



FISMA Compliance

with

AdminDroid



AdminDroid

FISMA Compliance with AdminDroid



The **Federal Information Security Management Act (FISMA)** is a U.S Federal law passed in the year 2002 with the intention of strengthening information security in federal agencies. It made mandatory for all federal agencies and their contractors to set-up an information security and protection programme. It is a part of the E-Government Act of 2002 which made the United States take a step towards technology aided and enhanced governance.

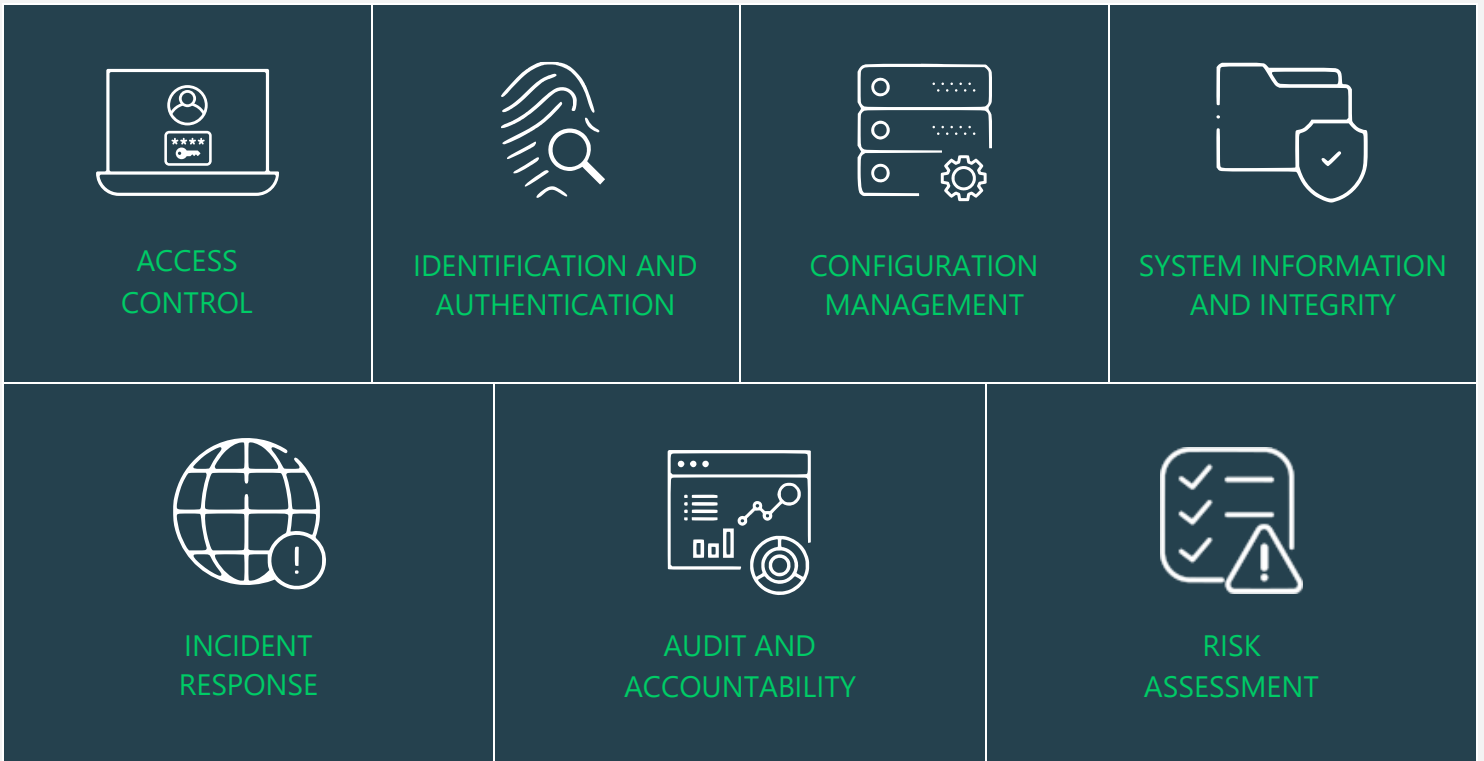
The **FISMA** Framework makes it mandatory for federal agencies to implement certain prescribed procedures to prove the reliability of their information system. By complying, the agencies have to identify and categorize the system and its various components based on security, following which an impact assessment is done to determine the appropriate security and privacy controls to be applied. The **National Institute of Standards and Technology (NIST)** was commissioned to develop the standards and guidelines for the mission.

