Alert NIST Compliance List

			Controls
#	**Alert name**	**Alert Description**	**NIST**
1	Logon from External Devices	A new external device was recognized by the system. This alert is generated when a new external device, such as a USB, is connected to the system.	AC-19 -a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and b. Authorize the connection of mobile devices to organizational systems AC-20 - 1. Access the system from external systems; and 2. Process, store, or transmit organization-controlled information using external systems; or b. Prohibit the use of [Assignment: organizationally-defined types of external systems]
2	Windows Firewall Service failed	This alert will triggered when the Windows Firewall Service failed to start.	SR-9 TAMPER RESISTANCE AND DETECTION Anti-tamper technologies, tools, and techniques provide a level of protection for systems, system components, and services against many threats, including reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components during distribution and when in use.
3	Windows Firewall Driver failed	This alert will triggered Windows Firewall Driver failed to start.	SR-9 TAMPER RESISTANCE AND DETECTION Anti-tamper technologies, tools, and techniques provide a level of protection for systems, system components, and services against many threats, including reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components during distribution and when in use.
4	Windows Firewall Termination	The Windows Firewall Driver detected a critical runtime error (Terminating).	SR-9 TAMPER RESISTANCE AND DETECTION Anti-tamper technologies, tools, and techniques provide a level of protection for systems, system components, and services against many threats, including reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components during distribution and when in use.
5	Detected Replay Attack	This event indicates that a Kerberos replay attack was detected- a request was received twice with identical information. This condition could be caused by network misconfiguration.	IA-4 IDENTIFIER MANAGEMENT Identifier management also addresses individual identifiers not necessarily associated with system accounts. Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.

6	SMB Activity to the Internet	This rule detects network events that may indicate the use of SMB(Also known as Windows file sharing traffic to the Internet). SMB is commonly used within networks to share files, printers, and other system resources amongst trusted systems.	SC-4 INFORMATION IN SHARED SYSTEM RESOURCES Preventing unauthorized and unintended information transfer via shared system resources stops information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system.
7	User Remote Access Denied	A user was denied access to Remote Desktop. By default, users are allowed to connect only if they are members of the Remote Desktop Users group or Administrators group.	AC-17 - Remote Access a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize each type of remote access to the system prior to allowing such connections.
8	Remote User Disconnected	If a user disconnects from an existing Terminal Services session, or switches away from an existing desktop using Fast User Switching, event 4779 is generated. This event is also triggered when a user disconnects from a virtual host.	AC-17 - Remote Access a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize each type of remote access to the system prior to allowing such connections.

9	Active Directory Password Change	Alert makes Active Directory auditing very easy by tracking Password Status Changes for Users like password set or changed details with the help of pre-defined reports and instant alerts.	AC-2 ACCOUNT MANAGEMENT f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]; g. Monitor the use of accounts; h. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. [Assignment: organization-defined time period] when accounts are no longer required; 2. [Assignment: organization-defined time period] when users are terminated or transferred; and 3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. [Assignment: organization-defined attributes (as required)]; j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency]; k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
10	Detecting Installed Applications	Alert will notify you when an installation is successfully completed. It also shows the user account that performed the installation process.	Direct- CM-11, a. Establish organization-defined policies governing the installation of software by users; b. Enforce software installation policies c. Monitor policy compliance
11	Detecting Uninstalled Applications	Alert will notify you when an uninstallation is successfully completed. It also shows the user account that performed the uninstallation process.	Direct- CM-11, a. Establish organization-defined policies governing the installation of software by users; b. Enforce software installation policies c. Monitor policy compliance
12	Critical Environment Error	This alert will trigger if any critical environmental error happened in an organization.	SI-4 SYSTEM MONITORING a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the organziation's monitoring objectives: and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through the following techniques and methods: c. Invoke internal monitoring capabilities or deploy monitoring devices: 1. Strategically within the system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Analyze detected events and anomalies; e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals,

			other organizations, or the Nation; f. Obtain legal opinion regarding system monitoring activities; and
13	Encrypted Policy Change	This computer's Security Settings\Public Key Policies\Encrypting File System data recovery agent policy was modified - either via Local Security Policy or Group Policy in Active Directory.	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on
14	System Audit Policy Change	This computer's system level audit policy was modified - either via Local Security Policy, Group Policy in Active Directory or the audipol command. According to Microsoft, this event is always logged when an audit policy is disabled, regardless of the "Audit Policy Change" sub-category setting. This and several other events can help identify when someone attempts to disable auditing to cover their tracks.	AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES a. Alert in the event of an audit logging process failure;
15	Audit Log was Cleared	The alert will trigger if the audit log was cleared.	AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES a. Alert in the event of an audit logging process failure;
16	Active Directory Password Reset	The alert attempt was made to reset an accounts password.	AC-2 ACCOUNT MANAGEMENT f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]; g. Monitor the use of accounts; h. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. [Assignment: organization-defined time period] when accounts are no longer required; 2. [Assignment: organization-defined time period] when users are terminated or transferred; and 3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. [Assignment: organization-defined attributes (as required)]; j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency]; k. Establish and implement a process for changing shared or group

			account authenticators (if deployed) when individuals are removed from the group; and
17	Modified User Accounts	The user identified by Subject: changed the user identified by Target Account. Attributes show some of the properties that were set at the time the account was changed. This event is logged both for local SAM accounts and domain accounts.	AC-2 ACCOUNT MANAGEMENT Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require for group and role membership; d. Specify: 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account; e. Require approvals by for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with g. Monitor the use of accounts; h. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. when accounts are no longer required; 2. when users are terminated or transferred; and 3. when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and j. Review accounts for compliance with account management requirements k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and l. Align account management processes with personnel termination and transfer processes.
18	Device Disabled by the User	This event is generated when a user successfully disables a device.	CM-6 CONFIGURATION SETTINGS a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration settings; c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.
19	SID History Added	This event generates when SID History was added to an account.	AU-2 - EVENT LOGGING a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations

			of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].
20	SID History Added Failed	This event generates when an attempt to add SID History to an account failed.	AU-2 - EVENT LOGGING a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].
21	Kerberos Policy Changes	This alert detects a change to the the domain's Kerberos policy. Kerberos policy is defined in GPOs linked to the root of the domain under Computer Configuration\Windows Settings\Security Settings\Account Policy\Kerberos Policy.	AU-2 EVENT LOGGING a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].
22	Detected Incomming Messages	RPC detected an integrity violation while decrypting an incoming message.	AU-2 EVENT LOGGING a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].
23	Request Enabled Device	A request was made to enable a device. This alert is generated if a user attempts to	CM-6 CONFIGURATION SETTINGS a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment:

		enable a device on the system. This does not mean that a device was successfully enabled.	organization-defined common secure configurations]; b. Implement the configuration settings; c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.
24	Sysmon Error	This alert is generated when an error occurred within Sysmon. They can happen if the system is under heavy load and certain tasked could not be performed or a bug exists in the Sysmon service.	SI-4 SYSTEM MONITORING a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods]; c. Invoke internal monitoring capabilities or deploy monitoring devices: 1. Strategically within the system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Analyze detected events and anomalies; e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation; f. Obtain legal opinion regarding system monitoring activities; and
25	Domain Policy Change	This alert is generated when an Active Directory Domain Policy is modified. It is logged on domain controllers and member computers.	AU-2 EVENT LOGGING a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].
26	Restore Administrator Password	An attempt was made to set the Directory Services Restore Mode administrator password. This alert is generated when DSRM administrator password is changed. It is logged only on domain controllers	IA-5 AUTHENTICATOR MANAGEMENT Manage system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; b. Establishing initial authenticator content for any authenticators issued by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators; e. Changing default authenticators prior to first use;

			f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur; g. Protecting authenticator content from unauthorized disclosure and modification; h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and i. Changing authenticators for group or role accounts when membership to those accounts changes.
27	Active Directory Privilege Operation	An operation was attempted on a privileged object.	AU-2 EVENT LOGGING a. Identify the types of events that the system is capable of logging in support of the audit function: b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging
28	Active Directory Services Access	A handle to an object was requested.	CM-5 ACCESS RESTRICTIONS FOR CHANGE Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.
29	Alert-Data Loss Prevention Rule	This Alert is generated when there is event associated with data loss	SC-7 BOUNDARY PROTECTION a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.
30	Error Logging Service	The event logging service encountered an error. This alert is generated when the event logging service encounters an error while processing an incoming event.	AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES a. Alert in the event of an audit logging process failure; and
31	User Privilege Assigned	This Alert is generated when a user privilege is assigned	AC-24 ACCESS CONTROL DECISIONS Establish procedures; Implement mechanisms] to ensureare applied to each access request prior to access enforcement.
32	User Privilege Removed	This Alert is generated when a user privilege is removed	AC-24 ACCESS CONTROL DECISIONS Establish procedures; Implement mechanisms] to ensureare applied to each access request prior to access enforcement.
33	User Account Unlocked	This Alert is generated when a user account is unlocked	AC-24 ACCESS CONTROL DECISIONS Establish procedures; Implement mechanisms] to ensureare applied to each access request prior to access enforcement.

34	Attempt to Disable Syslog Service	This Alert is generated when there is attempt to disable sys;og service	IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION Uniquely identify and authenticate] before establishing communications with devices, users, or other services or applications.
35	Attempt to Enable the Root Account	This Alert is generated when there is attempt to enable the root account	AC-2 ACCOUNT MANAGEMENT a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) Require approvals by for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with g. Monitor the use of accounts; h. Notify account managers when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and j. Review accounts for compliance with account management requirements; k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and l. Align account management processes with personnel termination and transfer processes.
36	Blocked File Import/Expor t Attempt	This Alert is generated when there is attempt to import or export a blocked file	SC-7 BOUNDARY PROTECTION . Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.
37	Failed File System Access (Linux)	This alert is generated when permission to access the file system is denied.	AC-3 ACCESS ENFORCEMENT Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
38	System File Permission Change (Linux)	This alert is generated when the system file permissions (Read, Write, Execute) are changed.	AU-2 EVENT LOGGING a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations

			of incidents; and e. Review and update the event types selected for logging
39	System File Permission Change (Windows)	Permissions on an object were changed. This alert is generated when someone changes the access control list on an object. The event identifies the object, who changed the permissions and the old an new permissions.	AU-2 EVENT LOGGING a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging