, (2) is delivered in short online modules convenient for employees (3) is updated frequently (at least annually) to represent the latest attack techniques, (4) is mandated for completion by all employees at least annually, and (5) is reliably monitored for employee completion. (CSC 9-3)

□ Validate and improve awareness levels through periodic tests to see whether employees will click on a link from suspicious e-mail or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller; targeted training should be provided to those who fall victim to the exercise. (CSC 9-4)

Guidance

Control 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.

The following are Capability Level 2 controls:

- CSC 9-1
- CSC 9-2
- CSC 9-3

The following are Capability Level 3 controls:

- CSC 9-4

There are no Capability Levels 1 & 5 controls for this control family.

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

8.Data Recovery	**9.Skills/Tranining**	10.Network Devices

In relation to Security Skills Assessment & Appropriate Training, which of the following Capability Level 4 controls has your organization implemented? Please check all that apply. (Ref:EX039)

□ Use security skills assessments for each of the mission-critical roles to identify skills gaps. Use hands-on, real-world examples to measure mastery. If you do not have such assessments, use one of the available online competitions that simulate real-world scenarios for each of the identified jobs in order to measure skills mastery. (CSC 9-5)

Please provide any additional information on your implementation of the Security Skills Assessment & Appropriate Training controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX040)

Guidance

Control 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.

The following are Capability Level 4 controls:

- CSC 9-5

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

In relation to Secure Configurations for Network Devices such as Firewalls, Routers & Switches, which of the following Capability Level 1 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX041)

□ Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization. The security configuration of such devices should be documented, reviewed, and approved by an organization change control board. Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system. (CSC 10-1)

□ All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, should be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need. (CSC 10-2)

□ Install the latest stable version of any security-related updates. (CSC 10-5)

□ Use automated tools to verify standard device configurations and detect changes. All alterations to such files should be automatically reported to security personnel. (CSC 10-3)

□ Manage network devices using two-factor authentication and encrypted sessions. (CSC 10-4)

Guidance

Control 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.

The following are Capability Level 1 controls:

- CSC 10-1
- CSC 10-2
- CSC 10-5

The following are Capability Level 3 controls:

- CSC 10-3
- CSC 10-4

There are no Capability Levels 2 & 4 controls for this control family.

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

9.Skills/Tranining	10.Network Devices	11.Network Controls

Q In relation to Secure Configurations for Network Devices such as Firewalls, Routers & Switches, which of the following Capability Level 5 controls has your organization implemented? Please check all that apply. (Ref:EX043)

□ Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices. (CSC 10-6)

Q Please provide any additional information on your implementation of the Secure Configurations for Network Devices such as Firewalls, Routers & Switches controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX044)

Guidance

Control 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.

The following are Capability Level 5 controls:

- CSC 10-6

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

10.Network Devices	**11.Network Controls**	12.Administrative Privileges

Q In relation to Limitation and Control of Network Ports, Protocols & Services, which of the following Capability Level 1 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX045)

□ Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. (CSC 11-2)

□ Keep all services up to date and uninstall and remove any unnecessary components from the system. (CSC 11-4)

□ Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers. (CSC 11-6)

□ Verify any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address. (CSC 11-5)

□ Ensure that only ports, protocols, and services with validated business needs are running on each system. (CSC 11-1)

□ Perform automated port scans on a regular basis against all key servers and compared to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed. (CSC 11-3)

Guidance

Control 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.

The following are Capability Level 1 controls:

- CSC 11-2

The following are Capability Level 2 controls:

- CSC 11-4
- CSC 11-6
- CSC 11-5
- CSC 11-1

The following are Capability Level 3 controls:

- CSC 11-3

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

10.Network Devices	**11.Network Controls**	12.Administrative Privileges

Q In relation to Limitation and Control of Network Ports, Protocols & Services, which of the following Capability Level 4 controls has your organization implemented? Please check all that apply. (Ref:EX047)

□ Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic should be blocked and an alert generated. (CSC 11-7)

Q Please provide any additional information on your implementation of the Limitation and Control of Network Ports, Protocols & Services controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX048)

Guidance

Control 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.

The following are Capability Level 4 controls:

- CSC 11-7

There are no Capability Level 5 controls for this control family.