The **Federal Information Security Modernization Act** of 2014 was signed in to reform the framework, so that **FISMA** addressed the evolving information technology and consequent security concerns. It largely addresses continuous compliance, monitoring and mitigation and periodic risk assessment and control evaluation.

CONTROL GROUPS

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

- [Access Control](#)
- [Identification and Authentication](#)
- [Configuration Management](#)
- [System and Information Integrity](#)
- [Incident Response](#)
- [Audit and Accountability](#)
- [Risk Assessment](#)



MAPPING OF FISMA COMPLIANCE CONTROL GROUPS AND REPORTS

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

- [Mapping of Control Groups to Report Collections](#)

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

- [Mapping of AdminDroid Report Categories to Control Groups](#)

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

- [Pre-compiled Report Bundle for FISMA Compliance](#)

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

MAPPING OF NIST SP 800-53 CONTROLS TO CONTROL FAMILIES

In the following table, key provisions of FISMA Provisions have been mapped to Control Families.

NIST SP 800-53 Controls	Control Containers
Family: Access Control	
<p>AC-2 Account Management</p> <ul style="list-style-type: none">a. Define and document the types of system accounts allowed for use within the system in support of organizational missions and business functions.b. Assign account managers for system accounts.c. Establish conditions for group and role membership.d. Specify authorized users of the system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create system accounts.f. Create, enable, modify, disable, and remove system accounts in accordance with [Assignment: organization-defined policy, procedures, and conditions].g. Monitor the use of system accounts;h. Notify account managers within [Assignment: organization-defined time-period for each situation]<ul style="list-style-type: none">1. When accounts are no longer required2. When users are terminated or transferred; and3. When individual system usage or need-to-know changes for an individual.i. Authorize access to the system based on:<ul style="list-style-type: none">1. A valid access authorization2. Intended system usage; and3. Other attributes as required by the organization or associated missions and business functions.j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency].k. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group; andl. Align account management processes with personnel termination and transfer processes.	<p style="text-align: center;"><u>Access Control</u></p>

<p>AC-3 Access Enforcement</p> <p>Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.</p> <p>AC-6 Least Privilege</p> <p>Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.</p>	<p>Access Control</p> <ul style="list-style-type: none"> Least Privilege
<p>AC-19 Access Control for Mobile Devices</p> <p>a. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.</p> <p>b. Authorize the connection of mobile devices to organizational systems and</p> <p>c. Protect and control mobile devices when outside of controlled areas.</p> <p>AC-20 Use of External Information Systems</p> <p>a. Access the information system from external information systems; and</p> <p>b. Process, store, or transmit organization-controlled information using external information systems.</p>	<p>Access Control</p> <ul style="list-style-type: none"> Access Control for Mobile Devices
<p>AC-21 Information Sharing</p> <p>a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for, and</p> <p>b. to assist users in making information sharing/collaboration decisions.</p>	<p>Access Control</p> <ul style="list-style-type: none"> Least Privilege
<p>Family: Identification and Authentication</p>	
<p>IA-2 Identification and Authentication (Organizational Users)</p> <p>Uniquely identify and authenticate organizational users or processes acting on behalf of organizational users.</p>	<p>Identification and Authentication</p> <ul style="list-style-type: none"> Identification and Authentication (Organizational Users)

