The purpose of this document is to walk individuals who solely manage servers through the *2022 IT Risk Assessment - Servers* assessment. The layout of the questions is similar to what the individual will see when completing the assessment using the Google Form.

2022 IT Risk Assessment - Servers

At Texas A&M, state law requires us to perform annual risk assessments for all IT resources (laptops, servers, applications, etc.). Usually this assessment is performed by professional IT staff for your unit, but in some cases it must be completed by individuals who manage or have admin rights on an IT resource.
The questions asked in this assessment are directly related to a security requirement which must be followed by anyone that manages an IT resource. When possible, we've provided a link directly to the university requirement that prompted each question.
This assessment has six main sections. Section 1 is used to gather general information; the assessment questions will start in either Section 2 or Section 3 depending on the type of servers (physical, virtual). Your answers for some questions will determine the questions in the next section; this is done to skip questions that do not apply to your IT resource.

A copy of the assessment results will be sent to the email address provided below. You are encouraged to keep the results for your records.

Section 1: General Information	
Section comments:	Section 1 is for gathering general information about the server.
a	**Name for the server:**
Comments:	Separate multiple names with a comma.
Answer Choices:	free text
b	**Server identification number used by the unit:**
Comments:	Separate multiple identification numbers with a comma. TAMU asset number used for/listed in FAMIS/Canopy, department level identification numbers, etc. Most departments add a service tag label on physical servers that help track it for general inventory management practices. This tag is often easily visible on the server. Virtual servers may not have an identification number and so put "N/A - virtual servers".
Answer Choices:	free text
c	**Quantity:**
Comments:	Provide the number of servers included in this assessment. Enter that number (e.g. 1, 2, 3)
Answer Choices:	free text

d	**Server description:**						
Comments:	Explain what the server is used for. For example: "This physical server is used for research." or "This includes the research cluster used to support my teaching and research."						
Answer Choices:	free text						
e	**Operating system (OS):**						
Comments:	Select the operating system for the server.						
Answer Choices:	Windows	macOS	Linux or other UNIX	Other			
f	**Number of people with authorized access to the server:**						
Comments:	Enter a number (e.g. 1, 2, 3)						
Answer Choices:	free text						
g	**What is the highest category of data stored or processed by this IT resource?**						
Comments:	If you are not sure how to classify the data, use the data classification calculator in the link below.						
Data calculator:	https://u.tamu.edu/datacalc						
Answer Choices:	Public	University-Internal	Confidential	Critical			
h	**What is the impact level of the server?**						
Comments:	If you are not sure what the server's impact level is, use the impact level calculator in the link below.						
Impact calculator:	https://u.tamu.edu/impactcalc						
Answer Choices:	Low	Moderate	High				
i	**If there are virtual servers, who manages the physical host/hypervisor?**						
Comments:	Select all that apply. If there are no virtual servers, select "N/A - no virtual servers".						
Answer Choices:	Manage personally	Unit IT staff managed	University managed (e.g., Aggie Cloud, etc.)	Vendor managed (AWS, Azure, etc.)	Other	N/A - no virtual servers	

j	If there are physical servers, where are they located?						
Comments:	Select all that apply. If there are no physical servers, select "N/A - no physical servers".						
Answer Choices:	Office	Lab	Shared workspace behind a lockable door	Unit IT server closet, server room, or data center	University managed data center (West Campus Data Center, Teague)	Other	N/A - no physical servers
k	**Type of server:**						
Comments:	Physical server – you are responsible/maintain the hardware and operating system. Virtual server – you are responsible/maintain the operating system. Manage both physical and virtual – you are responsible/maintain both physical and virtual servers. The servers should have the same operating system.						
Answer Choices:			Physical	Virtual	Manage both physical and virtual		
Next Section:	**Depends on answer choice for question k.**		**Section 2: Physical Access (Pg. 3)**	**Section 3: Access Management (Pg. 4)**	**Section 2: Physical Access (Pg. 3)**		

Only answer these questions if "Physical" or "Manage both physical and virtual" was the answer for question k in Section 1.