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

11.Network Controls	**12.Administrative Privileges**	13.Boundary Defense

In relation to Controlled Use of Administrative Privileges, which of the following Capability Level 1 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX049)

□ Configure all administrative passwords to be complex and contain letters, numbers, and special characters intermixed, and with no dictionary words present in the password. Pass phrases containing multiple dictionary words, along with special characters, are acceptable if they are of a reasonable length. (CSC 12-3)

□ Utilize access control lists to ensure that administrative accounts are used only for system administration activities, and not for reading e-mail, composing documents, or surfing the Internet. Web browsers and e-mail clients especially must be configured to never run as administrator. (CSC 12-7)

□ Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior. (CSC 12-1)

□ Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts. (CSC 12-4)

□ Ensure that all service accounts have long and difficult-to-guess passwords that are changed on a periodic basis, as is done for traditional user and administrative passwords. (CSC 12-5)

□ Configure operating systems so that passwords cannot be re-used within a timeframe of six months. (CSC 12-9)

□ Through policy and user awareness, require that administrators establish unique, different passwords for their administrative and non-administrative accounts. Each person requiring administrative access should be given his/her own separate account. Users should only use the Windows "administrator" or UNIX "root" accounts in emergency situations. Domain administration accounts should be used when required for system administration instead of local administrative accounts. (CSC 12-8)

□ Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system. (CSC 12-10)

□ Configure systems to issue a log entry and alert when unsuccessful login to an administrative account is attempted. (CSC 12-11)

□ Passwords should be hashed or encrypted in storage. Passwords that are hashed should be salted and follow guidance provided in NIST SP 800-132 or similar guidance. Files containing these encrypted or hashed passwords required for systems to authenticate users should be readable only with super-user privileges. (CSC 12-6)

Guidance

Control Objective: The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

The following are Capability Level 1 controls:

- CSC 12-3
- CSC 12-7

The following are Capability Level 2 controls:

- CSC 12-1
- CSC 12-4
- CSC 12-5
- CSC 12-9
- CSC12-8

The following are Capability Level 3 controls:

- CSC 12-10
- CSC 12-11
- CSC 12-6

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

11.Network Controls	**12.Administrative Privileges**	13.Boundary Defense

In relation to Controlled Use of Administrative Privileges, which of the following Capability Level 4 to 5 controls has your organization implemented? Please check all that apply. (Ref:EX051)

□ Use multifactor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics. (CSC 12-12)

□ When using certificates to enable multi-factor certificate-based authentication, ensure that the private keys are protected using strong passwords or are stored in trusted, secure hardware tokens. (CSC 12-13)

□ Block access to a machine (either remotely or locally) for administrator-level accounts. Instead, administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems. Users would use their own administrative accounts and enter a password each time that is different than their user account. (CSC 12-14)

□ Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive. (CSC 12-2)

Please provide any additional information on your implementation of the Controlled Use of Administrative Privileges controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX052)

Guidance

Control Objective: The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

The following are Capability Level 4 controls:

- CSC 12-12
- CSC 12-13
- CSC 12-14

The following are Capability Level 5 controls:

- CSC 12-2

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

12.Administrative Privileges	13.Boundary Defense	14.Audit Logs

Q In relation to Boundary Defense, which of the following Capability Level 1 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX053)

□ Deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (whitelists). Tests can be periodically carried out by sending packets from bogon source IP addresses (non-routable or otherwise unused IP addresses) into the network to verify that they are not transmitted through network perimeters. Lists of bogon addresses are publicly available on the Internet from various sources, and indicate a series of IP addresses that should not be used for legitimate traffic traversing the Internet. (CSC 13-1)

□ Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication. (CSC 13-7)

□ To lower the chance of spoofed e-mail messages, implement the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers. (CSC 13-3)

□ Design and implement network perimeters so that all outgoing web, file transfer protocol (FTP), and secure shell traffic to the Internet must pass through at least one proxy on a DMZ network. The proxy should support logging individual TCP sessions; blocking specific URLs, domain names, and IP addresses to implement a black list; and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites. Organizations should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter. Proxies can also be used to encrypt all traffic leaving an organization. (CSC 13-6)

□ To minimize the impact of an attacker pivoting between compromised systems, only allow DMZ systems to communicate with private network systems via application proxies or application-aware firewalls over approved channels. (CSC 13-11)

□ All enterprise devices remotely logging into the internal network should be managed by the enterprise, with remote control of their configuration, installed software, and patch levels. For third-party devices (e.g., subcontractors/vendors), publish minimum security standards for access to the enterprise network and perform a security scan before allowing access. (CSC 13-8)

Guidance

Control Objective: Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

The following are Capability Level 1 controls:

- CSC 13-1

The following are Capability Level 2 controls:

- CSC 13-7
- CSC 13-3
- CSC 13-6

The following are Capability Level 3 controls:

- CSC 13-11
- CSC 13-8

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

12.Administrative Privileges	13.Boundary Defense	14.Audit Logs

In relation to Boundary Defense, which of the following Capability Level 4 to 5 controls has your organization implemented? Please check all that apply. (Ref:EX055)

□ Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms. (CSC 13-9)

□ Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic. (CSC 13-4)

□ On DMZ networks, configure monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network. (CSC 13-2)

□ Network-based IPS devices should be deployed to complement IDS by blocking known bad signature or behavior of attacks. As attacks become automated, methods such as IDS typically delay the amount of time it takes for someone to react to an attack. A properly configured network-based IPS can provide automation to block bad traffic. When evaluating network-based IPS products, include those using techniques other than signature-based detection (such as virtual machine or sandbox-based approaches) for consideration. (CSC 13-5)

□ To limit access by an insider, untrusted subcontractor/vendor, or malware spreading on an internal network, devise internal network segmentation schemes to limit traffic to only those services needed for business use across the organization's internal network. (CSC 13-10)

□ To help identify covert channels exfiltrating data through a firewall, configure the built-in firewall session tracking mechanisms included in many commercial firewalls to identify TCP sessions that last an unusually long time for the given organization and firewall device, alerting personnel about the source and destination addresses associated with these long sessions. (CSC 13-12)

□ Deploy NetFlow collection and analysis to DMZ network flows to detect anomalous activity. (CSC 13-13)

Please provide any additional information on your implementation of the Boundary Defense controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX056)

Guidance

Control Objective: Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

The following are Capability Level 4 controls:

- CSC 13-9
- CSC 13-4
- CSC 13-2

The following are Capability Level 5 controls:

- CSC 13-5
- CSC 13-10
- CSC 13-12
- CSC 13-13

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

© 2015 CIS

13.Boundary Defense	14.Audit Logs	15.Controlled Access

In relation to Maintenance, Monitoring & Analysis of Audit Logs, which of the following Capability Level 2 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX057)

□ Include at least two synchronized time sources (i.e., Network Time Protocol - NTP) from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent, and are set to UTC (Coordinate Universal Time). (CSC 14-1)

□ Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis. (CSC 14-3)

□ Develop a log retention policy to make sure that the logs are kept for a sufficient period of time. Organizations are often compromised for several months without detection. The logs must be kept for a longer period of time than it takes an organization to detect an attack so they can accurately determine what occurred. (CSC 14-4)

□ Have security personnel and/or system administrators run biweekly reports that identify anomalies in logs. They should then actively review the anomalies, documenting their findings. (CSC 14-5)

□ Ensure that the log collection system does not lose events during peak activity, and that the system detects and alerts if event loss occurs (such as when volume exceeds the capacity of a log collection system). This includes ensuring that the log collection system can accommodate intermittent or restricted-bandwidth connectivity through the use of handshaking / flow control. (CSC 14-10)

□ Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format. (CSC 14-2)

Guidance

Control Objective: Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

The following are Capability Level 2 controls:

- CSC 14-1
- CSC 14-3
- CSC 14-4
- CSC 14-5

The following are Capability Level 3 controls:

- CSC 14-10
- CSC 14-2

There are no Capability Level 1 controls for this control family.

