AdminDroid

PCI-DSS Compliance

with

AdminDroid

AdminDroid

PCI-DSS Compliance
with AdminDroid

The **Payment Card Industry Data Security Standard** is a compendium of recommendations created to enhance the security of cardholder data and prevent misuse. Containing 12 sections and more than 200 controls, it addresses various aspects of data security. Compliance to the Standard involves the adoption of the recommendations by the firm handling the Cardholder data. **PCI-DSS** applies to any firm that stores, processes or sends sensitive cardholder data. Hence all merchants, acquirers, issuers, card brands, payment processors, payment gateways and service providers are subject to the regulation.

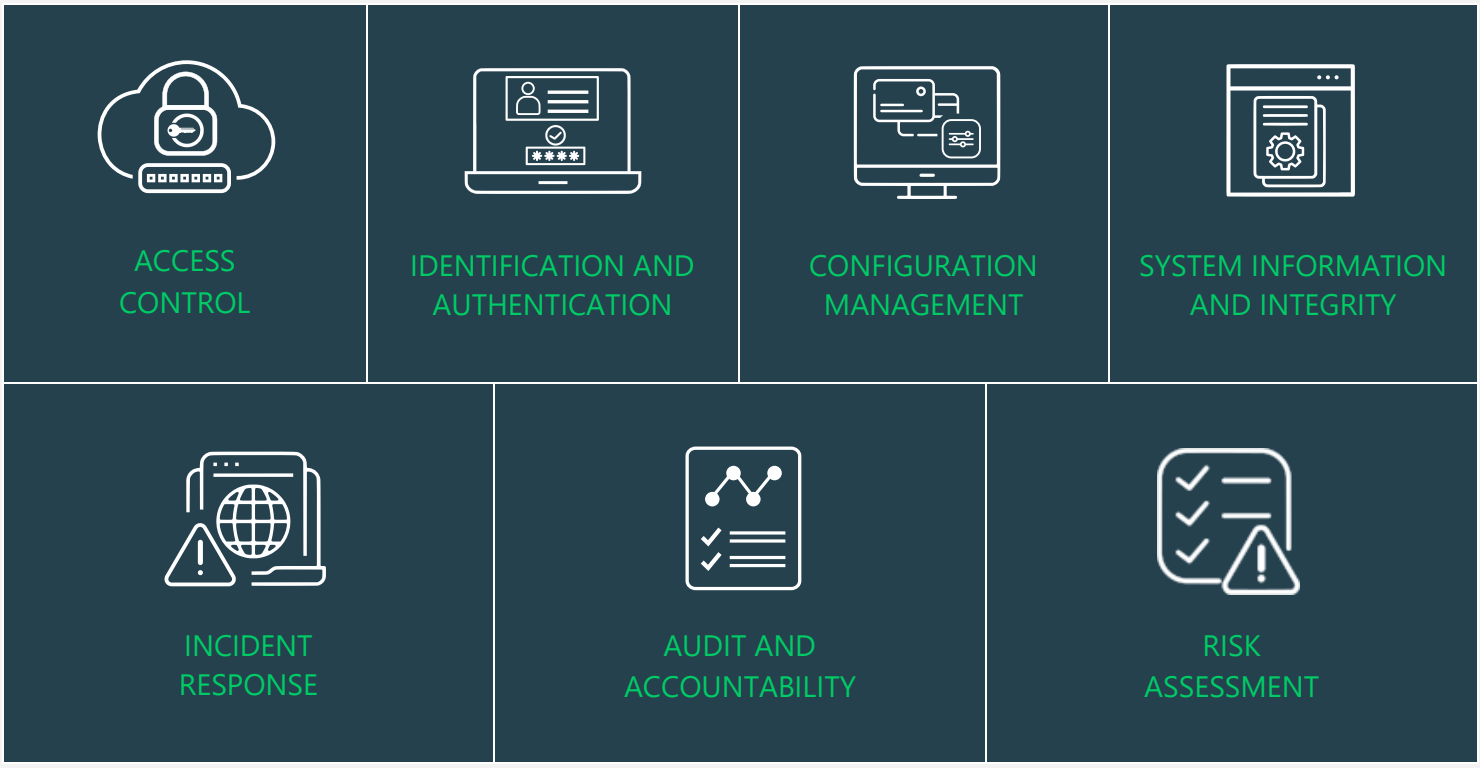
Non-Compliance may result in loss of reputation and customer base. In case of a breach, it may also draw fines.
PCI-DSS is developed, managed and continuously updated by the **Payment Card Industry Security Standards Council**.

It is an open forum founded by the five major international card brands- MasterCard, Visa Inc., American Express, Discovery Financial Services and JCB International.

CONTROL GROUPS

The whole process of IT Compliance to various regulations involves an organization developing and implementing controls that address the various facets of Information Technology. We have identified controls that **AdminDroid** can help with in implementation and grouped those controls under **Control Groups,** listed below, for management simplicity. Please note that the list of controls is not exhaustive and cannot guarantee full compliance with any regulation.

- Access Control
- Identification and Authentication
- Configuration Management
- System and Information Integrity
- Incident Response
- Audit and Accountability
- Risk Assessment



MAPPING OF PCI-DSS COMPLIANCE CONTROL GROUPS AND REPORTS

Fulfilling various compliance demands for Microsoft 365 is challenging, as the person should be proficient in both the compliance requirements and Microsoft 365. Also, it makes it more difficult as the person should have a clear understanding of all Microsoft 365 services with knowledge of how to pull various reports. No matter if you are an expert in one of them, we have composed two mappings for fulfilling your compliance needs. You can choose any of the below paths based on your expertise.

- **Mapping of Control Groups to Report Collections**

(If you are well known about compliance control and requirements, you can make use of this mapping.)

- **Mapping of AdminDroid Report Categories to Control Groups**

(If you are well known about Microsoft 365 services and report profiles, you can make use of this mapping.)

- **Pre-compiled Report Bundle for PCI-DSS Compliance**

(AdminDroid offers PCI-DSS ReportBoard which contains a collection of compliance reports compiled based on all compliance requirements. It allows bulk download, email, and scheduling and provides easy access to the reports.)