<p>IA-3 Device Identification and Authentication</p> <p>Uniquely identify and authenticate [<i>Assignment: organization-defined specific and/or types of devices</i>] before establishing a [<i>Selection (one or more): local; remote; network</i>] connection.</p>	<p>Identification and Authentication</p> <ul style="list-style-type: none"> • Device Identification & Authentication
<p>IA-4 Identifier Management</p> <p>Manage system identifiers by:</p> <ol style="list-style-type: none"> Receiving authorization from [<i>Assignment: organization-defined personnel or roles</i>] to assign an individual, group, role, or device identifier. Selecting an identifier that identifies an individual, group, role, or device. Assigning the identifier to the intended individual, group, role, or device and Preventing reuse of identifiers for [<i>Assignment: organization-defined time-period</i>]. 	<p>Access Control</p> <ul style="list-style-type: none"> • Inactive Users <p>Identification and Authentication</p> <ul style="list-style-type: none"> • Identifier Management
<p>IA-5 Authenticator Management</p> <p>Manage system authenticators by:</p> <ol style="list-style-type: none"> Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator. Establishing initial authenticator content for any authenticators issued by the organization. Ensuring that authenticators have sufficient strength of mechanism for their intended use. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators. Changing/refreshing authenticators [<i>Assignment: organization-defined time-period by authenticator type</i>] Protecting authenticator content from unauthorized disclosure and modification. Requiring individuals to take, and having devices implement, specific security controls to protect authenticators; and Changing authenticators for group/role accounts when membership to those account changes. 	<p>Identification and Authentication</p> <ul style="list-style-type: none"> • Authenticator Management

Family: Audit and Accountability

AU-3 Content of Audit Records

The system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Microsoft 365 audit log provides all your required details for all the reports. You can refer a report attached below for better understanding.

- All activities

AU-6 Audit Review, Analysis and Reporting

a. Review and analyse system audit records [*Assignment: organization-defined frequency*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*].

b. Report findings to [*Assignment: organization-defined personnel or roles*] and

c. Adjust the level of audit review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Monitor the risk-based activities done in your organization and ensure that they are reported and handled appropriately.

- Data loss prevention
- Threat management
- Information governance
- Permissions
- Mail flow alerts
- Other alerts

AU-7 Audit Reduction and Report Generation

Provide and implement an audit reduction and report generation capability that:

a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and

b. Does not alter the original content or time ordering of audit records.

[Audit and Accountability](#)

- Report Generation and Audit Reduction

Family: Configuration Management

CM-3 Configuration Change Control

- a. Determine the types of changes to the system that are configuration-controlled.
- b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security impact analyses.
- c. Document configuration change decisions associated with the system.
- d. Implement approved configuration-controlled changes to the system.
- e. Retain records of configuration-controlled changes to the system for [*Assignment: organization-defined time-period*].
- f. Monitor and review activities associated with configuration-controlled changes to the system; and
- g. Coordinate and provide oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element*] that convenes [*Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]*].

Configuration Management

- Configuration Change Control

CM-5 Access Restrictions for Change

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

Configuration Management

- Access Restrictions for Change

CM-6 Configuration Settings

- a. Establish and document configuration settings for components employed within the system using [Assignment: organization-defined common secure configurations] that reflect the most restrictive mode consistent with operational requirements.
- b. Implement the configuration settings.
- c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and
- d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Configuration Management

- Configuration Change Control

Family: System and Information Integrity

SI-4 System Monitoring

- a. Monitor the system to detect:
 - 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives] and
 - 2. Unauthorized local, network, and remote connections.
- b. Identify unauthorized use of the system through [Assignment: organization-defined techniques and methods].
- c. Invoke internal monitoring capabilities or deploy monitoring devices:
 - 1. Strategically within the system to collect organization-determined essential information and,
 - 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization.
- d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
- e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation.