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

13.Boundary Defense	14.Audit Logs	15.Controlled Access

Q In relation to Maintenance, Monitoring & Analysis of Audit Logs, which of the following Capability Level 4 to 5 controls has your organization implemented? Please check all that apply. (Ref:EX059)

□ Configure network boundary devices, including firewalls, network-based IPS, and inbound and outbound proxies, to verbosely log all traffic (both allowed and blocked) arriving at the device. (CSC 14-6)

□ For all servers, ensure that logs are written to write-only devices or to dedicated logging servers running on separate machines from the hosts generating the event logs, lowering the chance that an attacker can manipulate logs stored locally on compromised machines. (CSC 14-7)

□ Monitor for service creation events and enable process tracking logs. On Windows systems, many attackers use PsExec functionality to spread from system to system. Creation of a service is an unusual event and should be monitored closely. Process tracking is valuable for incident handling. (CSC 14-9)

□ Deploy a SIEM (Security Incident and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts. (CSC 14-8)

Q Please provide any additional information on your implementation of the Maintenance, Monitoring & Analysis of Audit Logs controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX060)

Guidance

Control Objective: Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

The following are Capability Level 4 controls:

- CSC 14-6
- CSC 14-7
- CSC 14-9

The following are Capability Level 5 controls:

- CSC 14-8

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

14.Audit Logs	**15.Controlled Access**	16.Account Monitoring and Control

Q In relation to Controlled Access Based on the Need to Know, which of the following Capability Level 5 controls has your organization implemented? Please check all that apply. (Ref:EX061)

□ Locate any sensitive information on separated VLANS with firewall filtering. All communication of sensitive information over less-trusted networks should be encrypted. (CSC 15-1)

□ Segment the network based on the trust levels of the information stored on the servers. Whenever information flows over a network with a lower trust level, the information should be encrypted. (CSC 15-3)

□ Use host-based data loss prevention (DLP) to enforce ACLs even when data is copied off a server. In most organizations, access to the data is controlled by ACLs that are implemented on the server. Once the data have been copied to a desktop system, the ACLs are no longer enforced and the users can send the data to whomever they want. (CSC 15-4)

□ Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data. (CSC 15-2)

Q Please provide any additional information on your implementation of the Controlled Access Based on the Need to Know controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX062)

□

Guidance

Control 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.

The following are Capability Level 5 controls:

- CSC 15-1
- CSC 15-3
- CSC 15-4
- CSC 15-2

There are no Capability Levels 1, 2, 3 & 4 controls for this control family.

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

15.Controlled Access	16.Account Monitoring and Control	17.Data Protection

In relation to Account Monitoring & Control, which of the following Capability Level 1 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX063)

□ Review all system accounts and disable any account that cannot be associated with a business process and owner. (CSC 16-1)

□ Ensure that all accounts have an expiration date associated with the account. (CSC 16-2)

□ Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails. (CSC 16-4)

□ Monitor account usage to determine dormant accounts, notifying the user or user's manager. Disable such accounts if not needed, or document and monitor exceptions (e.g., vendor maintenance accounts needed for system recovery or continuity operations). (CSC 16-7)

□ Require that all non-administrator accounts have strong passwords that contain letters, numbers, and special characters, be changed at least every 90 days, have a minimal age of one day, and not be allowed to use the previous 15 passwords as a new password. These values can be adjusted based on the specific business needs of the organization. (CSC 16-8)

□ Require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators should then disable accounts that are not assigned to active employees or contractors. (CSC 16-10)

□ Configure screen locks on systems to limit access to unattended workstations. (CSC 16-6)

□ Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity. (CSC 16-5)

□ Monitor attempts to access deactivated accounts through audit logging. (CSC 16-11)

□ Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time. (CSC 16-9)

□ For authenticated access to web services within an enterprise, ensure that account usernames and passwords are passed over an encrypted channel and associated password hash files are stored securely if a centralized service is not employed. (CSC 16-15)

□ Configure all systems to use encrypted channels for the transmission of passwords over a network. (CSC 16-16)

□ Verify that all password files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system. (CSC 16-17)

Guidance

Control 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.

