#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
5.4	**Auditing and Accountability**					
1.	Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk. Refer to CSP 5.13.6 for additional audit requirements related to mobile devices used to access CJI.					
	Based on inquiry and record examination, does the Tribe or TGRA implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior?	____	____	____	CSP 5.4	
	Does the Tribe or TGRA carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components?	____	____	____	CSP 5.4	
2.	Based on inquiry and record examination, does the Tribe or TGRA information system generate audit records for defined events?[1]	____	____	____	CSP 5.4.1	
	Does the Tribe or TGRA's information system produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcome of the events?	____	____	____	CSP 5.4.1	
	Does the Tribe or TGRA periodically review and update the list of agency-defined auditable events?	____	____	____	CSP 5.4.1	

[1] These defined events include identifying significant events which need to be audited as relevant to the security of the information system.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
3.	Based on inquiry and record examination, in the event a Tribe or TGRA does not use an automated system, does manual recording of activities still take place?	____	____	____	CSP 5.4.1	
4.	Based on inquiry and record examination, does the Tribe or TGRA log the following events:					
	1. Successful and unsuccessful system log-on attempts?	____	____	____	CSP 5.4.1.1(1)	
	2. Successful and unsuccessful attempts to use:					
	a. Access permission on a user account, file, directory or other system resource?	____	____	____	CSP 5.4.1.1(1)(a)	
	b. Create permission on a user account, file, directory or other system resource?	____	____	____	CSP 5.4.1.1(2)(b)	
	c. Write permission on a user account, file, directory or other system resource?	____	____	____	CSP 5.4.1.1(2)(c)	
	d. Delete permission on a user account, file, directory or other system resource?	____	____	____	CSP 5.4.1.1(2)(d)	
	e. Change permission on a user account, file, directory or other system resource?	____	____	____	CSP 5.4.1.1(2)(e)	
	3. Successful and unsuccessful attempts to change account passwords?	____	____	____	CSP 5.4.1.1(3)	
	4. Successful and unsuccessful actions by privileged accounts (i.e. root, Oracle, DBA, admin, etc.)?	____	____	____	CSP 5.4.1.1(4)	
	5. Successful and unsuccessful attempts for users to:					
	a. Access the audit log file?	____	____	____	CSP 5.4.1.1(5)(a)	
	b. Modify the audit log file?	____	____	____	CSP 5.4.1.1(5)(b)	
	c. Destroy the audit log file?	____	____	____	CSP 5.4.1.1(5)(c)	
5.	Based on record examination, does the Tribe or TGRA include the following content with every audited event?					
	1. Date and time of the event?	____	____	____	CSP 5.4.1.1.1(1)	
	2. The component of the information system (e.g., software component, hardware component) where the event occurred?	____	____	____	CSP 5.4.1.1.1(2)	
	3. Type of event?	____	____	____	CSP 5.4.1.1.1(3)	
	4. User/subject identity?	____	____	____	CSP 5.4.1.1.1(4)	
	5. Outcome (success or failure) of the event?	____	____	____	CSP 5.4.1.1.1(5)	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
6.	Based in inquiry and record examination, does the Tribe or TGRA information system provide alerts to appropriate agency officials in the event of an audit processing failure?[2]	____	____	____	CSP 5.4.2	
7.	Based on inquiry and record examination, has the Tribe or TGRA's responsible management official designated an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions?	____	____	____	CSP 5.4.3	
	Is the audit review/analysis conducted at a minimum once a week?[3]	____	____	____	CSP 5.4.3	
	Does the Tribe or TGRA increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information?	____	____	____	CSP 5.4.3	
8.	Based on record examination, does the Tribe or TGRA information system provide time stamps for use in audit record generation?	____	____	____	CSP 5.4.4	
	Do the time stamps include the date and time values generated by the internal system clocks in the audit records?	____	____	____	CSP 5.4.4	
	Are the internal information system clocks synchronized on an annual basis?	____	____	____	CSP 5.4.4	
9.	Based on examination, does the Tribe or TGRA information system protect audit information and audit tools from modification, deletion and unauthorized access?	____	____	____	CSP 5.4.5	
10.	Based on record examination, does the Tribe or TGRA retain audit records for at least one (1) year?	____	____	____	CSP 5.4.6	

[2] Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

[3] The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	Once the minimum retention time period has passed, does the Tribe or TGRA continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes?[4]	____	____	____	CSP 5.4.6	
11.	Based on record examination, does the Tribe or TGRA maintain a log for a minimum of one (1) year on all NCIC and III transactions?	____	____	____	CSP 5.4.7	
	Does the III portion of the log clearly identify both the operator and the authorized receiving agency?	____	____	____	CSP 5.4.7	
	Does the III log clearly identify the requester and the secondary recipient?	____	____	____	CSP 5.4.7	
	Does the identification on the log take the form of a unique identifier that is unique to the individual requester and to the secondary recipient throughout the minimum one-year retention period?	____	____	____	CSP 5.4.7	

[4] This includes, for example, retention and availability of audit records relative to information requests, subpoena, and law enforcement actions.