Section 2: Physical Access							
Section comments:	Section 2 is the start of the assessment when assessing physical servers and deals with where the server is maintained.						
1	**Is physical access to the room where the server is kept controlled to prevent unauthorized access?**						
Requirement:	https://it.tamu.edu/cc/PE-3						
Answer Choices:	No	Yes					
2	**Are measures in place to determine who has accessed the room where the server is kept?**						
Requirement:	https://it.tamu.edu/cc/PE-3						
Comments:	This may include AVST, card swipe, logs, biometrics, etc.						
Answer Choices:	No	Yes					
Next Section:	**Section 3: Access Management (Pg. 4)**						

These questions must always be answered.

Section 3: Access Management							
Section comments:	Section 3 is the start of the assessment if just assessing virtual servers. The section focuses on user account access, passwords, authentication systems, etc. It is broken up into parts based on the answers selected.						
1	**Is a documented procedure in place for granting access?**						
Requirement:	https://it.tamu.edu/cc/AC-2						
Answer Choices:	No documented procedure exists		Yes, a documented procedure exists				
2	**Is a documented procedure in place to ensure access is limited based on least privilege?**						
Requirement:	https://it.tamu.edu/cc/AC-6						
Comments:	The university employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with university missions and business functions. More information on least privilege can be found in the link below.						
More information:	https://en.wikipedia.org/wiki/Principle_of_least_privilege						
Answer Choices:	No documented procedure exists		Yes, a documented procedure exists				
3	**Is multifactor authentication used?**						
Requirement:	https://it.tamu.edu/cc/IA-2						
Comments:	Multifactor authentication adds an extra layer of security. Texas A&M University uses Duo for NetID to meet this requirement.						
Website link:	Duo:	https://it.tamu.edu/duo/					
Website link:	NetID:	https://infrastructure.tamu.edu/identity/netid.html					
Website link:	CAS:	https://infrastructure.tamu.edu/auth/CAS/cas.html					
Answer Choices:	No	Yes, alternate 3rd party tool	Yes, using Duo but not through CAS	Yes, through university CAS authentication			

4	**Have all default passwords been changed (e.g., blank administrator passwords, user ID/passwords that the supplier provided, or that came with the operating system like admin/admin, root/root, or sudo/sudo)?**					
Requirement:	https://it.tamu.edu/cc/CM-1					
Comments:	Example default passwords: blank administrator passwords, user ID/passwords that the supplier provided for the IT resource, or that came with the IT resource like admin/admin, root/root, or sudo/sudo Many servers come with a standard default account that uses the same standard name/password combination across all servers of that type, brand, series, etc. Malicious actors try to gain unauthorized access by using those account credentials.					
Answer Choices:	Default passwords not changed	Default passwords changed	No default accounts exist or accounts with default passwords have been removed			
5	**Do documented procedures exist for changing shared account (root, administrator, etc.) passwords when staff or duties change?**					
Requirement:	https://it.tamu.edu/cc/AC-5					
Answer Choices:	No documented procedure exists		Yes, a documented procedure exists	No shared accounts exist		
6	**How long can an IT resource be left unattended before the screen is locked?**					
Requirement:	https://it.tamu.edu/cc/AC-11					
Answer Choices:	No screen lock	Screen lock >30 minutes	Screen lock >15 minutes	Screen lock ≤15 minutes		
7	**Is the server open through the campus firewall?**					
Requirement:	https://it.tamu.edu/cc/SC-5					
Answer Choices:	No	Yes				
8	**Does the server use university central authentication (NetID)?**					
Website link:	NetID https://infrastructure.tamu.edu/identity/netid.html					
Comments:	Not referring to/accounts not in scope for this question: default or pre-defined accounts (e.g., the root user in a Linux operating system, local administrator on Windows).					
Answer Choices:		No	Yes, but some user accounts do not use NetID	Yes, exclusively NetID		
Next Section:	**Depends on answer choice for question 8.**		**3a: Access Management (Pg. 6)**	**Section 4: Resource Maintenance (Pg. 10)**		

Only answer these questions if "No" or "Yes, but some user accounts do not use NetID" was the answer for question 8 in Section 3.

