The purpose of this document is to walk individuals who manage servers through the*2020 IT Risk Assessment - Servers* assessment.

2020 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.

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.
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".
c	**Quantity:**
Comments:	Provide the number of servers included in this assessment. Enter that number (e.g. 1, 2, 3)
d	**Server description:**
Comments:	Briefly tell us about the server and what it 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."

e	**Type of server:**						
Comments:	Physical server – you are responsible/maintain the hardware and OS software. Virtual server – you are responsible/maintain the virtual server software. Physical and virtual servers should be assessed separately.						
Answer Choices:			Physical	Virtual			
Next Section:	**Depends on answer choice for question e.**		**Section 2: Physical Access (Pg 3)**	**Section 3: Access Management (Pg 3)**			
f	**If the server is virtual, who manages the physical host/hypervisor?**						
	If you do not manage the physical host/hypervisor, provide the resource's point of contact information (name, email address, university department or hosting vendor name). If you do not have virtual servers, enter N/A as your answer.						
g	**Operating system (OS):**						
Comments:	Select the operating system for the server.						
Answer Choices:	Windows	macOS	Linux or other UNIX	Other			
h	**Number of people with authorized access to the server:**						
Comments:	Enter a number (e.g. 1, 2, 3)						
i	**Where is the server located?**						
Comments:	Select all that apply. For virtual servers, consider answering for the location of the physical host/hypervisor.						
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, Wehner)	University (Aggiecloud) or Vendor (AWS, Azure, etc.) hosted	
j	**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			
k	**What is the impact level of the application?**						

Comments:	If you are not sure what the application'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				

Only answer these questions if "Physical" was the answer for question e 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 3)**						

These questions must always be answered.

Section 3: Access Management

Section comments:	Section 3 is the start of the assessment if assessing virtual servers and focuses on user account access, passwords, authentication systems, etc. It is broken up into parts based on the answers provided.						
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 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			
3	**Is multifactor authentication used?**						
Requirement:	https://it.tamu.edu/cc/IA-2						
Comments:	University-supplied multifactor tool is called Duo: https://it.tamu.edu/duo/.						
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						
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 many minutes of inactivity does the server allow before locking a user session?**						
Requirement:	https://it.tamu.edu/cc/AC-11						
Answer Choices:	No idle lockout	Idle lockout >30 minutes	Idle lockout between 16-30 minutes		Idle lockout ≤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)?**						
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 5)**		**Section 4: Resource Maintenance (Pg 8)**		

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	**Are User IDs (usernames) unique?**						
Requirement:	https://it.tamu.edu/cc/AC-11						
Answer Choices:	Users are not identified	Shared IDs are used	Shared & Unique IDs are used	Only Unique IDs 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 often are accounts (e.g. standard and elevated) reviewed for deactivation (due to inactivity, termination, etc.)?**						
Requirement:	https://it.tamu.edu/cc/PS-4						
Answer Choices:	Accounts are not reviewed	Ad hoc reviews & updates	Within 72 hours	Within 24 hours	Realtime based on event triggers		

5	**Are deactivated/disabled accounts removed after a set time period?**						
Requirement:	https://it.tamu.edu/cc/AC-2						
Answer Choices:	No	> 6 months	Within 6 months				
6	**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 8)**	**3b: Password Management (Pg 6)**	**3c: Authentication (Pg 7)**		

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-2						
Answer Choices:	Allows blank passwords	Allows < 8 characters passwords	Requires at least 8 characters	Requires > 15 character passwords			
2	**What are the minimum password complexity requirements being enforced?**						
Requirement:	https://it.tamu.edu/cc/IA-2						
Comments:	If less than 16 characters, password must contain three of the following four groups of characters: lower case letters, upper case letters, symbols or numbers. If the password is at least 16 characters long, there are no complexity requirements.						
Answer Choices:	No complexity requirements	Some complexity requirements	Requires 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 changed by a user?**						
Requirement:	https://it.tamu.edu/cc/IA-5						
Comments:	If the password is at least 16 characters long, then users are not required to meet the complexity requirements.						

