Alert PCI DSS Compliance List

			Controls
#	Alert name	Alert Description	PCI - DSS
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.	2.2.4 Only necessary services, protocols, daemons,and functions are enabled, and all unnecessary functionality is removed or disabled. 3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need. 5.3.3 For removable electronic media, the antimalware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted, OR • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.
2	Windows Firewall Service failed	This alert will triggered when the Windows Firewall Service failed to start.	10.7.1 and 10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).
3	Windows Firewall Driver failed	This alert will triggered Windows Firewall Driver failed to start.	10.7.1 and 10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).
4	Windows Firewall Termination	The Windows Firewall Driver detected a critical runtime error (Terminating).	10.7.1 and 10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls.

			• Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).
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.	8.5.1 MFA systems are implemented as follows: • The MFA system is not susceptible to replay attacks.
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.	2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.
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.	7.2.5 All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.
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.	7.2.5 All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.
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	8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows:

		the help of pre-defined reports and instant alerts.	
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.	6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.
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.	6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.
12	Critical Environment Error	This alert will trigger if any critical environmental error happened in an organization.	Requirement 10: Log and Monitor All Access to System Components and Cardholder Data 10.7.1 - Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).
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.	3.5.1.3 If disk-level or partition-level encryption is used (rather than file-, column-, or field—level database encryption) to render PAN unreadable, it is managed as follows: • Logical access is managed separately and independently of native operating system authentication and access control mechanisms. • Decryption keys are not associated with user accounts. • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely
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,	10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events

		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.	
15	Audit Log was Cleared	The alert will trigger if the audit log was cleared.	10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events
16	Active Directory Password Reset	The alert attempt was made to reset an accounts password.	8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows:
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.	7.2.4 All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months. • To ensure user accounts and access remain appropriate based on job function. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.
18	Device Disabled by the User	This event is generated when a user successfully disables a device.	10.2 Implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of and changes to identification and authentication mechanisms (including creation of new accounts, elevation of privileges), and all changes, additions, deletions to accounts with root or administrative privileges; initialization, stopping or pausing of the audit logs; creation and deletion of system-level objects 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Perform critical log reviews at least daily.
19	SID History Added	This event generates when SID History was added to an account.	10.2.1 - Audit logs are enabled and active for all system components and cardholder data.
20	SID History Added Failed	This event generates when an attempt to add SID History to an account failed.	10.2.1 - Audit logs are enabled and active for all system components and cardholder data.

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.	11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.
22	Detected Incomming Messages	RPC detected an integrity violation while decrypting an incoming message.	11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.
23	Request Enabled Device	A request was made to enable a device. This alert is generated if a user attempts to enable a device on the system. This does not mean that a device was successfully enabled.	10.2 Implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of and changes to identification and authentication mechanisms (including creation of new accounts, elevation of privileges), and all changes, additions, deletions to accounts with root or administrative privileges; initialization, stopping or pausing of the audit logs; creation and deletion of system-level objects 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Perform critical log reviews at least daily.
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.	10.2.1.7 Audit logs capture all creation and deletion of system-level objects.
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.	11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.
26	Restore Administrator Password	An attempt was made to set the Directory Services Restore Mode administrator	8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows: • Passwords/passphrases are changed periodically and upon suspicion or confirmation of compromise.

		password. This alert is generated when DSRM administrator password is changed. It is logged only on domain controllers	• Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases.
27	Active Directory Privilege Operation	An operation was attempted on a privileged object.	A3.4.1 User accounts and access privileges to inscope system components are reviewed at least once every six months to ensure user accounts and access privileges remain appropriate based on job function, and that all access is authorized.
28	Active Directory Services Access	A handle to an object was requested.	7.2 Access to system components and data is appropriately defined and assigned.
29	Alert-Data Loss Prevention Rule	This Alert is generated when there is event associated with data loss	A3.2.6.1 Response procedures are implemented to be initiated upon the detection of attempts to remove cleartext PAN from the CDE via an unauthorized channel, method, or process. Response procedures include: • Procedures for the prompt investigation of alerts by responsible personnel. • Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss.
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.	10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.
31	User Privilege Assigned	This Alert is generated when a user privilege is assigned	7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood. 7.2 Access to system components and data is appropriately defined and assigned. 7.3 Access to system components and data is managed via an access control system(s)
32	User Privilege Removed	This Alert is generated when a user privilege is removed	7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood. 7.2 Access to system components and data is appropriately defined and assigned. 7.3 Access to system components and data is managed via an access control system(s)
33	User Account Unlocked	This Alert is generated when a user account is unlocked	7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood. 7.2 Access to system components and data is appropriately defined and assigned.

			7.3 Access to system components and data is managed via an access control system(s)
34	Attempt to Disable Syslog Service	This Alert is generated when there is attempt to disable sys;og service	10.2.1.6 Audit logs capture the following: • All initialization of new audit logs, and • All starting, stopping, or pausing of the existing audit logs
35	Attempt to Enable the Root Account	This Alert is generated when there is attempt to enable the root account	8.2.2 Group, shared, or generic accounts, or other shared uthentication credentials are only used when necessary on an exception basis, and are managed as follows: • Account use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user.
36	Blocked File Import/Export Attempt	This Alert is generated when there is attempt to import or export a blocked file	1.2.4 An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks.
37	Failed File System Access (Linux)	This alert is generated when permission to access the file system is denied.	10.2.1 Audit logs are enabled and active for all system components and cardholder data.
38	System File Permission Change (Linux)	This alert is generated when the system file permissions (Read, Write, Execute) are changed.	11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.
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.	11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.