System and Information Integrity

- Information System Monitoring

<p>f. Obtain legal opinion regarding system monitoring activities and</p> <p>g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].</p>	
<p>SI-7 Software, Firmware and Information Integrity</p> <p>Employ integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].</p>	<p><u>System and Information Integrity</u></p> <ul style="list-style-type: none"> • Software Firmware and Information Integrity
<p>Family: Risk Assessment</p>	
<p>RA-1 Risk Assessment Policy and Procedures</p> <p>a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> 1. A risk assessment policy that: <ol style="list-style-type: none"> (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 2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls. <p>b. Designate an [Assignment: organization-defined senior management official] to manage the risk assessment policy and procedures.</p> <p>c. Review and update the current risk assessment:</p> <ol style="list-style-type: none"> 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency] <p>d. Ensure that the risk assessment procedures implement the risk assessment policy and controls; and</p> <p>e. Develop, document, and implement remediation actions for violations of the risk assessment policy.</p>	<p><u>Risk Assessment</u></p> <ul style="list-style-type: none"> • Policy and Procedures

RA-3 Risk Assessment

- a. Conduct a risk assessment, including the likelihood and magnitude of harm, from:
 - 1. The unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
 - 2. Privacy-related problems for individuals arising from the intentional processing of personally identifiable information;
- b. Integrate risk assessment results and risk management decisions from the organization and missions/business process perspectives with system-level risk assessments;
- c. Document risk assessment results in [Selection: security and privacy plans; risk assessment report; [Assignment: organization-defined document]];
- d. Review risk assessment results [Assignment: organization-defined frequency];
- e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; and
- f. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its Risk Assessment Risk Assessment environment of operation, or other conditions that may impact the security or privacy state of the system.

[Risk Assessment](#)

- Risk Assessment

RA-7 Risk Response

Risk assessment Risk Response Respond to findings from security and privacy assessments, monitoring, and audits.

[Risk Assessment](#)

- Risk Response

<p>RA-9 Criticality Analysis</p> <p>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].</p>	<p>Risk Assessment</p> <ul style="list-style-type: none"> Criticality Analysis
<p>Family: Incident Response</p>	
<p>IR-5 Incident Monitoring</p> <p>Track and document system security and privacy incidents.</p>	<p>Incident Response</p> <ul style="list-style-type: none"> Incident Monitoring Incident Analysis
<p>IR-9 Information Spillage Response</p> <p>Alerting [Assignment: Organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill.</p>	<p>Monitor the DLP activities to prevent the information spill and ensure that the respective person gets alerted if any spill happens in the organization.</p> <ul style="list-style-type: none"> DLP rule matched mails SharePoint DLP rule matches SharePoint DLP rule undo Data loss prevention alerts SharePoint IRM enabled lists SharePoint IRM enabled document libraries

MAPPING OF CONTROL GROUPS TO REPORT COLLECTIONS

The below mapping will help you to find out the various FISMA 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 <ul style="list-style-type: none">• All users• All External Users• Internal Guest Users Group Reports <ul style="list-style-type: none">• All Groups• Groups Created via Teams• Groups Created via Yammer• Groups Created via SharePoint• Empty Groups• Groups with Hidden membership
	Account Details Monitoring Monitor and review the details of and changes made to user accounts in your Microsoft 365 Environment to spot deviations from your Account Management Policies and Procedures.	User details Reports <ul style="list-style-type: none">• Created Users• Deleted users• All User Events• Enabled Users• Disabled Users User account Changes Reports <ul style="list-style-type: none">• Updated Users• License Changes• Recent password Changes User Managers Reports <ul style="list-style-type: none">• Managers & Direct Reports• Users with Managers• Users without Managers

Account Usage Monitoring

Review user activity across all Microsoft 365 services.