The following are Capability Level 1 controls:

- CSC 16-1
- CSC 16-2
- CSC 16-4
- CSC 16-7
- CSC 16-8
- CSC 16-10

The following are Capability Level 2 controls:

- CSC 16-6
- CSC 16-5
- CSC 16-11
- CSC 16-9

The following are Capability Level 3 controls:

- CSC 16-15
- CSC 16-16
- CSC 16-17

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

15.Controlled Access	**16.Account Monitoring and Control**	17.Data Protection

In relation to Account Monitoring & Control, which of the following Capability Level 4 to 5 controls has your organization implemented? Please check all that apply. (Ref:EX065)

□ Ensure that systems automatically create a report that includes a list of locked-out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire. This list should be sent to the associated system administrator in a secure fashion. (CSC 16-3)

□ Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well. (CSC 16-12)

□ Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works. (CSC 16-13)

□ Require multi-factor authentication for accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using Smart cards with certificates, One Time Password (OTP) tokens, or biometrics. (CSC 16-14)

Please provide any additional information on your implementation of the Account Monitoring & Control controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX066)

Guidance

Control 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.

The following are Capability Level 4 controls:

- CSC 16-3

The following are Capability Level 5 controls:

- CSC 16-12
- CSC 16-13
- CSC 16-14

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

16.Account Monitoring and Control	**17.Data Protection**	18.Incident Management

Q In relation to Data Protection, which of the following Capability Level 2 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX067)

- □ Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data. (CSC 17-1)
- □ Verify that cryptographic devices and software are configured to use publicly-vetted algorithms. (CSC 17-2)
- □ Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls. (CSC 17-3)
- □ Review cloud provider security practices for data protection. (CSC 17-4)
- □ Block access to known file transfer and e-mail exfiltration websites. (CSC 17-13)

Guidance

Control Objective: The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

The following are Capability Level 2 controls:

- CSC 17-1
- CSC 17-2
- CSC 17-3
- CSC 17-4

The following are Capability Level 3 controls:

- CSC 17-13

There are no Capability Level 1 controls for this control family.

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

16.Account Monitoring and Control	17.Data Protection	18.Incident Management

Q In relation to Data Protection, which of the following Capability Level 4 to 5 controls has your organization implemented? Please check all that apply. (Ref:EX069)

□ Move data between networks using secure, authenticated, and encrypted mechanisms. (CSC 17-7)

□ Only allow approved Certificate Authorities (CAs) to issue certificates within the enterprise; Review and verify each CAs Certificate Practices Statement (CPS) and Certificate Policy (CP). (CSC 17-10)

□ Define roles and responsibilities related to management of encryption keys within the enterprise; define processes for lifecycle. (CSC 17-14)

□ Deploy an automated tool on network perimeters that monitors for certain sensitive information (i.e., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel. (CSC 17-5)

□ Conduct periodic scans of server machines using automated tools to determine whether sensitive data (i.e., personally identifiable information, health, credit card, and classified information) is present on the system in clear text. These tools, which search for patterns that indicate the presence of sensitive information, can help identify if a business or technical process is leaving behind or otherwise leaking sensitive information. (CSC 17-6)

□ If there is no business need for supporting such devices, configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained. (CSC 17-8)

□ Use network-based DLP solutions to monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action taken to address them. (CSC 17-9)

□ Perform an annual review of algorithms and key lengths in use for protection of sensitive data. (CSC 17-11)

□ Monitor all traffic leaving the organization and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore it is essential that organizations be able to detect rogue connections, terminate the connection, and remediate the infected system. (CSC 17-12)

□ Where applicable, implement Hardware Security Modules (HSMs) for protection of private keys (e.g., for sub CAs) or Key Encryption Keys. (CSC 17-15)

Q Please provide any additional information on your implementation of the Data Protection controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX070)

Guidance

Control Objective: The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

The following are Capability Level 4 controls:

- CSC 17-7
- CSC 17-10
- CSC 17-14

The following are Capability Level 5 controls:

- CSC 17-5
- CSC 17-6
- CSC 17-8
- CSC 17-9
- CSC 17-11
- CSC 17-12
- CSC 17-15

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

17.Data Protection	18.Incident Management	19.Secure Network Engineering

In relation to Incident Response & Management, which of the following Capability Level 2 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX071)

- □ Ensure that there are written incident response procedures that include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling. (CSC 18-1)
- □ Assign job titles and duties for handling computer and network incidents to specific individuals. (CSC 18-2)
- □ Define management personnel who will support the incident handling process by acting in key decision-making roles. (CSC 18-3)
- □ Publish information for all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities. (CSC 18-6)

Guidance

Control 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.

