Security Log Requirement Table

Security Profile	LOGGING PLATFORM	AVAILABILITY	RETENTION	ATTRIBUTES	ACTIVITIES
High Security Profile Applications where any of the following attributes are true: • UCAL • SOX • Applications that store, transfer or use Confidential Data • Internet Facing • Prioritized Critical Services (PCS) • Enterprise Critical Services (ECS) or Critical Core Infrastructure (CCI)	• Splunk • IAAS	• Available for correlation within 5 minutes. • Available within 15 minutes of GIS contacting the log owner.	• Logging Online Retention: 90 Days • Logging Offline Retention: 1 Year	At a minimum, the required security audit logging attributes must include: a. The identity of the account accessing the system, (e.g., Standard accounts, secondary accounts, external accounts and service accounts.) b. Date and local time zone (or UTC) c. System name generating the log. d. Log recording system name. e. Source IP address. f. Port where available g. Session ID	At a minimum, the required security audit logging activities must include: a. Login/logoff event. In the event of a logon failure, the reason must be specified (e.g., invalid username, invalid password, account locked, etc.). b. Downloading and revisions to confidential information c. Creation of, amendments, or changes to customer accounts and financial transactions d. All privileged user activities including both successful and unsuccessful attempts. e. Web access events in extended log format [as applicable]: a. Timestamp b. http method c. Uri d. uri query string e. http User-Agent header f. http Referer header g. The true IP of the client or http X-Forwarded-For header f. System errors relevant to security events, including but not limited to: SQL errors that indicate a SQL injection, fuzzing, multiple failed logins, failed configuration change, failed/disabled anti-virus software, service failures
Low Security Profile All other Application types	• Splunk • IAAS	• Available for correlation within 15 to 60 minutes. • Available within 60 minutes of GIS contacting the log owner.	• Logging Online Retention: 30 Days • Logging Offline Retention: 3 months		
*Third party and externally hosted applications are out of scope					

- Refer to the Global Records Management Retention Schedule for retention schedule requirements
- For additional privileged access activity examples, refer to IAM4206 and IAM Privileged Access Table
- For additional confidential data examples, refer to DAP2015 and Data Classification Table