The purpose of this document is to walk individuals who solely manage applications through the *2022 IT Risk Assessment - Applications* 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 - Applications

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 five main sections. Section 1 is used to gather general information; the assessment questions start in Section 2. 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 application.
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 application.			
a	**Name of the application:**			
Answer Choices:	free text			
b	**Application description:**			
Comments:	Describe what the application does and/or what it is used for. For example: "This application is used to collect research data by...." or "This application is used for business function {insert function here} within the college."			
Answer Choices:	free text			
c	**Student Access:**			
Comments:	Select the answer choice that shows whether or not students use the application.			
Answer Choices:	No students have access to the application	This is a business application; only student workers have access	This application is used in teaching or research; some students have access	Any student may access this application

d	What is the highest category of data stored or processed by this application?						
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			
e	**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				
Next Section:	**Section 2: Access Management (Pg. 2)**						

Section 2: Access Management					
Section comments:	Section 2 is the start of the assessment and 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, default account passwords, etc.)?**						
Requirement:	https://it.tamu.edu/cc/CM-1						
Comments:	Many applications come from the vendor with a standard default account that uses the same standard name/password combination for every instance of the application. 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 many minutes of inactivity does the application 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 15-30 minutes		Idle lockout ≤15 minutes	Application does not support user sessions	
7	**Is the application open through the campus firewall?**						
Requirement:	https://it.tamu.edu/cc/SC-5						
Answer Choices:	No	Yes					

8	Does the application use university central authentication (NetID)?					
Comments:	Not referring to default or pre-defined accounts (e.g., the root user in a Linux operating system, local administrator on Windows). Link to the Division of IT Infrastructure Services for foundational identity and access services is below.					
Website link:	NetID https://infrastructure.tamu.edu/identity/netid.html					
Answer Choices:	[redacted]	No	Yes, but some user accounts do not use NetID	Yes, exclusively NetID		
Next Section:	**Depends on answer choice for question 8.**	**2a: Access Management (Pg. 4)**		**Section 3: Resource Maintenance (Pg. 9)**		

Only answer these questions if "No" or "Yes, but some user accounts do not use NetID" was the answer for question 8 in Section 2.

2a: Access Management							
Section comments:	This part of Section 2 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 application?**						
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	Application 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.**		**2d: No Authentication (Pg. 8)**	**2b: Password Management (Pg. 6)**	**2c: Authentication (Pg. 8)**		

Only answer these questions if "Passwords are used" was the answer for question 6 in 2a

2b: Password Management							
Section comments:	This part of Section 2 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	**Are passwords required to be changed during first login?**						
Requirement:	https://it.tamu.edu/cc/IA-5						
Answer Choices:	Users are not forced to change passwords on first login	Users are forced to change passwords on first login	Passwords are created by the user when the account is created				
4	**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				

5	**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	
6	**Are passwords hidden during authentication?**						
Requirement:	https://it.tamu.edu/cc/IA-6						
Answer Choices:	Passwords are shown in clear text		Password characters are masked		Password characters are invisible		
7	**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					
8	**Is a mechanism in place to report and reset lost or compromised passwords?**						
Requirement:	https://it.tamu.edu/cc/IA-5						
Answer Choices:	No password reset mechanism in place		Yes, use a non-secure password reset mechanism		Yes, use a secure password reset mechanism		
9	**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				
10	**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 3: Resource Maintenance (Pg. 9)**						

Only answer these questions if "N/A, use other form of authentication" was the answer for question 6 in 2a.

2c: 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 3: Resource Maintenance (Pg. 9)**

Only answer these questions if "Passwords are not used" was the answer for question 6 in 2a.

2d: No Authentication	
Section comments:	This part of Section 2 follows up on why authentication is not used.
1	**What activities can be performed on the application 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 application?**
Requirement:	https://it.tamu.edu/cc/AC-14
Answer Choices:	free text
Next Section:	**Section 3: Resource Maintenance (Pg. 9)**

These questions must always be answered.

Section 3: Resource Maintenance						
Section comments:	Section 3 focuses on how the application is maintained. It is broken up into parts based on the answers selected.					
1	**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		
2	**Is all data classified as Confidential (or higher) transmitted in an encrypted manner?**					
Requirement:	https://it.tamu.edu/cc/SC-8					
Answer Choices:	No	Yes	Not required, no Confidential (or higher) data transmitted			
3	**What is the application service model type?**					
Requirement:	https://rulesadmin.tamu.edu/rules/download/29.01.03.M0.13					
Comments:	Information about cloud service models are available on the Division of IT website:					
Website link:	Cloud Computing	https://u.tamu.edu/cloud-computing				
Answer Choices:			Not a cloud service	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Next Section:	**Depends on answer choice for question 3.**		**3a: Resource Maintenance (Pg. 10)**	**3d: Resource Maintenance (Pg. 13)**		

Only answer these questions if "Not a cloud service (on premise)" was the answer for question 3 in Section 3.

3a: Resource Maintenance							
Section comments:	This part of Section 3 follows up on source code access to the application.						
1	**Do you have access to the source code?**						
Answer Choices:			Vendor-provided (no/limited access to source code)	Open Source Application (full access to source code)	Developed internally (full ownership of source code)		
Next Section:	**Depends on answer choice for question 1.**		**3b: Resource Maintenance (Pg. 10)**	**3c: Resource Maintenance (Pg. 12)**			

Only answer these questions if "Vendor-provided (no/limited access to source code)" was the answer for question 1 in 3a.