The following are Capability Level 2 controls:

- CSC 18-1
- CSC 18-2
- CSC 18-3

The following are Capability Level 3 controls:

- CSC 18-6

There are no Capability Level 1 controls for this control family.

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

17.Data Protection	**18.Incident Management**	19.Secure Network Engineering

In relation to Incident Response & Management, which of the following Capability Level 4 to 5 controls has your organization implemented? Please check all that apply. (Ref:EX073)

☐ Devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. This reporting should also include notifying the appropriate Community Emergency Response Team in accordance with all legal or regulatory requirements for involving that organization in computer incidents. (CSC 18-4)

☐ Assemble and maintain information on third-party contact information to be used to report a security incident (i.e., maintain an e-mail address of security@organization.com or have a web page organization.com/security). (CSC 18-5)

☐ Conduct periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team. (CSC 18-7)

Please provide any additional information on your implementation of the Incident Response & Management controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX074)

Guidance

Control 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.

The following are Capability Level 4 controls:

- CSC 18-4

The following are Capability Level 5 controls:

- CSC 18-5
- CSC 18-7

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

18.Incident Management	**19.Secure Network Engineering**	20.Penetration Tests

Q In relation to Secure Network Engineering, which of the following Capability Level 2 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX075)

□ Deploy domain name systems (DNS) in a hierarchical, structured fashion, with all internal network client machines configured to send requests to intranet DNS servers, not to DNS servers located on the Internet. These internal DNS servers should be configured to forward requests they cannot resolve to DNS servers located on a protected DMZ. These DMZ servers, in turn, should be the only DNS servers allowed to send requests to the Internet. (CSC 19-3)

□ Design the network using a minimum of a three-tier architecture (DMZ, middleware, and private network). Any system accessible from the Internet should be on the DMZ, but DMZ systems should never contain sensitive data. Any system with sensitive data should reside on the private network and never be directly accessible from the Internet. DMZ systems should communicate with private network systems through an application proxy residing on the middleware tier. (CSC 19-1)

Guidance

Control Objective: Make security an inherent attribute of the enterprise by specifying, designing, and building-in features that allow high confidence systems operations while denying or minimizing opportunities for attackers.

The following are Capability Level 2 controls:

- CSC 19-3

The following are Capability Level 3 controls:

- CSC 19-1

There are no Capability Levels 1 & 4 controls for this control family.

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

18.Incident Management	**19.Secure Network Engineering**	20.Penetration Tests

Q In relation to Secure Network Engineering, which of the following Capability Level 5 controls has your organization implemented? Please check all that apply. (Ref:EX077)

□ Segment the enterprise network into multiple, separate trust zones to provide more granular control of system access and additional intranet boundary defenses. (CSC 19-4)

□ To support rapid response and shunning of detected attacks, engineer the network architecture and its corresponding systems for rapid deployment of new access control lists, rules, signatures, blocks, blackholes, and other defensive measures. (CSC 19-2)

Q Please provide any additional information on your implementation of the Secure Network Engineering controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX078)

Guidance

Control Objective: Make security an inherent attribute of the enterprise by specifying, designing, and building-in features that allow high confidence systems operations while denying or minimizing opportunities for attackers.

The following are Capability Level 5 controls:

- CSC 19-4
- CSC 19-2

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

19.Secure Network Engineering	**20.Penetration Tests**	21.Governance

Q In relation to Penetration Tests & Red Team Exercises, which of the following Capability Level 2 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX079)

□ Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks. (CSC 20-1)

□ Plan clear goals of the penetration test itself with blended attacks in mind, identifying the goal machine or target asset. Many APT-style attacks deploy multiple vectors--often social engineering combined with web or network exploitation. Red Team manual or automated testing that captures pivoted and multi-vector attacks offers a more realistic assessment of security posture and risk to critical assets. (CSC 20-5)

Guidance

Control Objective: Test the overall strength of an organization’s defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

The following are Capability Level 2 controls:

- CSC 20-1

The following are Capability Level 3 controls:

- CSC 20-5

There are no Capability Level 1 controls for this control family.