3a: Access Management							
Section comments:	This part of Section 3 focuses on user account access, authentication systems, etc.						
1	**Does each individual person have a unique logon ID/username for standard access (non-elevated privileges) to the IT resource?**						
Requirement:	https://it.tamu.edu/cc/AC-2						
Answer Choices:	IDs/usernames are not used	Only shared IDs/usernames are used	Shared & unique IDs/usernames are used	Only unique IDs/ usernames are used			
2	**Do any third parties (e.g., research affiliates, business associates, service providers, vendors, contractors) have access to the server?**						
Answer Choices:	No	Yes					
3	**Is a documented process in place for the granting and removal of access to third parties?**						
Requirement:	https://it.tamu.edu/cc/IA-8						
Answer Choices:	No documented process exists		Yes, a documented process exists		N/A - no third party will ever be granted access		
4	**How quickly are accounts for terminated employees disabled?**						
Requirement:	https://it.tamu.edu/cc/PS-4						
Answer Choices:	Accounts are not disabled	Greater than 72 hours	Within 72 hours	Within 24 hours	Realtime based on event triggers		
5	**Is there a documented process to remove the accounts of individuals who are no longer authorized to have access?**						
Requirement:	https://it.tamu.edu/cc/AC-2						
Answer Choices:	No documented process exists		Yes, a documented process exists				

6	Is an access banner displayed during authentication?						
Requirement:	https://it.tamu.edu/cc/AC-8						
Comments:	Per AC-8, the login notification (access banner) shall address the following items: (1) Unauthorized use is prohibited; (2) Usage may be subject to security testing and monitoring; (3) Misuse may be subject to criminal prosecution; (4) Users have no expectation of privacy except as otherwise provided by applicable privacy laws; and (5) A reference to University Standard Administrative Procedure 29.01.03.M0.02, Rules for Responsible Computing.						
Answer Choices:	No banner	Server lacks banner functionality	Displayed banner does not meet TAMU Security Control AC-8		Displayed banner meets TAMU Security Control AC-8		
7	**Does the authentication method utilize passwords?**						
Requirement:	https://it.tamu.edu/cc/IA-2						
Answer Choices:			Passwords are not used	Passwords are used	N/A - use other form of authentication		
Next Section:	**Depends on answer choice for question 6.**		**3d: No Authentication (Pg. 9)**	**3b: Password Management (Pg. 7)**	**3c: Authentication (Pg. 9)**		

Only answer these questions if "Passwords are used" was the answer for question 6 in Section 3a.

3b: Password Management							
Section comments:	This part of Section 3 focuses on password requirements.						
1	**What is the minimum required password length?**						
Requirement:	https://it.tamu.edu/cc/IA-5						
Answer Choices:	Allows blank passwords	Allows < 8 characters passwords	Requires ≥8 characters	Requires ≥16 character passwords			

2	**What are the minimum password complexity requirements being enforced?**					
Requirement:	https://it.tamu.edu/cc/IA-5					
Comments:	If passwords can be less than 16 characters, then they must contain three of the following four groups of characters: lower case letters, upper case letters, symbols or numbers. If passwords must be at least 16 characters long, then there are no complexity requirements.					
Answer Choices:	No complexity requirements	Some complexity requirements	Requires at least 3 of the following 4 groups of characters: lower case letters, upper case letters, symbols or numbers	At least 16 characters required - no complexity requirement		
3	**Is the password complexity enforced when a password is created or required to be changed?**					
Requirement:	https://it.tamu.edu/cc/IA-5					
Comments:	If passwords have to be at least 16 characters long, then users are not required to meet the complexity requirements.					
Answer Choices:	No	Yes	At least 16 characters required - no complexity requirement			
4	**How frequently are passwords required to be changed?**					
Requirement:	https://it.tamu.edu/cc/IA-5					
Answer Choices:	Password changes are not forced	Greater than a year	Requires annual changes	Requires semi-annual changes	Requires quarterly changes	At least 16 characters required - never expires
5	**When authentication fails, is the user informed of which part of the username/password combination is incorrect?**					
Requirement:	https://it.tamu.edu/cc/IA-6					
Comments:	Failed login boxes/messages after a failure should not indicate which part of the username/password combination is incorrect. Example message: "login and/or password incorrect."					
Answer Choices:	No	Yes				
6	**How many consecutive failed logon attempts are allowed before automatically locking the account or delaying the next logon prompt?**					
Requirement:	https://it.tamu.edu/cc/AC-7					
Comments:	Account lockouts help against brute force attacks.					
Answer Choices:	No account locking	>10 attempts	≤10 attempts			

7	How long until the IT resource re-enables an account after an account lockout?						
Requirement:	https://it.tamu.edu/cc/AC-7						
Answer Choices:	No account locking	Immediately	<15 minutes	≥15 minutes	Locked until administrator reset		
Next Section:	**Section 4: Resource Maintenance (Pg. 10)**						

Only answer these questions if "N/A, use other form of authentication" was the answer for question 6 in Section 3a.