3b: Resource Maintenance						
Section comments:	This part of Section 3 focuses on how the application is maintained when there is no access to the source code.					
1	**Is the application (including dependent libraries and APIs) still receiving security updates from the vendor or development organization?**					
Requirement:	https://it.tamu.edu/cc/SI-3					
Comments:	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					
Answer Choices:	No documented process exists	Yes, security patches/updates are installed using a documented process				

3	Is the university required schedule for installing security patches being followed?					
Requirement:	https://it.tamu.edu/cc/CM-1					
Comments:	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			
4	**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		
5	**Has an installation guide been created indicating all configurations and settings?**					
Requirement:	https://it.tamu.edu/cc/SA-10					
Answer Choices:	No	Provided by the Vendor	Yes			
6	**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				
Next Section:	**Section 4: Logs (Pg. 15)**					

Only answer these questions if "Open Source Application (full access to source code)" or "Developed internally (full ownership of source code)" was the answer for question 1 in 3a.

3c: Resource Maintenance							
Section comments:	This part of Section 3 focuses on how the application is maintained when there is access to the source code.						
1	**Is the application (including dependent libraries and APIs) still receiving security updates from the vendor or development organization?**						
Requirement:	https://it.tamu.edu/cc/SI-3						
Comments:	Security patches/updates are important because they fix known weaknesses and vulnerabilities that are used by malicious actors. If the application is developed internally, then the individual and/or team that created the application is the development organization.						
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						
Answer Choices:	No documented process exists	Yes, security patches/updates are installed using a documented process					
3	**Is the university required schedule for installing security patches being followed?**						
Requirement:	https://it.tamu.edu/cc/CM-1						
Comments:	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				
4	**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			

5	Has an installation guide been created indicating all configurations and settings?					
Requirement:	https://it.tamu.edu/cc/SA-10					
Answer Choices:	No	Provided by the Vendor	Yes			
6	**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				
7	**Is a documented System Development Life Cycle (SDLC) being followed?**					
Requirement:	https://it.tamu.edu/cc/SA-3					
Answer Choices:	No	Yes	N/A - no source code modification occurs			
8	**Is all source code stored in a source code repository which enforces version control?**					
Requirement:	https://it.tamu.edu/cc/SA-10					
Answer Choices:	No	Yes	N/A - no source code modification occurs			
Next Section:	**Section 4: Logs (Pg. 15)**					

Only answer these questions if "Infrastructure as a Service (IaaS)", "Platform as a Service (PaaS)", or "Software as a Service (SaaS)" was the answe for question 3 in Section 3.

3d: Resource Maintenance						
Section comments:	This part of Section 3 focuses on when the application is vendor managed.					
1	**Is the application (including dependent libraries and APIs) still receiving security updates from the vendor or development organization?**					
Requirement:	https://it.tamu.edu/cc/SI-3					
Comments:	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	**Does the service provider report all incidents, suspected or confirmed, that affect university data as soon as practical?**						
Requirement:	https://it.tamu.edu/cc/SA-4						
Answer Choices:	Unknown or no	Yes, to the application owner	Yes, to the university CISO				
3	**Does the contract or service agreement stipulate that university data is only used for the purpose of the business agreement?**						
Requirement:	https://it.tamu.edu/cc/SA-4						
Answer Choices:	Unknown or no	Yes					
4	**If the application stores or processes data that is regulated under a legal or contract framework (e.g., FERPA, HIPAA, PCI, CUI, etc.), does the contract or service agreement have specific language in place to ensure this data is properly managed according to the appropriate guidelines?**						
Requirement:	https://it.tamu.edu/cc/SA-4						
Answer Choices:	Unknown or no	Yes	No data covered under a legal or contract framework				
5	**Is the TAMUS records retention schedule followed for university data stored in the application?**						
Requirement:	https://rulesadmin.tamu.edu/rules/download/29.01.03.M0.13						
Answer Choices:	Unknown or no	Yes					
6	**Has the application undergone the university security review process?**						
Requirement:	https://rulesadmin.tamu.edu/rules/download/29.01.03.M0.13						
Website:	Reviewed Cloud Services:		https://it.tamu.edu/community/tools/reviewed-cloud-services.php				
Answer Choices:	No	Submitted for review	Yes, already approved				
Next Section:	**Section 5: Backups (Pg. 18)**						

Only answer these questions if coming from section 3b or 3c.

Section 4: Logs					
Section comments:	Section 4 focuses on logging requirements for the application. 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 5: Backups (Pg. 18)**	**4a: Logs (Pg. 15)**		**4b: 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 4.

4a: Logs							
Section comments:	This part of Section 4 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	**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 systems			
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 5: Backups (Pg. 18)						

Only answer these questions if "Logs sent to Division of IT Splunk service" was the answer for question 1 in Section 4.

4b: Logs							
Section comments:	This part of Section 4 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				
Next Section:	**Section 5: Backups (Pg. 18)**						

These questions must always be answered.

Section 5: Backups					
Section comments:	Section 5 focuses on data backup requirements for the application. 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:		No	Yes	Yes, third party/vendor responsibility	
Next Section:	**Depends on answer choice for question 1.**	**Done**	**5a: Backups (Pg. 19)**	**5b: Vendor Managed Backups (Pg. 19)**	

Only answer these questions if "Yes" was the answer for question 1 in Section 5.

5a: Backups						
Section comments:	This part of Section 5 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	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			
Next Section:	**Done**					

Only answer these questions if "Yes, third party/vendor responsibility" was the answer for question 1 in Section 5.

5b: Vendor Managed Backups						
Section comments:	This part of Section 5 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**					