Sample Audit Checklist for CJIS Security Policy (CJISSECPOL)

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	Audit and Accountability (AU)[1]					
1.	Based on inquiry and record examination, has the Tribe or TGRA developed, documented, and disseminated to organizational personnel with audit and accountability responsibilities an agency and system-level audit and accountability policy that:					
	• Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance?	____	____	____	AU-1, a.1.a	
	• Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines?	____	____	____	AU-1, a.1.b	
2.	Does the Tribe or TGRA have procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls?	____	____	____	AU-1, a.2	
3.	Has the Tribe or TGRA designated organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the audit and accountability policy and procedures?	____	____	____	AU-1, b	
4.	Based on inquiry and record examination, does the Tribe or TGRA review and update the current audit and accountability:					
	• Policy annually and following any security incidents involving unauthorized access to Criminal Justice Information (CJI) or Criminal Justice History Record Information (CHRI) or systems used to process, store, or transmit CJI / CHRI?	____	____	____	AU-1, c.1	
	• Procedures annually and following any security incidents involving unauthorized access to CJI / CHRI or systems used to process, store, or transmit CJI / CHRI?	____	____	____	AU-1, c.2	

[1] These requirements are sanctionable for audit beginning October 1, 2024.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
5.	Based on inquiry and record examination, has the Tribe or TGRA identified the types of events that the system is capable of logging in support of the audit function (e.g., authentication, file use, user/group management, events sufficient to establish what occurred, the sources of events, outcomes of events, and operational transactions)?	____	____	____	AU-2, a	
6.	Based on inquiry and record examination, has the Tribe or TGRA coordinated the event logging function with other organizational entities requiring audit- related information to guide and inform the selection criteria for events to be logged?	____	____	____	AU-2, b	
7.	Based on inquiry and record examination, has the Tribe or TGRA specified the following event types for logging within the system for all successful and unsuccessful:					
	• System log-on attempts?	____	____	____	AU-2, c.1	
	• Attempts to use:					
	o Access permission on a user account, file, directory, or other system resource?	____	____	____	AU-2, c.2.a	
	o Create permission on a user account, file, directory, or other system resource?	____	____	____	AU-2, c.2.b	
	o Write permission on a user account, file, directory, or other system resource?	____	____	____	AU-2, c.2.c	
	o Delete permission on a user account, file, directory, or other system resource?	____	____	____	AU-2, c.2.d	
	o Change permission on a user account, file, directory, or other system resource?	____	____	____	AU-2, c.2.e	
	• Attempts to change account passwords?	____	____	____	AU-2, c.3	
	• Actions by privileged accounts (i.e., root, Oracle, DBA, admin, etc.)?	____	____	____	AU-2, c.4	
	• Attempts for users to:					
	o Access the audit log file?	____	____	____	AU-2, c.5.a	
	o Modify the audit log file?	____	____	____	AU-2, c.5.b	
	o Destroy the audit log file?	____	____	____	AU-2, c.5.c	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
8.	Based on inquiry and record examination, has the Tribe or TGRA provided a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents?	____	____	____	AU-2, d	
9.	Based on inquiry and record examination, does the Tribe or TGRA review and update the event types selected for logging annually?	____	____	____	AU-2, e	
10.	Based on inquiry and record examination, does the Tribe or TGRA ensure that audit records contain information that establishes the following:					
	• What type of event occurred?	____	____	____	AU-3, a	
	• When the event occurred?	____	____	____	AU-3, b	
	• Where the event occurred?	____	____	____	AU-3, c	
	• Source of the event?	____	____	____	AU-3, d	
	• Outcome of the event?	____	____	____	AU-3, e	
	• Identity of any individuals, subjects, or objects/entities associated with the event?	____	____	____	AU-3, f	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
11.	Based on inquiry and record examination, does the Tribe or TGRA generate audit records containing the following additional information:					
	• Session, connection, transaction, and activity duration?	____	____	____	AU-3, (1) a	
	• Source and destination addresses?	____	____	____	AU-3, (1) b	
	• Object or filename involved?	____	____	____	AU-3, (1) c	
	• Number of bytes received and bytes sent (for client-server transactions) in the audit records for audit events identified by type, location, or subject?	____	____	____	AU-3, (1) d	
	• The Interstate Identification Index[2] (III) portion of the log shall clearly identify:					
	○ The operator (i.e., staff authorized to disseminate the CHRI response)?	____	____	____	AU-3, (1) e.1	
	○ The requestor (i.e., the applicant)?	____	____	____	AU-3, (1) e.3	
	○ The secondary recipient(i.e., the attorney representing the applicant, if applicable)?	____	____	____	AU-3, (1) e.4	
	NOTE: Please refer to the 2021 CHRI MOU, V.B.5(c)(i)(ii)(iii) for the corresponding requirements related to AU-3, (1) e.1, e.3 and e.4. These requirements are also identified at question #6 c. on the Sample Audit Checklist for the 2021 CHRI MOU.					
12.	Based on inquiry and record examination, does the Tribe or TGRA limit personally identifiable information (PII) contained in audit records to the following elements identified in the privacy risk assessment: Minimum PII necessary to achieve the purpose for which it is collected (see CJISSECPOL Section 4.3)?	____	____	____	AU-3, (3)	
13.	Based on inquiry and record examination, does the Tribe or TGRA allocate audit log storage capacity to accommodate the collection of audit logs to meet retention requirements?	____	____	____	AU-4	