3c: Authentication	
Section comments:	This part of Section 3 follows up with what type of authentication is used.
1	**What form of authentication is used?**
Requirement:	https://it.tamu.edu/cc/IA-2
Comments:	Example authentication methods: tokens, biometrics, SSH keys, smartphone authenticator applications.
Answer Choices:	free text
Next Section:	**Section 4: Resource Maintenance (Pg. 10)**

Only answer these questions if "Passwords are not used" was the answer for question 6 in Section 3a.

3d: No Authentication	
Section comments:	This part of Section 3 follows up on why authentication is not used.
1	**What activities can be performed on the server without identification or authentication?**
Requirement:	https://it.tamu.edu/cc/AC-14
Answer Choices:	free text
2	**Why is authentication not used before accessing the server?**
Requirement:	https://it.tamu.edu/cc/AC-14
Answer Choices:	free text
Next Section:	**Section 4: Resource Maintenance (Pg. 10)**

These questions must always be answered.

Section 4: Resource Maintenance						
Section comments:	Section 4 focuses on how the server is maintained. It is broken up into parts based on the answers selected.					
1	**Is the installed version of the operating system (OS) officially supported by the vendor?**					
Requirement:	https://it.tamu.edu/cc/SI-3					
Comments:	"Officially supported" means the vendor is still releasing patches/updates. Security patches/updates are important because they fix known weaknesses and vulnerabilities that are used by malicious actors.					
Answer Choices:	No	No, but a current exception request has been approved by the CISO	Yes			
2	**Is a documented process followed for installing security patches/updates?**					
Requirement:	https://it.tamu.edu/cc/CM-1					
Comments:	The process should cover both the OS level and all installed applications and/or software.					
Answer Choices:	No documented process exists	Yes, security patches/updates are installed using a documented process				
3	**Are proposed security patches validated before deploying?**					
Comments:	Validation examples: (a) Read/review the feedback from the community that have already installed the patches/updates. (b) Read/review the release notes. (c) Test the update/patch on a low impact resource before fully deploying. (d) Test the update/patch in a test or development environment/system.					
Requirement:	https://it.tamu.edu/cc/CM-1					
Answer Choices:	No	Yes				

4	**Is the university required schedule for installing OS level security patches being followed?**					
Requirement:	https://it.tamu.edu/cc/CM-1					
Comments:	OS security patches/updates released by the vendor or development organization. University required schedule: (a) Security patches categorized as "critical" by the vendor = installed within 30 days of release; (b) Security patches categorized as "high" by the vendor = installed within 45 days of release; (c) Other security patches = installed within 60 days of release.					
Answer Choices:	No	No, but a current exception request has been approved by the CISO	Yes			
5	**Is all software installed appropriately licensed?**					
Requirement:	https://it.tamu.edu/cc/CM-11					
Comments:	Free versions of proprietary software are likely to contain malware.					
Answer Choices:	No	Yes				
6	**Are any unsupported applications and/or software installed (e.g., the application is no longer receiving security updates from the vendor or development organization)?**					
Requirement:	https://it.tamu.edu/cc/SI-3					
Comments:	"Unsupported" means the vendor is no longer releasing patches/updates. Unsupported software not only leaves you and the university open to security risks but may cause other issues as software and hardware may stop working or be incompatible with newer systems.					
Answer Choices:	No	Yes, but a current exception request has been approved by the CISO	Yes			
7	**Is the university required schedule for installing security patches being followed for all installed software and/or applications?**					
Requirement:	https://it.tamu.edu/cc/CM-1					
Comments:	Security updates for applications and/or software are released by the various vendors or development organizations. University required schedule: (a) Security patches categorized as "critical" by the vendor = installed within 30 days of release; (b) Security patches categorized as "high" by the vendor = installed within 45 days of release; (c) Other security patches = installed within 60 days of release.					
Answer Choices:	No	No, but a current exception request has been approved by the CISO	Yes			