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

19.Secure Network Engineering	20.Penetration Tests	21.Governance

In relation to Penetration Tests & Red Team Exercises, which of the following Capability Level 4 to 5 controls has your organization implemented? Please check all that apply. (Ref:EX081)

- □ Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation. (CSC 20-4)
- □ Any user or system accounts used to perform penetration testing, should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over. (CSC 20-2)
- □ Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts. (CSC 20-6)
- □ Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively. (CSC 20-3)
- □ Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time. (CSC 20-7)
- □ Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems. (CSC 20-8)

Please provide any additional information on your implementation of the Penetration Tests & Red Team Exercises controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX082)

Guidance

Control Objective: Test the overall strength of an organization’s defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

The following are Capability Level 4 controls:

- CSC 20-4
- CSC 20-2
- CSC 20-6

The following are Capability Level 5 controls:

- CSC 20-3
- CSC 20-7
- CSC 20-8

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

20.Penetration Tests	21.Governance	22.Mobile Device

Q In relation to Organization/Governance, which of the following Capability Level 1 to 3 controls has your organization implemented? Please check all that apply. (Ref:EX083)

□ Company has a person with responsibilities in Cybersecurity Risk Management (CSC 21-1)

□ Company does active cyber risk management as part of your overall risk management (CSC 21-2)

□ Company has a cybersecurity policy patterned after (NIST 800-53, ISO 17799, or another industry standard) (CSC 21-3)

□ When your company must share sensitive information with their suppliers or 3rd parties, your company requires those suppliers to follow cybersecurity policies, and procedures based on industry standards (e.g. ISO 27000, NIST 800-53)? (CSC 21-4)

Guidance

The following are Capability Level 1 controls:

- CSC 21-1

The following are Capability Level 2 controls:

- CSC 21-2
- CSC 21-3

The following are Capability Level 3 controls:

- CSC 21-4

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

20.Penetration Tests	**21.Governance**	22.Mobile Device

Q In relation to Organization/Governance, which of the following Capability Level 4 to 5 controls has your organization implemented? Please check all that apply. (Ref:EX085)

□ When your company must share sensitive information with or provide access to their suppliers or 3rd parties, verify that they meet any data handling requirements (CSC 21-5)

□ Company performs or engages a 3rd party to perform an objective cybersecurity audit of the company's controls (CSC 21-6)

Q Please provide any additional information on your implementation of the Organization/Governance controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX086)

Guidance

The following are Capability Level 4 controls:

- CSC 21-5

The following are Capability Level 5 controls:

- CSC 21-6

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

21.Governance	**22.Mobile Device**	23.Feedback

Q In relation to Mobile Device, which of the following Capability Level 2 controls has your organization implemented? Please check all that apply. (Ref:EX087)

□ Do all mobile devices (e.g. smartphones, tablets), to include Bring Your Own Device (BYOD) have access control to the device? (CSC 22-1)

□ Do all mobile devices (e.g. smartphones, tablets), to include Bring Your Own Device (BYOD) at a minimum have configuration management to enforce policies provided by a centrally managed infrastructure? (CSC 22-2)

□ Do all mobile devices (e.g. smartphones, tablets), to include Bring Your Own Device (BYOD) at a minimum have the ability to remotely wipe the device? (CSC 22-3)

Q Please provide any additional information on your implementation of the Mobile Device controls in the text box below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (Ref:EX088)

Guidance

The following are Capability Level 2 controls:

- CSC 22-1
- CSC 22-2
- CSC 22-3

There are no Capability Levels 1, 3, 4 & 5 controls for this control family.

Tools for Automating Critical Security Controls

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim

Cyber Security/Cyber Security Questionnaire Questions:
Cybersecurity Questionnaire website:
www.myexostar.com/pim/cq

Critical Controls FAQ - provides further information on the controls and tools to help implement them.

Process FAQ: Cyber Security Questionnaire - provides context of why the questionnaire was put together and how it will be used.

24.Submission

Q Thank you for your response. (Ref:EX090)

First Name :

Last Name :

Job Title :

Email :

Guidance

CSC v5.1