[2] The III is an index pointer system that ties computerized criminal history record files of the FBI and the centralized files maintained by each III participating state into a national system.

Sample Audit Checklist for CJIS Security Policy (CJISSECPOL)

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
14.	Based on inquiry and record examination, does the Tribe or TGRA alert organizational personnel with audit and accountability responsibilities and system/network administrators within one (1) hour in the event of an audit logging process failure?	____	____	____	AU-5, a	
15.	Based on inquiry and record examination, does the Tribe or TGRA take the following additional actions: • Restart all audit logging processes and verify system(s) are logging properly?	____	____	____	AU-5, b	
16.	Based on inquiry and record examination, does the Tribe or TGRA review and analyze system audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity?	____	____	____	AU-6, a	
17.	Based on inquiry and record examination, does the Tribe or TGRA report findings to organizational personnel with audit review, analysis, and reporting responsibilities and organizational personnel with information security and privacy responsibilities?	____	____	____	AU-6, b	
18.	Based on inquiry and record examination, does the Tribe or TGRA adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information?	____	____	____	AU-6, c	
19.	Based on inquiry and record examination, does the Tribe or TGRA integrate audit record review, analysis, and reporting processes using automated mechanisms?	____	____	____	AU-6, (1)	
20.	Based on inquiry and record examination, does the Tribe or TGRA analyze and correlate audit records across different repositories to gain organization-wide situational awareness?	____	____	____	AU-6, (3)	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
21.	Based on inquiry and record examination, does the Tribe or TGRA provide and implement an audit record reduction and report generation capability that:					
	• Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents?	____	____	____	AU-7, a	
	• Does not alter the original content or time ordering of audit records?	____	____	____	AU-7, b	
22.	Based on inquiry and record examination, does the Tribe or TGRA provide and implement the capability to process, sort, and search audit records for events of interest based on the following content:					
	• Information included in AU-3[3]?	____	____	____	AU-7, (1)	
23.	Based on inquiry and record examination, does the Tribe or TGRA use internal system clocks to generate time stamps for audit records?	____	____	____	AU-8, a	
24.	Based on inquiry and record examination, does the Tribe or TGRA record time stamps for audit records that meet hundredths of a second (i.e., hh:mm:ss:00) interval and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp?	____	____	____	AU-8, b	
25.	Based on inquiry and record examination, does the Tribe or TGRA protect audit information and audit logging tools from unauthorized access, modification, and deletion?	____	____	____	AU-9, a	
26.	Based on inquiry and record examination, does the Tribe or TGRA alert organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators upon detection of unauthorized access, modification, or deletion of audit information?	____	____	____	AU-9, b	

[3] Please refer to questions #10-12 of this sample audit checklist.

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
27.	Based on inquiry and record examination, does the Tribe or TGRA authorize access to management of audit logging functionality to only organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators?	____	____	____	AU-9, (1)	
28.	Based on inquiry and record examination, does the Tribe or TGRA retain audit records for a minimum of one (1) year or until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements?	____	____	____	AU-11	
29.	Based on inquiry and record examination, does the Tribe or TGRA provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a[4] on all systems generating required audit logs?	____	____	____	AU-12, a	
30.	Based on inquiry and record examination, does the Tribe or TGRA allow organizational personnel with audit record generation responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators to select the event types that are to be logged by specific components of the system?	____	____	____	AU-12, b	
31.	Based on inquiry and record examination, does the Tribe or TGRA generate audit records for the event types defined in AU-2c[5] that include the audit record content defined in AU-3[6]?	____	____	____	AU-12, c	

[4] Please refer to question #5 of this sample audit checklist.

[5] Please refer to question #7 of this sample audit checklist.

[6] Please refer to questions #10-12 of this sample audit checklist.