MAPPING OF PCI-DSS PROVISIONS TO CONTROL FAMILIES

In the following table, key provisions of PCI-DSS have been mapped to Control Families

PCI-DSS Requirement	Control Containers
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs	
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	**Access Control** • Least Privilege
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	• Anti-Malware • Anti-Phishing
Requirement 6: Develop and maintain secure systems and applications	
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.	**System and Information Integrity** **1.Security Alerts, Advisories and Directives** **2.Secure Score reports** • Overall Score trend • Control settings scores daily trend • Control settings recent scores • Zero scores
6.4.5.2 Documented change approval by authorized parties.	Monitoring the service used to store your documents is sufficient. Considering Microsoft 365, you are required to audit the SharePoint sites. • SharePoint file modifications • OneDrive file modifications • OneNote section modification • Admins added • Site collection admin change request

6.5.6 All “high risk” vulnerabilities identified in the vulnerability identification process.	**Incident Response** • Information Spillage Response
6.5.10 Broken authentication and session management	• CA policies with grant access • CA policies with Session control
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	• All CA policy • Sign-in risk policy • User risk policy
Requirement 7: Restrict access to cardholder data by business need to know	
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	**Access Control** • Least Privilege
7.2 Establish an access control system(s) for systems components that restricts access based on a user’s need to know and is set to “deny all” unless specifically allowed.	**Access Control** • Least Privilege
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	• CA policy with restricted access
Requirement 8: Identify and authenticate access to system components	
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	**Identification and Authentication** • Identification and Authentication (Organizational Users) • Device Identification and Authentication
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	**Access Control** 1. Account Management Audit • Account Details Monitoring **Identification and Authentication** • Identifier Management

8.1.3 Immediately revoke access for any terminated users.	**Access Control** Account Details Monitoring • Deleted Users • Sign-In disabled Users
8.1.4 Remove/disable inactive user accounts within 90 days.	**Access Control** Account Management Audit • Inactive Users
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access.	**Identification and Authentication** Identification and Authentication (Organizational Users) • External Users • Guest Users
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	**Incident Response** • Incident Monitoring
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	• Session Control in CA policy
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	• Session Control in CA policy
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys. **8.2.3** Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above.	**Identification and Authentication** Authenticator Management • Self-service Password resets • Password Reset by admin • Reset forced by admins • Users with Weak Password allowed

8.2.4 Change user passwords/passphrases at least once every 90 days.	**Identification and Authentication** Authenticator Management
8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user and change immediately after the first use.	**Identification and Authentication** Authenticator Management • Password Reports
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator and including third-party access for support or maintenance) originating from outside the entity's network.	MFA Reports • Users with MFA • Users without MFA • Admins with MFA • Admins without MFA
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.	• Generic events in risky sign-ins
Requirement 10: Track and monitor all access to network resources and cardholder data	
10.1 Implement audit trails to link all access to system components to each individual user.	1. Ensure that unified audit log is enabled. For reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/turn-audit-log-search-on-or-off?view=o365-worldwide 2. Ensure mailbox audit log is enable • Audit Settings
10.2.2 All actions taken by any individual with root or administrative privileges.	**Access Control** 1. Account Usage Monitoring • All admin activities
10.2.3 Access to all audit trails.	**Audit and Accountability**

10.2.4 Invalid logical access attempts.	**Incident Response** • Incident Monitoring
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges and all changes, additions, or deletions to accounts with root or administrative privileges.	**Access Control** • Account Management Audit • Least Privilege
10.2.6 Initialization, stopping, or pausing of the audit logs.	• Audit Enabled and Disabled mailboxes
10.2.7 Creation and deletion of system-level objects.	• User Creation and Deletion • Groups • Files creation and deletion
10.3 Record at least the following audit trail entries for all system components for each event: **10.3.1** User identification **10.3.2** Type of event **10.3.3** Date and time **10.3.4** Success or failure indication **10.3.5** Origination of event **10.3.6** Identity or name of affected data, system component, or resource	Microsoft 365 audit trail provides all your required details for all the reports. You can refer a report attached below for better understanding. **Access Control** Account Usage Monitoring • All activities
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.	**Incident Response** Incident Monitoring • Anonymous IP address • Unlikely travel • Malicious IP address • Unfamiliar features • Malware infected IP address • Suspicious IP address • Leaked credentials • Investigations Threat Intelligence • Generic events • Generic admin confirmed user compromised • Password spray • Mcas impossible travel • Mcas suspicious inbox manipulation rules • Investigations threat intelligence sign in • Malicious IP address valid credentials blocked IP • Admin confirmed User compromised

Requirement 11: Regularly test security systems and processes.	
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	**Audit and Accountability** • Audit Review, Analysis, and Reporting • Report Generation and Audit Reduction
Requirement 12: Maintain a policy that addresses information security for all Personnel.	
12.1.1 Review the security policy at least annually and update the policy when the environment changes.	• All CA policy

MAPPING OF CONTROL GROUPS TO REPORT COLLECTIONS

The below mapping will help you to find out the various PCI-DSS compliance controls, and how to implement them in Microsoft 365 services using respective M365 reports for achieving your compliance requirements.

ACCESS CONTROL

Access Control measures ensure that information system accounts are handled properly and that access to accounts is granted based on organizational roles. The **AdminDroid Reporter** tool provides insight into such activity to support the formulation and maintenance of Access Control policies and controls

Control	Microsoft 365 Centric Control Implementation	Applicable AdminDroid Reports
1. Account Management Audit Audit the creation, deletion, enabling, disabling and modification of User Accounts.	**Account Types Monitoring** Identify and review all the different types of accounts in your Microsoft 365 Environment to identify accounts that do not support your business functions.	**User Reports** • All users • All External Users • Internal Guest Users **Group Reports** • All Groups • Groups Created via Teams • Groups Created via Yammer • Groups Created via SharePoint • Empty Groups • Groups with Hidden membership

	Account Details Monitoring Monitor and review the details of and changes made to user accounts in your Microsoft 365 Environment to spot deviations from your Account Management Policies and Procedures.	**User details Reports** • Created Users • Deleted users • All User Events • Enabled Users • Disabled Users **User account Changes Reports** • Updated Users • License Changes • Recent password Changes **User Managers Reports** • Managers & Direct Reports • Users with Managers • Users without Managers
	Account Usage Monitoring Review user activity across all Microsoft 365 services.	**Overall Activities** • All Activities • Admin Activities • Top Activity Summary • Daily Activity Summary • Activity by Department • Activity by City • Activity by State • Activity by Country • Activity by JobTitle • Activity by Company **Sharing & Access** • All file/folder sharing activity • All file/folder access activity • Files shared by External users • Files shared to External users • File/Folder accesses by External Users • File Deletion • Anonymous link creation • Anonymous link accessed • Files shared via Teams Channels • Files shared by External Users in Channels • Files shared via 1:1 chat • Files shared to External Users 1:1 chat

		OneDrive User Activities • Daily User Activities • User Activities • Active Users **Teams User Activities** • Daily Activities • Overall Activities **Yammer User Activities** • Daily Activities • Overall Activities **Skype User Activities** • Peer-to-Peer Sessions • Organized Conferences • Participated Conferences • File Transfers • Instant Messages **SharePoint Activities** • Daily Active users • Users File Access Summary • Users File Synced Summary • Users Internal File Sharing Summary • Users External File Sharing Summary • Users Page Visit Summary • Daily Summary of Users by Activity **Resource Usage by User Accounts** • Mailbox size over time • Daily mailbox quota status • Shared mailbox size over time • Archived mailbox over warning quota • Daily Site Storage • OneDrive Overall Storage **License & Subscription Usage** • Daily Activities • Subscription Usage • Unused Subscriptions • Licensed Users • Regain Licenses