Overall Activities

- All Activities
- Admin Activities
- Top Activity Summary
- Daily Activity Summary
- Activity by Department
- Activity by City
- Activity by State
- Activity by Country
- Activity by JobTitle
- Activity by Company

Sharing & Access

- All file/folder sharing activity
- All file/folder access activity
- Files shared by External users
- Files shared to External users
- File/Folder accesses by External Users
- File Deletion
- Anonymous link creation
- Anonymous link accessed
- Files shared via Teams Channels
- Files shared by External Users in Channels
- Files shared via 1:1 chat
- Files shared to External Users 1:1 chat

OneDrive User Activities

- Daily User Activities
- User Activities
- Active Users

Teams User Activities

- Daily Activities
- Overall Activities

Yammer User Activities

- Daily Activities
- Overall Activities

Skype User Activities

- Peer-to-Peer Sessions
- Organized Conferences
- Participated Conferences
- File Transfers
- Instant Messages

		<p>SharePoint Activities</p> <ul style="list-style-type: none"> • 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 <p>Resource Usage by User Accounts</p> <ul style="list-style-type: none"> • Mailbox size over time • Daily mailbox quota status • Shared mailbox size over time • Archived mailbox over warning quota • Daily Site Storage • OneDrive Overall Storage <p>License & Subscription Usage</p> <ul style="list-style-type: none"> • Daily Activities • Subscription Usage • Unused Subscriptions • Licensed Users • Regain Licenses
	<p>Inactive Users</p> <p>Identify inactive user accounts across all Microsoft 365 services to take decisions on termination of license or access.</p>	<p>Exchange Inactive Users</p> <ul style="list-style-type: none"> • By Last Mail Read • By Last Mail Sent • By Last Mail Received <p>SharePoint Inactive Users</p> <ul style="list-style-type: none"> • By Last File Access • By Last File Synced • By Last External Share • By Last Internal Share • By Last Page Access <p>OneDrive Inactive Users</p> <ul style="list-style-type: none"> • By Last File Accessed • By Last Internal Share • By Last External Share • By Last File Synced <p>Teams Inactive Users</p> <ul style="list-style-type: none"> • By Last Team Chat • By Last Private Chat • By Last Call Activity • By Last Meeting Activity

		<p>Yammer Inactive Users</p> <ul style="list-style-type: none"> • By Last Post Liked • By Last Post Posted • By Last Post Read • By Last Activity <p>Active Users Statistics</p> <ul style="list-style-type: none"> • 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
<p>2. Least Privilege</p> <p>Maintain the principle of least privilege while assigning access permissions and privileged roles.</p>	<p>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.</p>	<p>User License Reports</p> <ul style="list-style-type: none"> • Licensed Users • Users by Subscriptions • Unlicensed Users • Free Users • Trial Users <p>Admin Reports</p> <ul style="list-style-type: none"> • All Admins • Admin roles by user • User Added as Admins <i>(25 Reports)</i> • All Global Admins • Admins with Management Roles • Admins with Read Access Roles <p>Admin Role Changes</p> <ul style="list-style-type: none"> • Role Assignments • Role Scope Changes • Added Roles • Updated Roles <p>Role Configuration Changes</p> <ul style="list-style-type: none"> • Management Role • Role Assignments • Assignments Policy • Role Entry • Role Group • Role Scope <p>Mailbox Access</p> <ul style="list-style-type: none"> • Mailbox Non-Owner Access <p>Mailbox Permissions</p>

		<ul style="list-style-type: none"> • Access to Others Mailboxes • Mailbox Permission Summary • Mailbox Permission Detail • Mailbox with SendOnBehalf • Send As Permission • Full Permission • Read Permission • Guests' Mailbox Permission Summary • Admins Access to Others Mailboxes • Admins with Send-on-Behalf • Admins with Send-As • Admins with Full Access • Guests Access to Others Mailboxes
<p>3. Unsuccessful Logon Attempts</p> <p>Monitor unsuccessful attempts to logon to your information system accounts.</p>	<p>Monitor for and review failed logon attempts to accounts in your Microsoft 365 Environment to take further action.</p>	<p>User Failed Logins</p> <ul style="list-style-type: none"> • Failed User Logins • Users' Login Failure Summary • Failed Sign-ins • Failed logins in MFA challenge <p>Teams</p> <ul style="list-style-type: none"> • Login Activities <p>Admins Failed Logins</p> <ul style="list-style-type: none"> • Admins' Login Failure • Admins' Login Failure Summary
<p>4. Previous Logon (Access) Notification</p> <p>Audit the Previous logon time of the Microsoft 365 users.</p>	<p>Track the last logon time of the users to identify the location, IP address, and more for security requirements.</p>	<p>Last Logon Report</p> <ul style="list-style-type: none"> • 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