8	**Have all extra (unused) functionality (such as scripts, drivers, features, subsystems, file systems) been disabled or removed?**					
Requirement:	https://it.tamu.edu/cc/CM-1					
Answer Choices:	No	Yes	Extra functionality features were not installed			
9	**Is all data classified as Confidential (or higher) stored in an encrypted manner?**					
Requirement:	https://it.tamu.edu/cc/SC-13					
Answer Choices:	No	Yes, using selective file encryption	Yes, using whole disk encryption	Not required, no Confidential (or higher) data stored		
10	**When was the last vulnerability scan completed?**					
Requirement:	https://it.tamu.edu/cc/RA-5					
Comments:	Per the requirement, all IT resources, even those on a private subnet or firewalled off are to be scanned regularly by the Division of IT - Security Assessment team. If you have questions, talk to your unit IT staff.					
Answer Choices:	Never scanned	Scanned >12 months ago	Scanned <12 months ago	Scanned <6 months ago		
11	**How often is the baseline configuration of the server reviewed for alignment with manufacturer recommendations and industry best practices?**					
Requirement:	https://it.tamu.edu/cc/CM-2					
Comments:	Baseline configuration changes may be required over time as new threats and vulnerabilities occur. Link to the Center for Information Security Benchmarks is below.					
Website link:	https://www.cisecurity.org/					
Answer Choices:	Baseline configuration is not reviewed	Baseline configuration reviewed >12 months ago	Baseline configuration reviewed <12 months ago			
12	**Is a documented change process followed?**					
Requirement:	https://it.tamu.edu/cc/CM-3					
Comments:	A change may include: (1) Any implementation of new functionality; (2) Any interruption of service; (3) Any repair of existing functionality; (4) Any removal of existing functionality.					
Answer Choices:	No documented process exists	Yes, a documented process is followed				

13	**Is there a procedure in place to ensure the storage media related to the server is properly sanitized prior to disposal and/or release from your control?**				
Requirement:	https://it.tamu.edu/cc/MP-6				
Comments:	Storage media may include internal or external hard drives. Sanitizing the media removes data that was previously stored. It ensures your data that was stored on the server is not recovered by someone else after the server is no longer in your control.				
Answer Choices:	No documented procedure exists	Yes, a documented procedure exists			
14	**Is the university-supplied data loss prevention (DLP) software installed as appropriate?**				
Requirement:	https://it.tamu.edu/cc/RA-2				
Comments:	Spirion is the university-supplied DLP software. Talk to your unit IT staff to determine if it is appropriate on the server. If it is appropriate, they can help you install it on the server.				
Answer Choices:	No, even though it is appropriate	No, but a current exception request has been approved by the CISO	Yes	Determined it is not appropriate after a discussion with unit IT staff	
15	**Is the university-supplied anti-virus/anti-malware installed?**				
Requirement:	https://it.tamu.edu/cc/SI-3				
Comments:	CrowdStrike Falcon is the university-supplied anti-virus/anti-malware. This can only be provided to System part 02 members. Talk to your unit IT staff as they will be the ones that work with you to install it on the server.				
Answer Choices:	[redacted]	No	No, but a current exception request has been approved by the CISO	Yes	
Next Section:	**Depends on answer choice for question 15.**	**4b: Security Management (Pg. 14)**		**4a: Security Management (Pg. 14)**	

Only answer this question if "Yes" was the answer for question 15 in Section 4.

4a: Security Management							
Section comments:	This part of Section 4 follows up on security management.						
1	**Do you make changes to the university-supplied anti-virus/anti-malware to reduce its effectiveness?**						
Requirement:	https://it.tamu.edu/cc/SI-3						
Comments:	Changes can include disabling, bypassing, or altering.						
Answer Choices:	No	Yes					
Next Section:	**Section 5: Logs (Pg. 15)**						

Only answer this question if "No" or "No, but a current exception request has been approved by the CISO" was the answer for question 15 in Section 4.