	Inactive Users Identify inactive user accounts across all Microsoft 365 services to take decisions on termination of license or access.	**Exchange Inactive Users** • By Last Mail Read • By Last Mail Sent • By Last Mail Received **SharePoint Inactive Users** • By Last File Access • By Last File Synced • By Last External Share • By Last Internal Share • By Last Page Access **OneDrive Inactive Users** • By Last File Accessed • By Last Internal Share • By Last External Share • By Last File Synced **Teams Inactive Users** • By Last Team Chat • By Last Private Chat • By Last Call Activity • By Last Meeting Activity **Yammer Inactive Users** • By Last Post Liked • By Last Post Posted • By Last Post Read • By Last Activity **Active Users Statistics** • Last Active Time • Daily Active Users • Exchange Last Active Time • SharePoint Last Active Time • OneDrive Last Active Time • Teams Last Active Time • Yammer Last Active Time

2. Least Privilege Maintain the principle of least privilege while assigning access permissions and privileged roles.	Review administrative access privileges and license assignments made to your Microsoft 365 users and continuously monitor for related changes to ensure that the principle of least privilege is met.	**User License Reports** • Licensed Users • Users by Subscriptions • Unlicensed Users • Free Users • Trial Users **Admin Reports** • All Admins • Admin roles by user • User Added as Admins *(25 Reports)* • All Global Admins • Admins with Management Roles • Admins with Read Access Roles **Admin Role Changes** • Role Assignments • Role Scope Changes • Added Roles • Updated Roles **Role Configuration Changes** • Management Role • Role Assignments • Assignments Policy • Role Entry • Role Group • Role Scope **Mailbox Permissions** • Access to Others Mailboxes • Mailbox Permission Summary • Mailbox Permission Detail • Mailbox with SendOnBehalf • Send As Permission • Full Permission • Read Permission • Guests' Mailbox Permission Summary • Admins Access to Others Mailboxes • Admins with Send-on-Behalf • Admins with Send-As • Admins with Full Access • Guests Access to Others Mailboxes **Mailbox Access** • Mailbox Non-Owner Access

3. Unsuccessful Logon Attempts Monitor unsuccessful attempts to logon to your information system accounts.	Monitor for and review failed logon attempts to accounts in your Microsoft 365 Environment to take further action.	**User Failed Logins** • Failed User Logins • Users' Login Failure Summary • Failed Sign-ins • Failed logins in MFA challenge **Teams** • Login Activities **Admins Failed Logins** • Admins' Login Failure • Admins' Login Failure Summary
4. Previous Logon (Access) Notification Audit the Previous logon time of the Microsoft 365 users.	Track the last logon time of the users to identify the location, IP address, and more for security requirements.	**Last Logon Report** • Users' Last Logon Time • Users' last logon summary by users • Users' last logon summary by application • Users' last logon summary by city • Users' last logon summary by state • Users' last logon summary by country • Users' last logon summary by browser • Users' last logon summary by operating system
5. Access Control for Mobile Devices Authorize and audit the mobile devices connected to your organization's information system.	Identify and review the mobile devices used by your users to access key Microsoft 365 services to ensure that no unauthorized devices are used.	**Mobile Device Reports** • All Mobile Devices • Devices by Connected Mailbox • Mobile Devices by OS • Mobile Devices by Policy • Mobile Devices by Client Type • Mobile Devices by Access Type **Mobile Device Configuration Changes** • Mobile Device Configs • Active Sync Configs • Text Message Settings

6. Information Sharing Audit Audit the information sharing activities to permit only the authorized users to share and access the information.	Supervise the sharing & access data to secure the sensitive info from the unauthorized users and for post breach investigation.	**Sharing & Access Activities** • All File/Folder Sharing Activities • All File/Folder Access Activities • Files shared by External Users • Files shared to External Users • File/Folder Accesses by External Users • Anonymous link Accessed • Anonymous link Creation • Files Shared via Teams Channels • Files shared by External Users in Channels • Files shared via 1:1 chat • Files shared to External users 1:1 chat **SharePoint Access Requests Reports** • Requests Created • Requests Accepted • Requests Denied • All Events **SharePoint Sharing Invitations Reports** • Invites Created • Invites Accepted • Invites Revoked • All Events • External User Invites

IDENTIFICATION AND AUTHENTICATION

Identification and Authentication controls are set up to ensure that all users and devices are identifiable and appropriate authentication systems are in place to restrict access to sensitive data. The **AdminDroid** Reporter tool can be used to monitor and provide data to ensure the maintenance of the controls.

Control	Microsoft 365 Centric Control Implementation	Applicable AdminDroid Reports
1. Identification and Authentication (Organizational users) Audit and review the identification and authentication processes for users.	Review user account data in Azure Active Directory to check whether: **a**. All people listed in your organization who possess a valid business reason to access your Microsoft 365 Environment are assigned an account, and	Office 365 users
	b. To identify user accounts which cannot be tracked to an individual. Review the authentication requirements imposed on users to verify that all accounts of the users are protected in line with your organization's policy.	**MFA Reports** • Users with MFA • MFA Activated Users • Users' MFA details **MFA Configured Policies Analytics** • Policies with MFA • MFA Policies Assignment Overview • MFA Policies Assignment Details **CA Policy Assignment Details analytics** • Password policies Reports • Policies with User Assignments • User conditions on Access Policies • Guest/External user conditions on Access Policies **Password Reports** • Password expired users • Soon to Password expire users • Password never expire users • Users with Password expiry • Password never changed • Password not changed in 90 days • Recent password changers • Users with weak password allowed

2. Device Identification and Authentication Review and audit the identification processes for devices in information system.	Review device additions, modifications, deletions, and other such activity to spot any unauthorized changes.	**Mobile Devices** • All Mobile Devices • Devices by Connected Mailbox • Mobile Devices by OS • Mobile Devices by Client type • Mobile Devices by Access State **Device Audit** • Added Devices • Updated Devices • Deleted Devices • Owner changes • User changes • Credential changes • All Device Operations • Sign-ins with Device details • Mobile Sign-ins • Non-compliant Device sign-ins • Unmanaged Device sign-ins
3. Identifier Management Audit the provisioning, modification and deprovisioning of users and groups.	Review the creation, deletion and modification of users and groups in your Microsoft 365 Environment to ensure that unauthorized activity does not take place and that identifiers that do not comply with your organization's policy are not used.	**User Audit** • Created Users • Updated Users • License Changes • Deleted Users **Group Audit** • Created Groups • Deleted Groups • Updated Groups • Group Member Changes **Mailbox Info** • All Mailboxes • Shared Mailboxes • Archived Mailboxes
4. Authenticator Management Audit the changes to authenticators by users and administrators for policy compliance and review changes to authentication policies.	Audit the changes to passwords effected by users and administrators to spot any unauthorized or inappropriate modifications.	**Password Reports** • Password never expire users • Password never changed • Recent Password changers • Password not changed in 90 days • Users with weak password allowed **Password Changes** • User Password Changes • Password Reset by Admin • Forced/Expired Password resets • Reset Forced by Admin • All Password Changes

5. Re-Authentication Monitor logins to your information system to identify cases such as password expiry that need action.	Monitor failed login attempts to your Microsoft 365 Environment to look out for issues that need administrative help.	**User Logins** • Failed User Logins • Failed Sign-ins • Failed in MFA challenge

AUDIT AND ACCOUNTABILITY

Audit and Accountability measures are necessary to maintain a record of all activities of an employee or process so that when a problem surfaces, he or she can be held accountable. The **AdminDroid Reporter** Tool offers a holistic view of all the happenings in your Microsoft 365 Environment through reports that are easy to understand and handle. Kindly note that **AdminDroid** does not store any audit data.

Control	Microsoft 365 Centric Control Implementation	Applicable AdminDroid Reports
1. Audit Events Generate audit records containing information that establishes what type of event occurred, when and where it occurred, the source and outcome of the event and the identity of the individuals associated with the event.	Collect information that answers the What, who, when and where questions about events across all services in your Microsoft 365 Environment.	**Office 365 Workload Based Activities** • Azure AD Activities • Exchange Activities • SharePoint Activities • OneDrive Activities • OneNote Activities • Power BI Activities • Teams Activities • Stream Activities • Security & Compliance • Compliance Search Activities
2. Audit Review, Analysis and Reporting Regularly review the audit records to spot any unusual or inappropriate activity and report the findings to the assigned or appropriate personnel in your organization.	Review your audit trail across all services of your Microsoft 365 Environment.	**Office 365 Workload Based Activities** • Azure AD Activities • Exchange Activities • SharePoint Activities • OneDrive Activities • OneNote Activities • Power BI Activities • Teams Activities • Stream Activities • Security & Compliance • Compliance Search Activities

		Audit Settings • Audit Enabled • Audit Disabled • Admin Audit Enabled • Owner audit Enabled • Delegate audit Enabled
	Export the audit trail in a format of your choice for reporting inappropriate activity to the designated personnel.	Export the audit report in a range of formats including PDF and Microsoft Excel using the Export Feature.
3. Report Generation and Audit Reduction Provide summary reports to support on demand audit review, analysis and reporting requirements and investigation requirements without altering the audit log.	Review detailed visualizations of audit trail data to easily spot anomalous behaviour without having to go through the raw audit information.	• Dashboard.Audit • Dashboard.AzureAD • Dashboard.Security • Dashboard.Exchange • Dashboard.UsageandAdoption
4. Non-Repudiation Monitor and record user activity in your information system to counter claims of repudiation.	Configure alerts on suspicious user activity in your Microsoft 365 Environment to ensure non-repudiation.	**All User Summary** • All user summary by activity

5. Cross-organizational Auditing Audit the activity of extra- or cross-organizational users and processes in your Microsoft 365 Environment.	Audit the activity of external users across Microsoft 365 services to look out for any suspicious events.	**Overall External user summary** • External User summary by activity • External User summary by activity type • External User summary by alert policy name • External User summary by security • External User summary by category • External User summary by policy type • External User summary system alerts

SYSTEM AND INFORMATION INTEGRITY

System and Information Integrity measures are setup to protect information systems and data in case of a breach or attack by outsiders or insiders. The **AdminDroid Reporter** tool provides detailed reports on user activity to help in your breach investigation.

Control	Microsoft 365 Centric Control Implementation	Applicable AdminDroid Reports
1. Flaw Remediation Identify, report, and correct the flaws in software and firmware for the organizations' Security.	Monitor the added or updated applications in your organization to test and remediate the flaws.	**Application Audit** • Added Applications • Updated Applications
2. Software, Firmware, and Information Integrity Employ integrity verification schemes to detect unauthorized changes to your information system.	Review the secure score of Microsoft 365 services to understand the security and integrity status of your Microsoft 365 Environment.	**Overall (Secure score)** **AdminDroid** offers more detailed Secure Score Reports for each Microsoft 365 service. • Control Settings Scores Daily Trend • Control Settings Recent Scores • Zero Score • Full Score • All Tenants Score Trend • Tenant Seats Score Trend • Industry Type Score Trend

3. Information System Monitoring Monitor your information system to detect indicators of potential attacks and unauthorized activity.	Review audit data in your Microsoft 365 Environment across services with a focus on the risk laden areas to detect any anomalies.	**All Low-Level Reports** (The Advanced Search Tool helps you in zeroing in on the exact report you need) **Overall Activities** • Admin Activities • All Failed Activities • All Activities **Office 365 Workload Based Activities** • Azure AD Activities • Exchange Activities • SharePoint Activities • OneDrive Activities • OneNote Activities • Power BI Activities • Teams Activities • Stream Activities • Security and Compliance • Compliance Search Activities
4. Security Alerts, Advisories and Directives Receive, generate, and disseminate alerts and advisories on your information system whenever deemed necessary.	Configure alerts and review them based on their severity in your Microsoft 365 Environment whenever and wherever they come up.	**Alert Severity** • High severity • Medium severity • Low Severity **Alert Category** • Data Loss Prevention • Threat Management • Information Governance • Permissions • Mail Flow • Others
5. Security Function Verification Verify the security operation of your information system and notify whenever any security verification test failure takes place.	Monitor for and review security verification failures such as failed login attempts in your Microsoft 365 Environment.	**User Logins** • Failed User Logins • Users' Login Failure Summary **MFA Reports** • MFA Non-Activated Users • Failed Sign-ins • Failed in MFA challenge • MFA Disabled

6. Spam Protection Employ and regularly update spam protection features in your information system.	Monitor and regularly review the quantity and content of spam mail received by your Microsoft 365 Environment.	**Advanced Threat Protection** • Anti-Spam • Spam Mails Received • Spam Mails Sent/Received
7. Memory Protection Identify any malware or phishing attacks in your organization to protect the memory locations.	Track and review the malware and phishing details regularly in your Microsoft 365 environment.	**Advanced Threat Protection** • Anti-Malware • Phishing filter • Anti-Phishing • Malware Mails Received

INCIDENT RESPONSE

Incident Response controls are employed to facilitate the planning of response measures in case of a security incident. They also are required to provide proper training to staff and personnel and in the testing of plans. The **AdminDroid Reporter** tool helps in the monitoring and analysis aspects of a breach investigation by providing the necessary information in concise reports.

Control	Implementation of Control in Microsoft 365	Applicable AdminDroid Reports
1. Incident Monitoring Monitor and detect security incidents in your information system in a timely manner.	Review user and administrator activity such as login failures to spot any suspicious events which could lead to a security incident.	**Risky Login Attempts** • Failed to Pass MFA challenge • Legacy/basic auth attempts • Expired password login attempts • Admins login failure • Admins login failure summary • Disabled User Login Attempts • Failed Sign-ins • Failed in MFA challenge **Risky Sign-ins** • Confirmed Risky Sign-ins • Open Risky Sign-ins **Password Changes** • User password changes • Self-service password resets

		Risky Sign-ins by Risk Level • High Risky Sign-ins • Medium Risky sign-ins • Low Risky sign-ins • Hidden Risky sign-ins **Sign-ins with Prompts** • Strong Auth Enrollment Prompted Sign-ins • Signed-in via Alternate Auth Method • Password reset Prompts • Multiple O365 Accounts Prompts • Keep Me Signed-in Prompts **Administrative Users Reports** • User added as admins
	Identify information security hazards to your Microsoft 365 Environment and review their status until closure.	**Advance Threat Protection** • Safe Attachment • Safe Link • Anti-Spam • Anti-Malware • Phishing Filter • Junk Email • DKIM Config • All ATP Activities • Anti-Phishing • ATP Config
2. Incident Analysis Analyse and investigate the events and activity deemed anomalous in your information system.	Analyse the security incident to understand its impact on your Microsoft 365 Environment and determine the appropriate response.	**Overall Activities** • All Activities • Admin Activities • All Failed Activities **Sharing & Access** • All File/Folder Sharing Activities • All File/Folder Access Activities • Anonymous User Activities • External User Activities • Guest User Activities • Files shared by External users • Files shared to External users • File Deletion • File/Folder Accesses by External Users • Anonymous Link Creation • Anonymous Link Accessed

		Office 365 Workload Based Activities • Azure AD Activities • Exchange Activities • SharePoint Activities • OneDrive Activities • OneNote Activities • Power BI Activities • Teams Activities • Stream Activities • Security and Compliance • Compliance Search Activities
3. Information Spillage Response Identify, alert, isolate and eradicate the contamination in your information system.	Configure alerts in your Microsoft 365 Environment to identify any suspicious activity that may lead to an information breach.	**Alert Category** • Data Loss Prevention • Threat Management • Information Governance • Mail flow

CONFIGURATION MANAGEMENT

Configuration Management controls are necessary to ensure the proper configuration of the information system, to make sure that the configuration is in line with policies and procedures and all changes to the configuration are authorized and properly documented.

Control	Implementation of Control in Microsoft 365	Applicable AdminDroid Report
1. Configuration Change Control Audit the changes to the configuration of your organization's information system components.	Review changes to the configuration of devices and other services in the Microsoft 365 Environment to ensure that changes are being made by authorized personnel in line with your change management procedures.	**Device Audit** • Device Config changes **Advance Threat Protection** • Safe attachment • Safe link • Anti-Spam • Anti-Malware • Phishing Filter • Junk Email • DKIM Config • All ATP Activities • Anti-phishing • ATP config

		Mobile Device Audit • Mobile Device Configs • Active Sync Configs • Text Message Settings **Data Loss Prevention** • DLP Configs **Mail Flow** • Mail Flow Configs • Connector Configs • Accepted Domains • Remote Domain • Hybrid Configs • Federation Configs **Add On Management** • Bots • Connectors • Tabs • All Activities **Site Collections** • SharePoint Sharing Configs • SharePoint DLP Actions
2. Access Restrictions for Change Establish and enforce logical access restrictions associated with changes to the information system.	Ensure that Microsoft 365 configuration change rights is limited to authorized personnel by identifying the users or groups with administrative roles and reviewing changes related to these roles.	**Admin Reports** • All admins • Admin Roles by Users • All Global Admins • Admins with Management Roles • Admins with Read Access Roles **Overall Activities** • All activities • Admin Activities • All Failed Activities **Admin Role Changes** • All Role Member Changes • Role Assignments • Role Scope Changes • All Role Operations

3. Configuration Settings Monitor for changes to the configuration settings of the IT Products within your information system.	Monitor and identify the changes to the configuration of your Microsoft 365 Environment to make sure that no unauthorized changes are made.	**Device Audit** • Device Config Changes **Directory Audit** • Directory Setting Changes • Domain Changes
4. Software Usage Restrictions and User Installed Software Enforce software installation policies and monitor their effective implementation in your information system.	Monitor applications added through Azure Active Directory to ensure that they follow your organization's software installation policies.	**Software Installs** • Office activations • Project client • Visio client • Activations user Counts • Activation Counts **Application Audit** • Added applications • Consent to applications • OAuth2 permission grant

RISK ASSESSMENT

Risk Assessment Controls are mandatory to secure your organization from various risks, threats, and attacks. Monitoring risk assessments, critical resources, risk responses will help you to ensure the security of the organization. Make sure these controls are periodically monitored and documented properly.

Control	Implementation of Control in Microsoft 365	Applicable AdminDroid Report
1. Policy and Procedures **a.** Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: (i) [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and (ii) Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls; **b.** Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and **c.** Review and update the current risk assessment:	Monitor all the security related policies and its conditions configured in your Microsoft 365 environment.	**CA Policy Configuration Analytics** • All CA policies • Recently modified CA policies • CA Policies with Grant Control details • CA Policies with Session Control details **CA Policy Assignment Details analytics** • User Conditions of CA policies • Groups Conditions of CA policies • Roles Conditions of CA policies • Application Conditions of CA policies • Platform Conditions of CA policies • Location Conditions of CA policies • Guest/External user conditions of CA policies • Policies with All as Condition Values

(i) Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and (ii) Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].		**MFA Configured Policies Analytics** • Policies with MFA • MFA policies Assignment Overview • MFA policies Assignment Details
2. Risk Assessment **a.** Conduct a risk assessment, including: (i) Identifying threats and vulnerabilities in the system. **b.** Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments. **c.** Review risk assessment results [Assignment: organization-defined frequency]. **d.** Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]. **e.** Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system	Review all the risky logins with its details detected by the security policies.	**Risky Sign-ins by Risk Level** • High Risky Sign-ins • Medium Risky Sign-ins • Low Risky Sign-ins • Hidden Risky Sign-ins **Risky Sign-ins by Detection Timing** • Real Time Risk Detections • Near Real Time Risk Detections • Offline Risk Detections **Risky Sign-ins by Risk Event Type** • All Risky Sign-In Events • Anonymous IP Address • New Country • Unlikely Travel • Malicious IP Address • Unfamiliar Features • Malware Infected IP Address • Suspicious IP Address • Leaked Credentials • Investigations Threat Intelligence • Generic Events • Generic Admin Confirmed user compromised • Password Spray • MCAS impossible travel • MCAS suspicious inbox manipulation rules • Investigations Threat Intelligence sign in linked • Malicious IP address valid credentials blocked IP • Admin confirmed user compromised

3. Risk Response Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.	Monitor all the responses taken by the users for the risky activities detected in the organization.	**Risky Sign-ins by Risk Resolved Method** • Admin Generated Temporary Password • User Performed Secured Password Change • User Performed Secured Password Reset • Admin Confirmed Sign-in Safe • AI Confirmed Sign-in Safe • User Passed MFA Driven by • Risk Based Policy • Admin Dismissed All Risk for User • Admin Confirmed Sign-in Compromised **Risky Sign-ins by Risk Status** • Marked As Safe • Marked As Remediated • Marked As Dismissed • Marked As Compromised
4. Criticality Analysis Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].	Identify and analyse all the critical resources to secure your organization from unauthorized access or data breach.	**Risky Sign-ins** • Confirmed Risky Sign-ins • Open Risky Sign-ins • Admin Confirmed User Compromised • Risk Status Marked as Compromised **Sign-ins with Prompts** • Strong Auth Enrollment Prompted Sign-ins • Signed-in Via Alternate Auth Method • Password reset Prompts • Multiple O365 Accounts Prompts • Keep Me Signed-in Prompts

MAPPING OF ADMINDROID REPORT CATEGORIES TO CONTROL GROUPS

The below mapping will help you to identify how various Microsoft 365 reporting fulfilling the PCI-DSS compliance controls to meet your compliance requirements.

Report Category	Control Groups	Applicable AdminDroid Reports
User Logins (Audit.AzureAD.UserLogins)	Unsuccessful Logon Attempts Previous Logon (Access) Notification Re-Authentication Security Function Verification	• Successful User Logins • Failed User Logins • Failed Sign-ins • Failed logins in MFA challenge • MFA Disabled • User Login Count Summary • User's First Logon Time • User's Last Logon Time • All User Logins • Users' Login Failure Summary • Users' last logon summary by users • Users' last logon summary by application • Users' last logon summary by city • Users' last logon summary by state • Users' last logon summary by country • Users' last logon summary by browser • Users' last logon summary by operating system
Password Changes (Audit.AzureAD.PasswordChanges)	Authenticator Management Account Management Audit	• User Password Changes • Password Reset by Admin • Forced/Expired Password Reset • Forced by Admin • All Password Changes
User Audit (Audit.AzureAD.UserAudit)	Account Management Audit Identifier Management	• Created Users • Updated Users • License Changes • Deleted Users • All User Events

Group Audit (Audit.AzureAD.GroupAudit)	Identifier Management	• Created Groups • Deleted Groups • Updated Groups • Group Member Changes
Admin Role Changes (Audit.AzureAD.AdminRole)	Account Management Audit Access Restrictions for Change	• All Role Member Changes • All Role Operations • Role Assignments • Role Scope Changes • Deleted Roles • Updated Roles • Added Roles
Application Audit (Audit.AzureAD.ApplicationAudit)	Software Usage Restrictions and User Installed Software	• Added applications • Consent to Applications • OAuth2 Permission grant
Directory Audit (Audit.AzureAD.DirectoryAudit)	Configuration Settings	• Domain Changes • Setting Changes
Device Audit (Audit.AzureAD.DeviceAudit)	Device Identification and Authentication Configuration Change Control Configuration Settings	• Added Devices • Deleted Devices • Updated Devices • Config Changes • Credential Changes • Owner Changes • User Changes • All Device Operations • Sign-ins with Device details • Mobile Sign-ins • Non-compliant Device sign-ins • Unmanaged Device sign-ins

Risky Login Attempts (Audit.Security.RiskyLoginAttempts)	Incident Monitoring Unsuccessful Logon Attempts	• Failed to Pass MFA • Legacy/Basic Auth Attempt Challenge • Expired Password Login Attempts • Admin's Login Failures • Admin's Login Failure Summary • Disabled User Login Attempts • Failed Sign-ins • Failed in MFA challenge
Administrative Users Reports (Audit.Security.UserAddedAsAdmins)	Least Privilege	• User added as admins *(25 reports)*

Mailbox Access (Audit.Exchange.MailboxAccess)	Least Privilege	• MFA Non-owner access
Mailbox Permissions (Audit.Exchange.MailboxPermissions)	Least Privilege	• Access to Others Mailboxes • Mailbox Permission Summary • Mailbox Permission Detail • Mailbox with Send on Behalf • Send as Permission • Full Permission • Read Permission • Guests' Mailbox Permission Summary • Admins Access to Others Mailboxes • Admins with Send-on-Behalf • Admins with Send-As • Admins with Full Access • Guests Access to Others Mailboxes

Advanced Threat Protection (Audit.Exchange.ATP)	Incident Monitoring Configuration Change Control Spam Protection Memory Protection	• Safe Attachment • Safe Link • Anti-Spam • Anti-Phishing • Anti-Config • Spam Mails Received • Spam Mails Sent/Received • Anti-Malware • Phishing Filter • Junk Email • DKIM Config • All ATP Activities
Role Changes (Audit.Exchange.RoleChanges)	Least Privilege	• Management • Role Assignments • Assignments Policy • Role Entry • Role Scope • Role group
Mail Flow (Audit.Exchange.MailFlow)	Configuration Change Control	• Mail Flow Configs • Transport Rules • Connector Configs • Accepted Domains • Remote Domain • Hybrid Configs • Federation Configs
Mobile Device Audit (Audit.Exchange.MobileDevice)	Access Control for Mobile Devices Configuration Change Control	• Mobile Device Configs • Active Sync Configs • Text Message Configs
Data Loss Prevention (Audit.Exchange.DataLossPrevention)	Configuration Change Control	• DLP Configs • Rule Matches

Access Requests (Audit.SharePoint.AccessRequests)	Information Sharing Audit	• Requests Created • Requests Accepted • Requests Denied • Modified Files
Sharing Invitations (Audit.SharePoint.SharingInvitations)	Information Sharing Audit	• Invites Created • Invites Accepted • Invites Revoked • All Events • External User Invites
File Activities (Audit.SharePoint.FileActivities)	Information Sharing Audit	• All Events

Teams (Audit.Teams.Teams)	Unsuccessful Logon Attempts	• Login Activities
Add On Management (Audit.Teams.AddOnManagement)	Configuration Change Control	• Bots • Connectors • Tabs • All Activities

All User Summary (Audit.Alerts.AllUserSummary)	Non-Repudiation	• All user summary by activity

External User Summary (Audit.Alerts.ExternalUserSummary)	Cross-organizational Auditing	• Overall External user summary • External user summary by activity • External user summary by activity type • External user summary by alert policy name • External user summary by security • External user summary by category • External user summary by policy type • External user summary system alerts
Alert Severity (Audit.Alerts.AlertSeverity)	Security Alerts, Advisories and Directives	• High severity • Medium severity • Low severity
Alert Category (Audit.Alerts.AlertCategory)	Security Alerts, Advisories and Directives Information Spillage Response	• Data Loss Prevention • Threat Management • Information Governance • Permissions • Mail flow • Others

Overall (Audit.SecureScore.Overall)	Software, Firmware and Information Integrity	• Control Settings Scores Daily Trend • Control Settings Recent Scores • Zero Score • Full Score • Overall score trend • All Tenants Score Trend • Tenant Seats Score Trend • Industry Type Score Trend

Overall Activities (Audit.General.Overall)	Account Usage Monitoring Information System Monitoring Incident Analysis Access Restrictions for Change	• Admin Activities • All Failed Activities • All Activities • Top Activity Summary • Daily activity summary • Activity by Department • Activity by City • Activity by State • Activity by Country • Activity by JobTitle • Activity by Company
Office 365 Workload Based Activities (Audit.General.O365WBA)	Audit Events Audit Review Analysis & Reporting Information System Monitoring Incident Analysis	• Azure AD Activities • Exchange Activities • SharePoint Activities • OneDrive Activities • OneNote Activities • Power BI Activities • Teams Activities • Stream Activities • Security and Compliance • Compliance Search Activities
Sharing & Access Audit.General.SharingAndAccess	Incident Analysis Information Sharing Audit	• Anonymous User Activities • External User Activities • Guest User Activities • All File/Folder Sharing Activities • All File/Folder Access Activities • Files shared by External users • Files shared to External users • File/Folder accesses by External Users • File Deletion • Anonymous link creation • Anonymous link accessed • Files shared via Teams Channels • Files shared by External Users in Channels • Files shared via 1:1 chat • Files shared to External Users 1:1 chat

User Reports (Stat.AzureAD.UserReports)	Account Management Audit Identification and authentication (Organizational Users)	• All Users • Disabled Users • Enabled Users • Recently Created • Deleted Users • Users not in any Group • Cloud Users • Synced Users • Release Track Users • All Contacts • Users with Errors • Internal Guest Users
License Reports (Stat.AzureAD.LicenseReports)	Least Privilege	• Licensed Users • Users by Subscriptions • Unlicensed Users • Free Users • Trial Users
Group Reports (Stat.AzureAD.Group)	Account Type Monitoring	• All Groups • Group Members • Cloud Groups • Nested Groups • Synced Groups • Deleted Groups
Manager Reports (Stat.AzureAD.ManagerReports)	Account Details Monitoring	• Managers & Direct Reports • Users with Manager • Users without Manager
License & Subscription Usage (Stat.AzureAD.LicenseReports)	Account Usage Monitoring	• Daily Activities • Subscription Usage • Unused Subscriptions • Licensed Users • Regain Licenses

MFA Reports (Stat.Security.MFAReports)	Identification and Authentication (Organizational Users) Security Function Verification	• User with MFA • Users without MFA • MFA Enabled • MFA Enforced Users • MFA Activated Users • MFA Non-Activated User • MFA Device Details
Password Reports (Stat.Security.PasswordReports)	Identification and Authentication (Organizational Users) Authenticator Management	• Password Policies • Password Expired Users • Password soon to Expire Users • Password Never Expire Users • Users with Password Expiry • Password never changed • Password not changed in 90 days • Recent password changers • Users with weak password allowed
Admin Reports (Stat.Security.AdminReports)	Access Restrictions for Change Least Privilege	• All Admins • Admin Roles by Users • All Global Admins • Admins with Management Roles • Admins with Read Access Roles
External User Reports (Stat.Security.ExternalUserReports)	Account Management Audit	• All External Users

Mailbox Info (Stat.Exchange.MailboxInformation)	Identifier Management	• All Mailboxes • Shared Mailboxes • Archived Mailboxes

Shared Mailbox Info (Stat.Exchange.SharedMailboxInfo)	Account Usage Monitoring	• Shared mailbox size over time
Mailbox Usage (Stat.Exchange.MailboxUsage)	Account Usage Monitoring	• Mailbox size over time • Daily mailbox quota status • Archived mailbox over warning quota • Daily Site Storage
Audit Settings (Stat.Exchange.AuditSettings)	Audit Review, Analysis and Reporting	• Audit enabled mailboxes • Audit disabled mailboxes • Admin Audit enabled • Owner audit enabled • Delegate audit enabled
Mobile Devices (Stat.Exchange.MailboxInfo)	Access Control for Mobile Devices Device Identification and Authentication	• All Mobile Devices • Devices by Connected Mailbox • Mobile Device by OS • Mobile Device by Policy • Mobile Dives by Client Type • Mobile Devices by Access State

Site Collections (Stat.SharePoint.Site)	Configuration Change Control	• Sharing Configs • SharePoint DLP Actions
Inactive Users (Stat.SharePoint.InactiveUsers)	Inactive Users	• By Last File Accessed • By Last File Synced • By Last External Share • By Last Internal Share • By Last Page Access

Daily Activation Summary (Stat.SharePoint.DailySummary)	Account Usage Monitoring	• Daily Active users • Users File Access Summary • Users File Synced Summary • Users Internal File Sharing Summary • Users External File Sharing Summary • Users Page Visit Summary • Daily Summary of Users by Activity

Inactive Users (Stat.OneDrive.InactiveUsers)	Inactive Users	• By Last File Accessed • By Last File Synced • By Last External Share • By Last Internal Share
Daily Summary (Stat.OneDrive.DailySummary)	Account Usage Monitoring	• Daily Activities • User Activities • Active Users

User Activities (Stat.Teams.UserActivities)	Account Usage Monitoring	• Daily Activities • Overall Activities
Inactive Users (Stat.Teams.InactiveUsers)	Account Management Audit Inactive Users	• By Last Team Chat • By Last Private Chat • By Last Call Activity • By Last Meeting Activity

Inactive Users (Stat.Yammer.InactiveUsers	Inactive Users	• By Last Post Liked • By Last Post Posted • By Last Post Read • By Last Activity
User Activities (Stat.Yammer.UserActivities)	Account Management Audit	• Daily Activities • Overall Activities

User Activities (Stat.Skype.UserActivities)	Account Usage Monitoring	• Peer to peer Sessions • Organized Conference • Participated Conference • File Transfer • Instant Messages

Active Users (Stat.General.ActiveUsers)	Account Management Audit	• Last Active Time • Daily Active Users • Exchange Last Active Time • SharePoint Last Active Time • OneDrive Last Active Time • Teams Last Active Time • Yammer Last Active Time
Office 365 Group Creations (Stat.General.Office365GroupCreations)	Account Management Audit	• Groups created via Teams • Groups created via Yammer • Groups created via SharePoint • Empty Groups • Groups with Hidden membership
Software Installs (Stat.General.SoftwareInstalls)	Software Usage Restrictions and User Installed Software	• Office activations • Project client • Visio client

Risky Sign-ins (Anal.Sign-inAnal.RiskySign-Ins)	Criticality Analysis Incident Monitoring	• Confirmed Risky Sign-ins • Open Risky Sign-ins • Admin Confirmed User Compromised • Risk Status Marked as Compromised
Sign-ins with Prompts (Anal.Sign-inAnal.Sign-InsWithPrompt)	Criticality Analysis Incident Monitoring	• Strong Auth Enrollment Prompted Sign-ins • Signed-in Via Alternate Auth Method • Password reset Prompts • Multiple O365 Accounts Prompts • Keep Me Signed-in Prompts
Risky Sign-ins by Risk Level (Anal.Sign-InAnal.ByRiskLevel)	Risk Assessment Incident Monitoring	• High Risky Sign-ins • Medium Risky Sign-ins • Low Risky Sign-ins • Hidden Risky Sign-ins
Risky Sign-ins by Detection Timing (Anal.Sign-In.Anal.ByDetectTiming)	Risk Assessment	• Real Time Risk Detections • Near Real Time Risk Detections • Offline Risk Detections
Risky Sign-ins by Risk Status (Anal.Sign-InAnal.ByRiskStatus)	Risk Response	• Marked As Safe • Marked As Remediated • Marked As Dismissed • Marked As Compromised

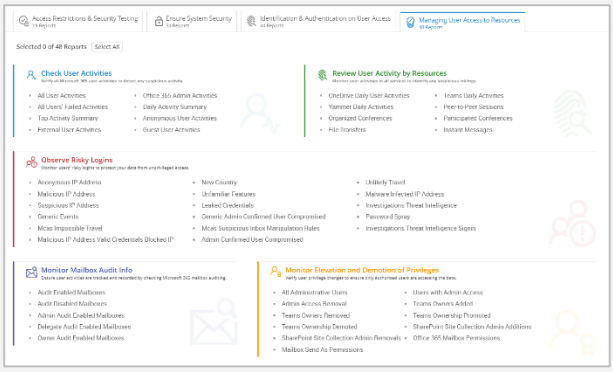
Risky Sign-ins by Risk Event Type (Anal.Sign-InAnal.ByRiskEventType)	Risk Assessment	• All Risky Sign-In Events • Anonymous IP Address • New Country • Unlikely Travel • Malicious IP Address • Unfamiliar Features • Malware Infected IP Address • Suspicious IP Address • Leaked Credentials • Investigations Threat Intelligence • Generic Events • Generic Admin Confirmed user compromised • Password Spray • MCAS impossible travel • MCAS suspicious inbox manipulation rules • Investigations Threat Intelligence sign in linked • Malicious IP address valid credentials blocked IP • Admin confirmed user compromised
Risky Sign-ins by Risk Resolved Method (Anal.Sign-InAnal.ByResolvedMethod)	Risk Response	• Admin Generated Temporary Password • User Performed Secured Password Change • User Performed Secured Password Reset • Admin Confirmed Sign-in Safe • AI Confirmed Sign-in Safe • User Passed MFA Driven by Risk Based Policy • Admin Dismissed All Risk for User • Admin Confirmed Sign-in Compromised

CA Policy Configuration (Anal.CAP.PolicyConfiguration)	Policy and Procedures	• All CA policies • Recently modified CA policies • CA Policies with Grant Control details • CA Policies with Session Control details

CA Policy Assignment Details (Anal.CAP.AssignmentDetails)	Policy and Procedures Identification and Authentication (Organizational Users)	• User conditions on Access Policies • Guest/External user conditions on Access Policies • Groups Conditions of CA policies • Roles Conditions of CA policies • Application Conditions of CA policies • Platform Conditions of CA policies • Location Conditions of CA policies • Policies with All as Condition Values • Password policies Reports • Policies with User Assignments
MFA Configured Policies (Anal.CAP.MFAConfigPolicies)	Policy and Procedures Identification and Authentication (Organizational Users)	• Policies with MFA • MFA policies Assignment Overview • MFA policies Assignment Details

Pre-compiled Report Bundle for PCI-DSS Compliance

- Familiarizing every compliance requirement and putting it into action will be challenging for compliance admins.
- AdminDroid comes up with compliance ReportBoards specially made for achieving compliance in your organization without a hitch.
- Respective Microsoft 365 reports are grouped together based on compliance control requirements and further categorized to make it feasible for monitoring various activities required to achieve compliance.



☞ Explore PCI-DSS Report Board

(You will be redirected to AdminDroid demo to view ReportBoard)

Outline of PCI-DSS Compliance Report Categorization

Access Restrictions & Security Testing

Verify the access restrictions of users using the file access, modifications, deletions activities of users.

- Access Management Monitoring *(8 Reports)*
- Monitor File Access and Sharing *(5 Reports)*
- Track File Modifications & Deletions *(6 Reports)*

Ensure System Security

Monitor the system threats, authentication details, secure scores, etc., for your organization's security.

- Detect Threats & Alerts *(10 Reports)*
- Monitor System Authentication & Deletion *(5 Reports)*
- Manage Vulnerability by Secure Scores *(4 Reports)*
- Ensure Email Threat Configurations *(8 Reports)*
- Monitor Mail with Threats *(7 Reports)*

Identification & Authentication on User Access

Check the user's access by reviewing their details like authentications, failed logins, device details, and more.

- Identify Organization Users *(8 Reports)*
- Track Group Details *(6 Reports)*
- Identify User Devices *(6 Reports)*
- Monitor User Authentication Details *(9 Reports)*
- Track Inactive User Accounts *(6 Reports)*
- Review Users' Failed Login Attempts *(5 reports)*
- Verify Device Details *(5 Reports)*

Managing User Access to Resources

Review the various resources accessed by the users to prevent any unnecessary accesses and to protect your data.

- Check User Activities *(8 Reports)*
- Observe Risky Logins *(17 Reports)*
- Review User Activity by Resources *(8 Reports)*
- Monitor Mailbox Audit Info *(5 Reports)*
- Monitor Elevation and Demotion of Privileges *(11 Reports)*

How can AdminDroid help implement other Security and Compliance requirements?

Apart from aligning with PCI-DSS security standards, AdminDroid also offers various security controls to ensure compliance with your Microsoft 365 Environment.

We have listed here the other security controls using which you can establish conformity to Cloud Environment regulations.

Explore >

AdminDroid

Our mission is to solve everyday challenges of IT admins and save their time. We strive to provide admin-friendly software with a user-friendly interface, at a budget-friendly pricing. Try AdminDroid, and you'll love how it simplifies your Microsoft 365 management!

For a live demonstration of our flagship tool, AdminDroid Microsoft 365 Reporter, visit below.

Live Demo **Download**

Connect with us

linkedin.com/company/admindroid/ reddit.com/r/AdminDroid/ twitter.com/admiindroid

facebook.com/admindroid youtube.com/admindroid admindroid.com

github.com/admindroid-community