Answer Choices:	No	Yes					
4	**How often are users forced to change their passwords?**						
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 portion of the authentication process failed?**						
Requirement:	https://it.tamu.edu/cc/IA-6						
Answer Choices:	Message indicates if it was the User ID (username) or password that failed		Message provides no indication as to the failure reason				
6	**How many consecutive invalid access attempts are allowed before automatically locking the account or delaying the next login 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 or less attempts				
7	**How long before the system 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 or longer	Locked until administrator reset		
Next Section:	**Section 4: Resource Maintenance (Pg 8)**						

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, smartphone authenticator applications.
Answer Choices:	free text
Next Section:	**Section 4: Resource Maintenance (Pg 8)**

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 serrver 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 8)**

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 provided.					
1	**Is the installed version of the operating system (OS) officially supported by the vendor?**					
Requirement:	https://it.tamu.edu/cc/SI-3					
Answer Choices:	No	No, but an exception has been approved by the CISO	Yes			
2	**Is a documented process followed for installing security updates/patches?**					
Requirement:	https://it.tamu.edu/cc/CM-1					

Answer Choices:	No documented process exists		Yes, a documented process exists				
3	**Are the proposed security updates/patches tested before deploying?**						
Requirement:	https://it.tamu.edu/cc/CM-1						
Answer Choices:	No	Yes					
4	**How long after a security update is released before the server is updated?**						
Requirement:	https://it.tamu.edu/cc/CM-1						
Comments:	Security updates for operating systems or applications/software are released by the vendor or development organization.						
Answer Choices:	Do not update	greater than 60 days	within 60 days	within 30 days	Immediately		
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						
Answer Choices:	No	Yes, but an exception has been approved by the CISO		Yes			
7	**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				
8	**Is stored data encrypted?**						
Requirement:	https://it.tamu.edu/cc/SC-13						
Answer Choices:	No encryption	Selective file encryption	Whole disk encryption				
9	**When was the last vulnerability scan?**						
Requirement:	https://it.tamu.edu/cc/RA-5						
Answer Choices:	Never scanned	Scanned >12 months ago	Scanned <12 months ago	Scanned <6 months ago			

10	**Is data loss protection (DLP) software used?**						
Requirement:	https://it.tamu.edu/cc/RA-2						
Answer Choices:	No	Yes	Yes, use the university-supplied DLP software				
11	**Is the university-supplied anti-virus/anti-malware installed?**						
Requirement:	https://it.tamu.edu/cc/SI-3						
Answer Choices:			No	No, but an exception has been approved by the CISO		Yes	
Next Section:	**Depends on answer choice for question 11.**		**Section 5: Logs (Pg 10)**			**4a: Security Management (Pg 10)**	

Only answer this question if "Yes" was the answer for question 11 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 10)**						

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 provided.
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 (Pg 14)**	**5a: Logs (Pg 11)**		**5b: Logs (Pg 13)**

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					
7	**Is access to University-Internal (or higher) data 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	**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)			
9	**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 application						
Answer Choices:	Logs are never reviewed	Manually on an ad hoc basis	Manually on a regular schedule	Real-time using automated sytems			
10	**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					
11	**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 (Pg 14)**						

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					
7	**Is access to University-Internal (or higher) data 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	**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 (Pg 14)**				

These questions must always be answered.

Section 6: Backups

Section comments:	Section 6 focuses on data backup requirements for the server. It is broken up into parts based on the answers provided.					
1	**Are data backups performed?**					
Requirement:	https://it.tamu.edu/cc/CP-9					
Answer Choices:			No	Yes	Yes, third party/vendor responsibility	
Next Section:	**Depends on answer choice for question 1.**		**Done**	**6a: Backups (Pg 14)**	**Done**	

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

6a: Backups

Section comments:	This part of Section 6 focuses on data backup requirements.					
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	Ad hoc testing	Scheduled test performed at least annually	Scheduled test performed at least quarterly		
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			
Next Section:	**Done**					