<p>5. Access Control for Mobile Devices</p> <p>Authorize and audit the mobile devices connected to your organization’s information system.</p>	<p>Identify and review the mobile devices used by your users to access key Microsoft 365 services to ensure that no unauthorized devices are used.</p>	<p>Mobile Device Reports</p> <ul style="list-style-type: none"> • 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 <p>Mobile Device Configuration Changes</p> <ul style="list-style-type: none"> • Mobile Device Configs • Active Sync Configs • Text Message Settings
<p>6. Information Sharing Audit</p> <p>Audit the information sharing activities to permit only the authorized users to share and access the information.</p>	<p>Supervise the sharing & access data to secure the sensitive info from the unauthorized users and for post breach investigation.</p>	<p>Sharing & Access Activities</p> <ul style="list-style-type: none"> • 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 <p>SharePoint Access Requests Reports</p> <ul style="list-style-type: none"> • Requests Created • Requests Accepted • Requests Denied • All Events <p>SharePoint Sharing Invitations Reports</p> <ul style="list-style-type: none"> • Invites Created • Invites Accepted • Invites Revoked • All Events • External User Invites

IDENTIFICATION AND AUTHENTICATION

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

Control	Microsoft 365 Centric Control Implementation	Applicable AdminDroid Reports
<p>1. Identification and Authentication (Organizational users)</p> <p>Audit and review the identification and authentication processes for users.</p>	<p>Review user account data in Azure Active Directory to check whether:</p> <p>a. All people listed in your organization who possess a valid business reason to access your Microsoft 365 Environment are assigned an account, and</p> <p>b. To identify user accounts which cannot be tracked to an individual.</p> <p>Review the authentication requirements imposed on users to verify that all accounts of the users are protected in line with your organization's policy.</p>	<p style="text-align: center;">Office 365 users</p> <p>MFA Reports</p> <ul style="list-style-type: none"> • Users with MFA • MFA Activated Users • Users' MFA details <p>MFA Configured Policies Analytics</p> <ul style="list-style-type: none"> • Policies with MFA • MFA Policies Assignment Overview • MFA Policies Assignment Details <p>CA Policy Assignment Details analytics</p> <ul style="list-style-type: none"> • Password policies Reports • Policies with User Assignments • User conditions on Access Policies • Guest/External user conditions on Access Policies <p>Password Reports</p> <ul style="list-style-type: none"> • 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

<p>2. Device Identification and Authentication</p> <p>Review and audit the identification processes for devices in information system.</p>	<p>Review device additions, modifications, deletions, and other such activity to spot any unauthorized changes.</p>	<p>Mobile Devices</p> <ul style="list-style-type: none"> • All Mobile Devices • Devices by Connected Mailbox • Mobile Devices by OS • Mobile Devices by Client type • Mobile Devices by Access State <p>Device Audit</p> <ul style="list-style-type: none"> • Added Devices • Updated Devices • Deleted Devices • Owner changes • User changes • Credential changes • All Device Operations • Sign-ins with Device details • Mobile Sign-ins • Non-compliant Device sign-ins • Unmanaged Device sign-ins
<p>3. Identifier Management</p> <p>Audit the provisioning, modification and deprovisioning of users and groups.</p>	<p>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.</p>	<p>User Audit</p> <ul style="list-style-type: none"> • Created Users • Updated Users • License Changes • Deleted Users <p>Group Audit</p> <ul style="list-style-type: none"> • Created Groups • Deleted Groups • Updated Groups • Group Member Changes <p>Mailbox Info</p> <ul style="list-style-type: none"> • All Mailboxes • Shared Mailboxes • