ad
AdminDroid

ISO Compliance

with

AdminDroid

AdminDroid

ISO:27001 Compliance with AdminDroid

The **ISO (the International Organization for Standardization)** and **IEC (the International Electrotechnical Commission)** form the specific system for worldwide standardization. The members or authorities of ISO and IEC take part in developing the standards and controls for **Information Security Management Systems (ISMS)**. The third edition of ISO/IEC 27001 was developed and published in October 2022, which is technically revised and combined to reduce the existing 114 controls.

ISO/IEC 27001:2022 has **93 controls** that provide security measures to protect your organization's sensitive data. Every organization can adopt these controls based on their security requirements, size, an organization needs, and processes used. Though this edition is evolved, organizations have **3 years duration** to move from the 2013 edition to the 2022 edition.

These security controls can be used by both internal and external parties to audit the organization's ability to achieve information security requirements. To make this process easier for you, we have deeply analyzed and compiled this document which helps you to be compliant with ISO 27001.

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 INFORMATION AND INTEGRITY

INCIDENT RESPONSE

AUDIT AND ACCOUNTABILITY

RISK ASSESSMENT

PLANNING

PROGRAM MANAGEMENT

SYSTEM AND SERVICES ACQUISITION

SYSTEM & COMMUNICATION PROTECTION

MAPPING OF ISO:27001 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.)

MAPPING OF ISO:27001 STANDARDS WITH CONTROL FAMILIES

Control	Families
5. Organizational Controls	
5.1 Policies for Information Security Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	**Configuration Management** • Information System Monitoring **Risk Assessment** • Policy and procedures
5.2 Information security roles and responsibilities Information security roles and responsibilities shall be defined and allocated according to the organization's needs.	**Access Control** • Least Privilege
5.4 Management responsibilities Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	**Planning** 1. System Security and Privacy Plans 2. Central Management
5.6 Contact with special interest groups The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	**Access Control** 1. Account Management Audit • Account Types Monitoring
5.7 Threat Intelligence 2022 Update Information relating to information security threats shall be collected and analyzed to produce threat intelligence.	**System and Information Integrity** 1. Information system monitoring 2. Security alerts, advisories, and directives 3. Spam protection 4. Memory protection **Incident Response** 1. Incident Monitoring

5.9 Inventory of information and other associated assets An inventory of information and other associated assets, including owners, shall be developed and maintained.	**Hardware assets** **Identification and Authentication** 1. Account Management Audit • Added Devices • Device Owner Changes • All Mobile Devices **Software Resources** • All Sites • SPO site owners • All Office 365 groups • Office 365 group owners
5.10 Acceptable use of information and other associated assts Rules for acceptable use and procedures for handling information and other associated assets shall be identified, documented, and implemented.	**Incident Response** 2. Incident Analysis • Sharing & Access
5.11 Return of assets Personnel and other interested parties, as appropriate, shall return all the organization's assets to their possession upon change or termination of their employment, contract or agreement.	**Access Control** 1. Least Privilege • Mailbox Permissions ○ User access to other's mailboxes **Identification and Authentication** 1. Device Identification & Authentication • Device Deletion
5.12 Classification of Information Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability, and relevant interested party requirements.	**Configuration Management** 1. Configuration Change Control **Planning** 1. System Security and Privacy Plans • Sensitivity labels

5.13 Labelling of Information An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	**Planning** 1. System Security and Privacy Plans • Sensitivity label applied for SPO files • Sensitivity label changed for SPO files • Sensitivity label removed for SPO files • Site label applied • Site label changed • Site label removed • File label applied • File label changed • File label removed
5.14 Information Transfer Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	**Incident Response** 1. Incident Analysis • Sharing & Access **Access Control** • Information Sharing Audit
5.15 Access control Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	**Access Control**
5.16 Identity management The full life cycle of identities shall be managed.	**Identification and Authentication**
5.17 Authentication information Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	**Identification and Authentication**
5.18 Access rights Access rights to information and other associated assets shall be provisioned, reviewed, modified, and removed in accordance with the organization's topic-specific policy on and rules for access control.	**Access Control**

5.23 Information security for use of cloud services 2022 Update Processes for acquisition, use, management, and exit from cloud services shall be established in accordance with the organization's information security requirements.	• Service Principal Sign-ins • All Sign-ins (Also, we recommend you can monitor all the sign-ins of each cloud services and any third-party cloud services used in your organization)
5.24 Information security incident management planning and preparation. The organization shall plan and prepare for managing information security incidents by defining, establishing, and communicating information security incident management processes, roles, and responsibilities.	**Incident Response**
5.25 Assessment and decision on information security events The organization shall assess information security events and decide if they are to be categorized as information security incidents.	**Incident Response** 1. Information Spillage Response **Risk Assessment** 1. Risk Assessment 2. Criticality Analysis
5.26 Response to information security incidents Information security incidents shall be responded to in accordance with the documented procedures.	**Incident Response** **Risk Assessment** 1. Risk Response
5.28 Collection of evidence The organization shall establish and implement procedures for the identification, collection, acquisition, and preservation of evidence related to information security events.	**Planning** 1. System Security and Privacy Plans • eDiscovery Cases • Security Filters • Legal Hold • Compliance Search Activities
5.33 Protection of records Records shall be protected from loss, destruction, falsification, unauthorized access, and unauthorized release.	**Planning** 2. System Security and Privacy Plans • Data Loss Prevention

5.34 Privacy and protection of personal identifiable information (PII) The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements	**Planning** 1. System Security and Privacy Plans • Data Loss Prevention • Sensitivity Labels
5.35 Independent review of information security The organization's approach to managing information security and its implementation including people, processes, and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	**Audit and Accountability**
6. People Controls	
6.7 Remote working Security measures shall be implemented when personnel are working remotely to protect information accessed, processed, or stored outside the organization's premises.	**Configuration Management** 1. Least Functionality • Policies with Location Assignments
6.8 Information security event reporting The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	**System and Information Integrity** 1. Security Alerts, Advisories, and Directives • User activity alerts • Triggered Alert Policies • Alerts Summary by users • Alerts Summary by external users Moreover, you can benefit from AdminDroid's Advanced Alerting feature to stay on top of suspicious actions, unusual behaviors, etc. Also, we recommend you monitor all the event logs and any third-party tools you use in your organization.
8. Technological Controls	
8.1 User end point devices Information stored on, processed by or accessible via user end point devices shall be protected.	**Access Control** • Access control for mobile device

8.2 Privileged access rights The allocation and use of privileged access rights shall be restricted and managed.	Access Control • Least Privilege
8.3 Information access restriction Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	Access Control
8.4 Access to source code Read and write access to source code, development tools, and software libraries shall be appropriately managed	Access Control 2. Least Privilege • SharePoint Site Collection Permissions • OneDrive Site Permissions
8.5 Secure authentication Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	Identification and Authentication
8.6 Capacity management The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	System and Communication Protection • Resource availability
8.7 Protection against malware Protection against malware shall be implemented and supported by appropriate user awareness.	System Information and Integrity • Memory Protection
8.8 Management of technical vulnerabilities Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	Risk Assessment • Vulnerability Monitoring and Scanning
8.9 Configuration management 2022 Update Configurations, including security configurations, of hardware, software, services, and networks shall be established, documented, implemented, monitored, and reviewed.	Configuration Management

8.10 Information deletion Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	- Inactive files - Inactive sites
8.12 Data leakage prevention 2022 Update Data leakage prevention measures shall be applied to systems, networks, and any other devices that process, store, or transmit sensitive information.	**Planning** 1. System Security and Privacy Plans - Data Loss Prevention
8.13 Information backup Backup copies of information, software, and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	**System and Information Integrity** 1. Information Management, Retention, and Refresh - Recycled a SharePoint File Version - Recycled all minor versions of a File in SharePoint - Recycled all versions of a file in SharePoint - Admins deleted a file version permanently by script - Recycled versions of a file in OneDrive - Recycled a OneDrive file version
8.15 Logging Logs that record activities, exceptions, faults, and other relevant events shall be produced, stored, protected, and analyzed.	**Audit and Accountability**
8.16 Monitoring activities 2022 Update Networks, systems, and applications shall be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents.	**Risk Assessment**

8.19 Installation of software on operational systems Procedures and measures shall be implemented to securely manage software installation on operational systems.	**Configuration Management** 1. Software usage restrictions and user installed software
8.20 Networks security Networks and network devices shall be secured, managed, and controlled to protect information in systems and applications.	**Identification and Authentication** 1. Device Identification and Authentication • Added Devices • All Device operations • All Mobile Devices • Mobile Device configuration changes
8.26 Application security requirements Information security requirements shall be identified, specified, and approved when developing or acquiring applications.	**Configuration Management** 1. Software Usage Restrictions and User Installed Software • Azure AD applications • Consent to applications
8.32 Change management Changes to information processing facilities and information systems shall be subject to change management procedures.	**Configuration Management** • Configuration Change Control • Access Restrictions for Change • Configuration Settings

MAPPING OF CONTROL GROUPS TO REPORT COLLECTIONS

The below mapping will help you to find out the various ISO 27001 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 • Groups Created via Stream • Groups Created via Outlook • 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 Job Title • Activity by Company **User Activities** • Anonymous User Activities • External User Activities • Guest User Activities • Users Activity Count • Users Failed Activity Count **Sharing & Access Activity** • 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 • Secure links used to access SPO files • Access Extended Files • Secure links used to access a OneDrive Item **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** • 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 • By Last Activity Date (ReportBoard) **SharePoint Inactive Users** • By Last File Access • By Last File Synced • By Last External Share • By Last Internal Share • By Last Page Access • By Last Activity Date (ReportBoard) **OneDrive Inactive Users** • By Last File Accessed • By Last Internal Share • By Last External Share • By Last File Synced • By Last Page Access (ReportBoard) **Teams Inactive Users** • By Last Team Chat • By Last Private Chat • By Last Call Activity • By Last Organized Meeting • By Last Attended Meeting **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 • Recently Created Admins **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 • Mailbox Non-Owner Access • 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

		SharePoint Site Collection Permissions • Admin Added • Admin Removed • Member Permissions Setting Changes • Disable Member Permissions using Script • Permission Level Added • Permission Level Removed • Permission Level Modified • Hub Site Permission Sync Enabled • Hub Site Permission Sync Disabled **OneDrive Site Permissions** • Admin Added • Admin Removed • Permission Level Added • Permission Level Removed • Permission Level Modified **Role Configuration Changes** • Assigning Roles to Bulk Users • eDiscovery Members • eDiscovery Admins
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 • Teams Login Activities • Failed Sign-ins • Failed logins in MFA challenge **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 **Device Configuration** • Device Access Policy • Device Configurations • Device Tenant Configurations
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 • Access Extended Files **SharePoint Access Requests Reports** • Requests Created • Requests Accepted • Requests Denied • Requests Updated • Access Request Settings Modified • All Events **SharePoint Sharing Invitations Reports** • Invites Created • Invites Accepted • Invites Revoked • Invites Blocked • Invites Updated • Guest User Expiration Changed • All Events • External User Invites

		SharePoint Secure Links • Secure Links Created • Secure Links Used • Secure Links Deleted • Secure Links Updated • Added to Secure Link • Removed from Secure Link **OneDrive Sharing Invitations Reports** • Invites Created • Invites Accepted • Invites Revoked • Invites Blocked • Invites Updated • Guest User Expiration Changed **OneDrive Secure Links** • Secure Links Created • Secure Links Used • Secure Links Deleted • Secure Links Updated • Added to Secure Link • Removed from Secure Link
6. Session Termination Automatically terminate a user session after a specific period asking user to reauthenticate.	Audit the policies enabled to control user sessions to prevent unauthorized usage of user accounts in the organization.	All Conditional Access Policies with Session Control Details
6. Use of External Systems Audit the information sharing activities to permit only the authorized users to share and access the information.	Audit the external devices used by the users and monitor changes on device settings, etc	• All Mobile Devices • Mobile Device Configuration Changes • Device Access Policy • Device Configurations • Device Tenant Configurations

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.	• Users with MFA • MFA Activated Users • Users' MFA details • MFA Enabled Users • MFA Enforced Users • 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 • Policies with MFA • MFA Policies Assignment Overview • MFA Policies Assignment Details • Password policies Reports • Policies with User Assignments • User conditions on Access Policies • Guest/External user conditions on Access Policies

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 • Mobile Device Config changes • Sign-ins with Device details • Mobile Sign-ins • Non-compliant Device sign-ins • Unmanaged Device sign-ins • Device Access Policy • Device Configurations • Device Tenant Configurations
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 • Created External Users • Updated External Users • Deleted External Users • License/Plans Assignment **Group Audit** • Created Groups • Deleted Groups • Updated Groups • Group Member Changes **Mailbox Info** • All Mailboxes • Shared Mailboxes • Archived Mailboxes

		SharePoint Groups • Groups Created • Groups Updated • Groups Deleted • Members Added • Members Removed • External User Added • External User Removed **OneDrive Groups** • Groups Created • Groups Updated • Members Added • Members Removed • External User Added • External User Removed **Teams Management** • Activities on Teams • Activities on Channel • Private Channels Created • All Ownership Changes **Teams Membership Changes** • Member Added • Member Removed • Owners Added • Owners Removed • Ownership Promoted • Ownership Demoted **Private Channel Membership Changes** • Member Added • Member Removed • Owners Added • Owners Removed • Ownership Promoted • Ownership Demoted

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 • Expired password login attempts • Admins login failures

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 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
6. Protection of Audit Information Provide least privileged access to users for accessing audit information and configure alerts to inform admins about suspicious activities on Microsoft 365 audit information.	Configure alerts on suspicious admin activities accessing audit log and delegate access to required individuals	• Utilize 'Granular delegation' feature to delegate access to users and prevent unauthorized access or modifications of audit log • Audit Microsoft 365 admin activities in AdminDroid to analyze what they are doing with the audit log information.
7. Audit Record Retention Retain your audit log for a minimum of 3 to 5 years to investigate threats and to fulfil compliance requirements.	Preserve Microsoft 365 audit log to identify suspicious activities and to meet organization requirements.	Using AdminDroid, you can retain your audit log information as long as you want. It helps in eDiscovery case investigations and compliance control achievements.
8. Monitoring for Information Disclosure Monitor organization information accessed by anonymous users and sites shared externally to prevent unauthorized disclosure of sensitive information in the organization.	Audit anonymous links, files accessed by anonymous users, SharePoint sites shared externally, and more to identify unauthorized access of confidential data.	• Anonymous User Activities • Anonymous Link Creation • Anonymous Link Accessed • Site Invitations Shared to External Users • Guest User Expiration Changed • Guest User Expiration Changed for OneDrive

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 • Teams Installed Apps
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.	**AdminDroid** offers more detailed Secure Score Reports for each Microsoft 365 service. • Overall Score Trend • 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** • All Activities • Admin Activities • All Failed 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 • O365 Audit Log Changes

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** - Information Alerts - Data Loss Prevention - Threat Management - Information Governance - Permissions - Mail Flow - Others - User activity alerts - Triggered alert policies - Alerts summary by users - Alerts summary by external users
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 - Incoming External Spam Mails - Outgoing External Spam Mails - Internal Spam Mails - Malware detected files
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 - Incoming External Phish Mails - Outgoing External Phish Mails - Internal Phish Mails - Incoming External Malware Mails - Outgoing External Malware Mails - Internal Malware Mails - Malware detected files

8. System Monitoring Monitor suspicious or risky activities happened in the organization. Analyse the anomalies and respond accordingly to protect the information system.	Track risky logins, suspicious access of user accounts, sites, etc. Analyze the risk severity and other details to act accordingly.	• Confirmed risky sign-ins • Open risky sign-ins • High risky sign-ins • Medium risky sign-ins • Low risky sign-ins • Hidden risky sign-ins • Failed to pass mfa challenge • Legacy/basic auth attempts • Expired password login attempts • Admin’s login failures • Disabled user login attempts • Mailbox non-owner access • Mailbox guest access • Guest access to other mailboxes • Admin mailboxes with full access • Mailbox permission detail • Site access requests accepted • Anonymous links accessed • Guest user expiration changed • External user invites • OneDrive resources accessed using anonymous links • High severity alerts • Medium severity alerts • Low severity alerts • Informational alerts
9. Informational Management, Retention, and Refresh Retain your information for minimum period and manage them securely for various purposes and to avoid data compromise or suspicious exfiltration activities.	Monitor retention policies, file versioning details, hold placed on various information, etc., in the organization.	• Retention settings App retention settings • Retention tag Audit Log Retention • Mailboxes with litigation hold • Mailboxes with retention hold • Mailboxes with In-place hold • Changed retention label Legal Hold • Version recycled SPO files • All minor versions recycled SPO files • All versions recycled SPO files • Admin deleted a SPO file version permanently by script • Version recycled OneDrive files • All version recycled OneDrive files

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 **Threat Policy** • Phishing Overrides • Spam Filtering (duplicate) • SecOps Mailbox Overrides **Mail Security Policy** • Quarantined Mail • Inbound Connector • Outbound Connector **Security and Alert Policy** • Malicious Links • Malicious Attachments • Activity Alerts • Protection Alerts • Malware Filters
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 - 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 **Threat Policy** • Phishing Overrides • Spam Filtering (duplicate) • SecOps Mailbox Overrides **Mail Security Policy** • Inbound Connector • Outbound Connector **Audit Activities and Permission** • Audit Configuration • M365 Audit Log Changes • Audit Log Retention **Information Protection Policy** • Auto-Sensitivity Labels • Sensitivity Labels • Sensitivity Label Policies **DLP Configurations** • DLP Policies • EDM Schema • DLP Sensitive Info • Detection Reports • Policy Config • Policy Tip Config

		Record Management - File Plan Configurations **Device Configurations** - Device Access Policy - Device Configurations - Device Tenant Configurations **Retention and Risk Analysis** - Retention Settings - App Retention Settings - Insider Risk Configurations - Organization Segments - Communication Compliance - Privacy Management
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 **Teams Apps Management** • Installed Apps
5. Least Functionality Restrict the use of certain software and/or services defined in the organization.	Audit Conditional access policies and its details to identify the access allowed and denied for users in the organization.	• All Conditional Access Policies • Recently modified policies • Policies with Grant control details • Policies with Session control details • Policies with User Assignments • Policies with Group Assignments • Policies with Role Assignments • Policies with Application Assignments • Policies with Platform Assignments • Policies with Location Assignments • Policies with Devices Assignments

6. Information Location Identify users who have access to the information processed or stored in the organization.	Monitor users’ access permissions on mailboxes, sites, files, apps, devices, and more to recognize who is having access to crucial information.	• User added as admins • App role assignments • Device owner changes • Device user changes • Mailbox owner access • Mailbox non-owner access • Mailbox admins access • Mailbox guest access • Mailbox permission SendAs permission • Public folder permission • Folder permission • Management role • Role assignments • SPO admin added • SPO access request accepted • SPO sharing invites accepted • SPO anonymous links accessed • SPO secure links used • Accessed files • Access extended files • Viewed pages • Page view extended • External users' activities on pages • OneDrive admin added • OneDrive anonymous links accessed • Secure links used • OneDrive sharing invites accepted • Accessed files Access extended files • Viewed pages Page view extended • eDiscovery case admins • eDiscovery case memberships • Accessed Notes Sections accessed • Power BI viewing activities • Teams members added • Teams owners added • Teams ownership promoted • Private channels member added • Private channels owners added • Private channels ownership promoted • Stream admin role changes

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 **MFA Configured Policies Analytics** • Policies with MFA • MFA policies Assignment Overview • MFA policies Assignment 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 **Threat Policy** • Phishing Overrides • Spam Filtering (duplicate) • SecOps Mailbox Overrides **Mail Security Policy** • Quarantined Mail • Inbound Connector • Outbound Connector

(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].		**Information Protection Policy** • Auto-Sensitivity Labels • Sensitivity Labels • Sensitivity Label Policies **DLP Configurations** • DLP Policies • EDM Schema • DLP Sensitive Info • Detection Reports • Policy Config • Policy Tip Config **Record Management** • File Plan Configurations **Device Configurations** • Device Access Policy • Device Configurations • Device Tenant Configurations **Retention and Risk Analysis** • Retention Settings • App Retention Settings • Insider Risk Configurations • Organization Segments • Communication Compliance • Privacy Management

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 in External Tenants **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

5. Vulnerability Monitoring and Scanning Analyse and recognize the vulnerabilities affecting the organization information and resolve the legitimate risks.	Audit the resolved risks, malware, spam, spoof, and various threats occurred in the organization. Also, review the policies for protecting information from threats.	• Risk Resolved details • Risky user sign-ins marked as remediated • Incoming external malware • Internal malware • Incoming external Phish mails • Internal phish mails • External spoof mails • Internal spoof mails • Incoming external spam mails • Internal spam mails • Malware detected files
6. Threat Hunting Detect advanced threats happened in the organization to prevent cyber threats. Additionally, monitor unusual activity occurred in the organization.	Audit unusual file activities, email traffic, malware, etc., periodically.	Utilize AdminDroid alerting to stay on top of unusual activities, unusual email traffic, malicious identifications, and much more to secure your Microsoft 365 environment.

PLANNING

Measures available in Planning are required to develop security and privacy plans as well as implementation of these plans in your organization's information system. Also, you need to manage them to secure your sensitive data. AdminDroid Microsoft 365 reporting tool provides all-inclusive details of various security policies and configurations implemented and modified in your organization.

Control	Implementation of Control in Microsoft 365	Applicable AdminDroid Reports
1. System Security and Privacy Plans Develop security and privacy plans for the information system to avoid various threats and data exposure.	Identify Identify all the security and privacy related policies created and configured in the Office 365 environment.	• Added Azure AD policy **Security and Alert Policy** • Malicious Links • Malicious Attachments • Activity Alerts • Protection Alerts • Malware Filters

		Advance Threat Protection • Safe attachment • Safe link • Anti-Spam • Anti-Malware • Phishing Filter • Junk Email • DKIM Config • All ATP Activities • Anti-phishing • ATP config • Exchange DLP configs **Sensitivity Label Activities** • File label applied for SPO files • File label changed for SPO files • File label removed for SPO files • Site label applied • Site label changed • Site label removed • File label applied for OneDrive files • File label changed for OneDrive files • File label removed for OneDrive files **Threat Policy** • Phishing Overrides • Spam Filtering • SecOps Mailbox Overrides **Mail Security Policy** • Inbound Connector • Outbound Connector **Information Protection** • Auto-Labeling policies • Sensitivity Labels • Sensitivity Label Policies **Audit Activities and Permission** • Audit Configuration **Data Loss Prevention** • DLP Policies • EDM Schema • DLP Sensitive Info • Policy Config • Policy Tip Config

		Retention and Risk Analysis • Retention Settings • App Retention Settings • Insider Risk Configurations • Organization Segments • Communication Compliance • Privacy management **Device Configurations** • Device Access Policy • Device Configurations • Device Tenant Configurations **EDiscovery** • EDiscovery cases • Security filters • Legal holds
2. Rules of Behaviour		• CA Policy (Prompt)
3. Central Management Centrally manage all the org-wide policies and controls. Avoid unauthorized modification of any controls.	Track all the security and privacy related policy configuration changes that happened in the organization.	• Azure AD policy modifications **Advance Threat Protection** • Safe attachment • Safe link • Anti-Spam • Anti-Malware • Phishing Filter • Junk Email • DKIM Config • All ATP Activities • Anti-phishing • ATP config • Exchange DLP configs **Threat Policy** • Phishing Overrides • Spam Filtering • SecOps Mailbox Overrides **Mail Security Policy** • Inbound Connector • Outbound Connector

		Security and Alert Policy • Malicious Links • Malicious Attachments • Activity Alerts • Protection Alerts • Malware Filters **Information Protection** • Auto-labeling policies • Sensitivity Labels • Sensitivity Label Policies **Audit Activities and Permission** • Audit Configuration **Data Loss Prevention** • DLP Policies • EDM Schema • DLP Sensitive Info • Policy Config • Policy Tip Config **Retention and Risk Analysis** • Retention Settings • App Retention Settings • Insider Risk Configurations • Organization Segments • Communication Compliance • Privacy management **Device Configurations** • Device Access Policies • Device Configurations • Device Tenant Configurations

PROGRAM MANAGEMENT

Control	Implementation of Control in Microsoft 365	Applicable AdminDroid Reports
2. Personally Identifiable Information Quality Management		- Usage reporting (Name change settings) - All PII related settings - Updated usage report settings (**Workload:** CoreReporting)

SYSTEM AND SERVICES ACQUISITION

System and Services Acquisition standards help organizations to review and allocate resources, document all details, develop life cycle, and more. AdminDroid Microsoft 365 reporter provides reports related to system development lifecycle with deep insights to control security privileges in the organization.

Control	Implementation of Control in Microsoft 365	Applicable AdminDroid Reports
1. System Development Life Cycle Recognize the users who are having security related roles in your Microsoft 365 environment and document it properly.	Monitor admin roles assigned to users periodically to stay on top of users who are having critical security roles in the organization.	- Global Admin - Azure Info Protection Admin - Privileged Auth Admin - eDiscovery Case Admin - Compliance Admin - Compliance Data Admin - Authentication Admin

SYSTEM AND COMMUNICATION PROTECTION

System and Communication Protection controls are necessary to secure your information and sharing of information. It helps to securely manage your information from various threats and intruders. AdminDroid Microsoft 365 reporting and auditing tool offers comprehensive reports on information security which enables you to visualize anomalies and protect your organization's data.

Control	Implementation of Control in Microsoft 365	Applicable AdminDroid Reports
1. Information in Shared System Resources Identify and prevent unauthorized sharing of information via shared resources.	Track shared mailbox and public folder permissions, inbox rules, memberships, and more to avoid unauthorized sharing of information in Microsoft 365.	• Shared mailbox members • Shared mailbox forwarding • Shared mailbox permission detail • Recently added public folders • Mail public folders
2. Resource Availability Utilize the resources by allocating available resources to the prioritized groups, sites, or mailboxes.	Monitor the availability of quota in mailboxes, sites, etc., to use the organization storage wisely.	• Mailbox Over Warning Quota • Mailbox Size Over Time • Daily Overall Storage Used • Daily Quota Status • Shared Mailbox Size Over Time • Archived Mailbox Over Warning Quota • Mailbox Quota • SPO Site Over Warning Quota • Daily Site Storage • OneDrive Storage Over Time • OneDrive Overall Storage • Teams Over Warning Quota • Private Channels Over Warning Quota • Overall Storage Used by Office 365 Groups

3. Transmission Confidentiality and Integrity Ensure that the information transferred from the organization is protected from threats.	Keep an eye on connectors used in the Microsoft 365 to identify suspicious transmission of information.	**Mail Security Policy** • Inbound Connector • Outbound Connector
4. Trusted Path Enforce trusted communication between user and security functions of the information system.	Audit the conditional access policies enforced 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
5. External Malicious Code Identification Identify the malicious codes or URLs detected to protect your organization from various security threats.	Stay on top of external malware detections in your organization and take necessary actions instantly.	• Incoming External Malware Mails • Malware Engine Based Detections • Detonation Malware Detections • Reputation Malware Detections • File Based Malware Detections • URL Based Malware Detections • Campaign Malware Detections
6. Usage Restrictions Implement and restrict the use of certain devices and other services in the organization to avoid unintended modifications.	Track conditional access policies with their assignment details and device access policies to know the restrictions applied in the organization.	**CA Policy Configuration Analytics** • All CA policies • Recently modified CA policies • CA Policies with Grant Control details • CA Policies with Session Control details **Device Configurations** • Device Access Policy • Device Configurations • Device Tenant Configurations

MAPPING OF ADMINDROID REPORT CATEGORIES TO CONTROL GROUPS

The below mapping will help you to identify how various Microsoft 365 reporting fulfilling the ISO 27001 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 Information Location	- User added as admins - 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 Information Location	- Added applications - Consent to Applications - OAuth2 Permission grant - App role assignments
Directory Audit (Audit.AzureAD.DirectoryAudit)	Configuration Settings	- Domain Changes - Setting Changes
Policy Audit (Audit.AzureAD.PolicyAudit)	System Security and Privacy Plans Central Management	- Added Policy - Updated Policy

Device Audit (Audit.AzureAD.DeviceAudit)	Device Identification and Authentication Configuration Change Control Configuration Settings Information Location	• 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 Re-Authentication System Monitoring	• Failed to Pass MFA Challenge • 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 System Development Life Cycle	• User added as admins *(25 reports)*
External User Audit (Audit.Security.ExternalUserAudit)	Identifier Management	• Created External Users • Updated External Users • Deleted External Users • License/Plans Assignment

Mailbox Access (Audit.Exchange.MailboxAccess)	Least Privilege System Monitoring Information Location	• Mailbox Owner access • MFA Non-owner access • Mailbox Guest access
Mailbox Permission Changes (Audit.Exchange.MailboxPermissionChanges)	Information Location	• Mailbox Permission • SendAs Permission • Public Folder Permission • Folder Permission
Public Folder Audit (Audit.Exchange.MailboxPermissions)	Information in Shared System Resources	• Recently Added Public Folders • Mail Public Folders
Advanced Threat Protection (Audit.Exchange.ATP)	Incident Monitoring Configuration Change Control Spam Protection Memory Protection System Security and Privacy Plans Central Management	• Safe Attachment • Safe Link • Anti-Spam • Anti-Phishing • Anti-Config • Anti-Malware • Phishing Filter • Junk Email • DKIM Config • All ATP Activities
Role Changes (Audit.Exchange.RoleChanges)	Least Privilege Information Location	• Management role • 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 Use of External Systems	- Mobile Device Configs - Active Sync Configs - Text Message Configs
Data Loss Prevention (Audit.Exchange.DataLossPrevention)	Configuration Change Control System Security and Privacy Plans Central Management	- DLP Configs - Rule Matches

Spam Mails (Audit.Email.SpamMails)	Spam Protection Vulnerability Monitoring and Scanning	- Incoming External Spam Mails - Outgoing External Spam Mails - Internal Spam Mails
Phish Mails (Audit.Email.PhishMails)	Memory Protection Vulnerability Monitoring and Scanning	- Incoming External Phish Mails - Outgoing External Phish Mails - Internal Phish Mails
Spoof Mails (Audit.Email.SpoofMails)	Vulnerability Monitoring and Scanning	- External Spoof Mails - Internal Spoof Mails

Malware Mails (Audit.Email.MalwareMails)	Memory Protection Vulnerability Monitoring and Scanning External Malicious Code Identifications	• Incoming External Malware Mails • Outgoing External Malware Mails • Internal Malware Mails
By Malware Detections (Audit.Email.ByMalwareDetections)	External Malicious Code Identifications	• Malware Engine Based Detections • Detonation Malware Detections • Reputation Malware Detections • File Based Malware Detections • URL Based Malware Detections • Campaign Malware Detections

Site Collections (Audit.SharePoint.SiteCollections)	Least Privilege Information Location	• Admin Added • Admin Removed
Site Collection Configuration (Audit.SharePoint.SiteCollection Configuration)	Least Privilege	• Member Permissions Setting Changes • Disable Member Permissions Using Script
Site Collection Configuration (Audit.SharePoint.SiteCollection Configuration)	Identifier Management	• Groups Created • Groups Updated • Groups Deleted • Members Added • Members Removed • External User Added • External User Removed

Access Requests (Audit.SharePoint.AccessRequests)	Information Sharing Audit System Monitoring Information Location	• Requests Created • Requests Accepted • Requests Denied • Modified Files • Requests Updated • Access Requests Settings Modified • All Events
Sharing Invitations (Audit.SharePoint.SharingInvitations)	Information Sharing Audit System Monitoring Monitoring for Information Disclosure Information Location	• Invites Created • Invites Accepted • Invites Revoked • All Events • External User Invites
Secure Links (Audit.SharePoint.SecureLinks)	Account Usage Monitoring Information Sharing Audit Information Location	• Secure links created • Secure links used • Secure links deleted • Secure links updated • Added to secure link • Removed from secure link
File Access Activities (Audit.SharePoint.FileAccessActivities)	Information Sharing Audit Information Location	• All Events • Accessed Files • Access Extended Files
File Change Activities (Audit.SharePoint.FileChange Activities)	Spam Protection Memory Protection Vulnerability Monitoring and Scanning Information Management, Retention, and Refresh	• Malware detected files • Changed retention label
Page Activities (Audit.SharePoint.PageActivities)	Information Location	• Viewed pages • Page view extended • External users' activities

Site Permissions (Audit.SharePoint.SitePermissions)	Least Privilege	• Permission Level Added • Permission Level Removed • Permission Level Modified
Hub Site Activities (Audit.SharePoint.HubSiteActivities)	Least Privilege	• Hub Site Permission Sync Enabled • Hub Site Permission Sync Disabled

Administrative Changes (Audit.OneDrive.Administrative Changes)	Least Privilege Information Location	• Admins Added • Admins Removed
Groups (Audit.OneDrive.Groups)	Identifier Management	• Groups created • Groups updated • Members added • Members removed • External user added • External user removed
Secure Links (Audit.OneDrive.SecureLinks)	Account Usage Monitoring Information Sharing Audit Information Location	• Secure links created • Secure links used • Secure links deleted • Secure links updated • Added to secure link • Removed from secure link

Sharing Invitations (Audit.OneDrive.SharingInvitations)	Information Sharing Audit Monitoring for Information Disclosure Information Location	• Invites created • Invites accepted • Invites revoked • Invites blocked • Invites updated • Guest user expiration changed
File Access Activities (Audit.OneDrive.FileAccessActivities)	Information Location	• Accessed files • Access extended files
Page Activities (Audit.OneDrive.PageActivities)	Information Location	• Viewed pages • Page view extended
Site Permissions (Audit.OneDrive.SitePermissions)	Least Privilege	• Permission Level Added • Permission Level Removed • Permission Level Modified

Teams (Audit.Teams.Teams)	Unsuccessful Logon Attempts	• Login Activities
Teams Management (Audit.Teams.TeamsManagement)	Identifier Management	• Permission Level Added • Permission Level Removed • Permission Level Modified

Teams Apps Management (Audit.Teams.TeamsAppsManagement)	Flaw Remediation Software Usage Restrictions and User Installed Software	• Teams Installed Apps
Teams Membership Changes (Audit.Teams.TeamsMembershipChanges)	Identifier Management Information Location	• Member Added • Member Removed • Owners Added • Owners Removed • Ownership Promoted • Ownership Demoted
Private Channel Membership Changes (Audit.Teams.PrivateChannelMembershipChanges)	Identifier Management Information Location	• Member Added • Member Removed • Owners Added • Owners Removed • Ownership Promoted • Ownership Demoted
Add On Management (Audit.Teams.AddOnManagement)	Configuration Change Control	• Bots • Connectors • Tabs • All Activities

Threat Policy (Audit.Security&Compliance.ThreatPolicy)	Incident Monitoring Configuration Change Control Risk Assessment System Security and Privacy Plans Central Management	• Phishing Overrides • Spam Filtering • SecOps Mailbox Overrides

Mail Security Policy (Audit.Security&Compliance.MailSecurityPolicy)	Incident Monitoring Configuration Change Control Risk Assessment System Security and Privacy Plans Central Management Transmission Confidentiality and Integrity	• Quarantined Mail • Inbound Connector • Outbound Connector
Security and Alert Policy (Audit.Security&Compliance.SecurityandAlertPolicy)	Incident Monitoring System Security and Privacy Plans Central Management	• Malicious Links • Malicious Attachments • Activity Alerts • Protection Alerts • Malware Filters
eDiscovery (Audit.Security&Compliance.eDiscovery)	Least Privilege Information Location System Development Lifecycle	• eDiscovery Members • eDiscovery Case Admins
Audit Activities and Permissions (Audit.Security&Compliance.AuditActivitiesandPermissions)	Least Privilege Configuration Change Control Information Management, Retention, and Refresh System Security and Privacy Plans Central Management	• Assigning Roles to Bulk Users • Audit configuration • M365 audit log changes • Audit log retention
Information Protection Policy (Audit.Security&Compliance.InformationProtectionPolicy)	Configuration Change Control Risk Assessment System Security and Privacy Plans Central Management	• Auto-sensitivity labels • Sensitivity labels • Sensitivity label policies

Data Loss Prevention (Audit.Security&Compliance.DataLoss Prevention)	Configuration Change Control Risk Assessment System Security and Privacy Plans Central Management	• DLP policies • EDM schema • DLP sensitive info • Detection reports • Policy config • Policy tip config
Records Management (Audit.Security&Compliance.Records Management)	Information Management, Retention, and Refresh Configuration Change Control	• Retention tag • File plan configurations
Device Configurations (Audit.Security&Compliance.Device Configurations)	Access Control to Mobile Devices Use of External Systems Device Identification and Authentication Configuration Change Control Risk Assessment System Security and Privacy Plans Central Management Usage Restrictions	• Device Access Policy • Device Configurations • Device Tenant Configurations
Retention and Risk Analysis (Audit.Security&Compliance.Retention andRiskAnalysis)	Information Management, Retention, and Refresh Configuration Change Control Risk Assessment System Security and Privacy Plans Central Management	• Retention settings • App retention settings • Insider risk configurations • Organization segments • Communication compliance • Privacy management

OneNote Activities (Audit.OneNote.OneNoteActivities)	Information Location	- Accessed Notes
OneNote Section Activities (Audit.OneNote.OneNoteSectionActivities)	Information Location	- Section Accessed
Power BI & Microsoft Stream	Information Location	- PowerBI Viewing Activities - Stream Admin Role Changes

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 System Monitoring	- High severity - Medium severity - Low severity - Informational Alerts

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 - User Activity Count - Users Failed Activity Count
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 - O365 Audit Log Changes

Sharing & Access Audit.General.SharingAndAccess	Incident Analysis Information Sharing Audit Account Usage Monitoring Cross Organizational Auditing Monitoring for Information Disclosure System Monitoring Information Location	• 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 Users • 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 - Recently Created Admins
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 Information in Shared System Resources Resource Availability	- Shared mailbox size over time
Mailbox Usage (Stat.Exchange.MailboxUsage)	Account Usage Monitoring Resource Availability	- Mailbox Over Warning Quota - Mailbox size over time - Daily Overall Storage Used - Daily mailbox quota status - Archived mailbox over warning quota - Mailbox Quota
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 Use of External Systems	• 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
Mailbox Permissions (Stat.Exchange.MailboxPermissions)	Least Privilege System Monitoring	• 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
Mailboxes on Hold (Stat.Exchange.MailboxesonHold)	Information Management, Retention, and Refresh	• Mailboxes with Litigation Hold • Mailboxes with Retention Hold • Mailboxes with In-place Hold

Site Collections (Stat.SharePoint.Site)	Configuration Change Control Resource Availability	• Sharing Configs • SharePoint DLP Actions • Site Over Warning Quota

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 • By Last Activity Date
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
Site Usage Summary (Stat.SharePoint.SiteUsageSummary)	Resource Availability	• Daily Site Storage

Inactive Users (Stat.OneDrive.InactiveUsers)	Inactive Users	• By Last File Accessed • By Last File Synced • By Last External Share • By Last Internal Share • By Last Page Access
OneDrive Storage (Stat.OneDrive.OneDriveStorage)	Resource Availability	• Storage Over Time • Overall Storage

Daily Summary (Stat.OneDrive.DailySummary)	Account Usage Monitoring	• Daily Activities • User Activities • Active Users

Teams (Stat.Teams.Teams)	Resource Availability	• Teams Over Warning Quota • Private Channels Over Warning Quota
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 Organized Meeting • By Last Attended Meeting

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 Resource Availability	• Groups created via Teams • Groups created via Yammer • Groups created via SharePoint • Groups created via Stream • Groups created via Outlook • Groups with Hidden membership • Empty Groups • Overall Storage Used
Software Installs (Stat.General.SoftwareInstalls)	Software Usage Restrictions and User Installed Software	• Office activations • Project client • Visio client

Sign-ins (Anal.Sign-inAnal.Sign-ins)	Unsuccessful Logon Attempts Re-Authentication Security Function Verification Criticality Analysis	• Failed Sign-ins • Sign-ins in External Tenants

Risky Sign-ins (Anal.Sign-inAnal.RiskySign-Ins)	Criticality Analysis Incident Monitoring System 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 System 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 Criticality Analysis Vulnerability Monitoring and Scanning	• 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 Criticality Analysis	• 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 Vulnerability Monitoring and Scanning	• Risk Resolved Details • 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 Least Functionality Trusted Path Usage Restrictions	• All CA policies • Recently modified CA policies • CA Policies with Grant Control details • CA Policies with Session Control details

CA Policy Assignment Overview (Anal.CAP.PolicyAssignmentOverview)	Least Functionality	- All Policy Assignments - Policies with User Assignments - Policy with Group Assignments - Policy with Role Assignments - Policy with Application Assignments - Policies with Platform Assignments - Policies with Location Assignments - Policies with Devices Assignments
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

How can AdminDroid help implement other Security and Compliance requirements?

Apart from aligning with ISO 27001 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.

CJIS
HIPAA
PCI DSS
GLBA
SOX
ISO
GDPR
FISMA

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		