4b: Security Management						
Section comments:	This part of Section 4 follows up on security management.					
1	**Is any anti-virus/anti-malware installed?**					
Requirement:	https://it.tamu.edu/cc/SI-3					
Comments:	Sometimes the university-supplied anti-virus/anti-malware cannot not be installed due to certain restraints or compatibility issues. If that is the case, then anti-virus software that is compatible and/or supported by the vendor should be used.					
Answer Choices:	No, but available and allowed	No, since there is no supported anti-virus available or allowed	Yes			
Next Section:	**Section 5: Logs (Pg. 15)**					

These questions must always be answered.

Section 5: Logs					
Section comments:	Section 5 focuses on logging requirements for the server. It is broken up into parts based on the answers selected.				
1	**Where are logs stored?**				
Requirement:	https://it.tamu.edu/cc/AU-2				
Comments:	A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network.				
Answer Choices:		Unknown or no logs are stored	Logs stored locally	Logs sent to external server	Logs sent to Division of IT Splunk service
Next Section:	**Depends on answer choice for question 1.**	**Section 6: Backups & Recovery (Pg. 19)**	**5a: Logs (Pg. 15)**		**5b: Logs (Pg. 17)**

Only answer these questions if "Logs stored locally" or "Logs sent to external server" was the answer for question 1 in Section 5.

5a: Logs						
Section comments:	This part of Section 5 focuses on logging requirements.					
1	**Are the date and time recorded with each logged event?**					
Requirement:	https://it.tamu.edu/cc/AU-3					
Answer Choices:	Date & Time are not recorded	Date & Time are recorded				
2	**Do logged events include the User IDs (usernames)?**					
Requirement:	https://it.tamu.edu/cc/AU-3					
Answer Choices:	No	Yes				
3	**Are authentication attempts logged?**					
Requirement:	https://it.tamu.edu/cc/AU-2					
Answer Choices:	No logging	Logs only failed attempts	Logs successful & failed attempts			

4	**Do logged events include the origination of the event?**						
Requirement:	https://it.tamu.edu/cc/AU-3						
Answer Choices:	No	Yes					
5	**Do logged events include the event type?**						
Requirement:	https://it.tamu.edu/cc/AU-3						
Answer Choices:	No	Yes					
6	**Are there log entries that indicate when the logging process is enabled/disabled?**						
Comments:	Turning the audit logs off (or pausing them) prior to performing illicit activities is a common practice for malicious users wishing to avoid detection.						
Answer Choices:	Unknown or no	Yes	Logging cannot be disabled				
7	**Is access to data classified as University-Internal (or higher) logged?**						
Requirement:	https://it.tamu.edu/cc/AU-2						
Answer Choices:	No access logging	Access logging is enabled	There is no access to University-Internal (or higher) data				
8	**Do logged events include the outcome (success or failure) of the event?**						
Requirement:	https://it.tamu.edu/cc/AU-3						
Answer Choices:	No	Failure only	Yes				
9	**Is the system clock/time synchronized with an approved time service?**						
Requirement:	https://it.tamu.edu/cc/AU-8						
Answer Choices:	Clock is not synchronized	Clock is synchronized via independent NTP service		Clock is synchronized via university approved NTP service (ntp[1-3].tamu.edu)			
10	**How are logs monitored?**						
Requirement:	https://it.tamu.edu/cc/AU-2						
Comments:	Reviewing logs manually or with the use of a tool, is a proactive measure administrators can take to help detect possible security threats or issues that impact the performance or security of the servers.						
Answer Choices:	Logs are never reviewed	Manually on an ad hoc basis	Manually on a regular schedule	Real-time using automated systems			

11	Are controls in place to prevent the deletion or modification of logs?						
Requirement:	https://it.tamu.edu/cc/AU-9						
Answer Choices:	Logs are not protected	Logs are protected					
12	Are logs kept a minimum of 30 days?						
Requirement:	https://it.tamu.edu/cc/AU-11						
Answer Choices:	No	Yes					
Next Section:	**Section 6: Backups & Recovery (Pg. 19)**						

Only answer these questions if "Logs sent to Division of IT Splunk service" was the answer for question 1 in Section 5.

5b: Logs						
Section comments:	This part of Section 5 focuses on logging requirements when logs are sent to the Division of IT Splunk service.					
1	Are the date and time recorded with each logged event?					
Requirement:	https://it.tamu.edu/cc/AU-3					
Answer Choices:	Date & Time are not recorded	Date & Time are recorded				
2	Do logged events include the User IDs (usernames)?					
Requirement:	https://it.tamu.edu/cc/AU-3					
Answer Choices:	No	Yes				
3	Are authentication attempts logged?					
Requirement:	https://it.tamu.edu/cc/AU-2					
Answer Choices:	No logging	Logs only failed attempts	Logs successful & failed attempts			
4	Do logged events include the origination of the event?					
Requirement:	https://it.tamu.edu/cc/AU-3					
Answer Choices:	No	Yes				

5	**Do logged events include the event type?**						
Requirement:	https://it.tamu.edu/cc/AU-3						
Answer Choices:	No	Yes					
6	**Are there log entries that indicate when the logging process is enabled/disabled?**						
Comments:	Turning the audit logs off (or pausing them) prior to performing illicit activities is a common practice for malicious users wishing to avoid detection.						
Answer Choices:	Unknown or no	Yes	Logging cannot be disabled				
7	**Is access to data classified as University-Internal (or higher) logged?**						
Requirement:	https://it.tamu.edu/cc/AU-2						
Answer Choices:	No access logging	Access logging is enabled	There is no access to University-Internal (or higher) data				
8	**Do logged events include the outcome (success or failure) of the event?**						
Requirement:	https://it.tamu.edu/cc/AU-3						
Answer Choices:	No	Failure only	Yes				
9	**Is the system clock/time synchronized with an approved time service?**						
Requirement:	https://it.tamu.edu/cc/AU-8						
Answer Choices:	Clock is not synchronized	Clock is synchronized via independent NTP service		Clock is synchronized via university approved NTP service (ntp[1-3].tamu.edu)			
Next Section:	**Section 6: Backups & Recovery (Pg. 19)**						

These questions must always be answered.

Section 6: Backups & Recovery					
Section comments:	Section 6 focuses on data backup requirements and recovery procedures for the server. It is broken up into parts based on the answers selected.				
1	**Are data backups performed?**				
Requirement:	https://it.tamu.edu/cc/CP-9				
Comments:	Backups help prevent data from being lost if the primary storage media has been corrupted and/or stolen.				
Answer Choices:	[redacted]	No	Yes	Yes, third party/vendor responsibility	
Next Section:	**Depends on answer choice for question 1.**	**Done**	**6a: Backups & Recovery (Pg. 19)**	**6b: Vendor Managed Backups (Pg. 20)**	

Only answer these questions if "Yes" was the answer for question 1 in Section 6.

6a: Backups & Recovery						
Section comments:	This part of Section 6 focuses on data backup requirements and recovery procedures.					
1	**How often are data backups performed?**					
Requirement:	https://it.tamu.edu/cc/CP-9					
Answer Choices:	Ad hoc backups performed	Scheduled monthly backups performed	Scheduled weekly backups performed	Scheduled daily backups performed		
2	**How frequently is data recovery tested to ensure the backup works?**					
Requirement:	https://it.tamu.edu/cc/CP-9					
Answer Choices:	Do not test	Performed but not on an annual basis	Performed at least annually (ad hoc or scheduled)	Performed at least quarterly (ad hoc or scheduled)		
3	**Are the backup media encrypted?**					
Requirement:	https://it.tamu.edu/cc/CP-9					
Answer Choices:	No	Yes	Not required, no Confidential (or higher) data			

4	Are recovery procedures in place for the server?					
Requirement:	https://it.tamu.edu/cc/CP-10					
Comments:	Recovery procedures include more than just the backups. They help ensure the administrator can get the server back to a known secure state after a disruption, compromise, or failure.					
Answer Choices:	No documented procedures exist	Yes, documented procedures exist				
Next Section:	**Done**					

Only answer these questions if "Yes, third party/vendor responsibility" was the answer for question 1 in Section 6.

6b: Vendor Managed Backups							
Section comments:	This part of Section 6 focuses on data backups managed by the third party/vendor.						
1	**Is there documentation from the third party/vendor concerning their backup policies and procedures?**						
Requirement:	https://it.tamu.edu/cc/CP-9						
Answer Choices:	Unknown or No	Yes					
2	**Does the frequency and extent of backups performed by the third party/vendor meet your requirements as determined by the potential impact of data loss or corruption?**						
Requirement:	https://it.tamu.edu/cc/CP-9						
Answer Choices:	No	Yes					
Next Section:	**Done**						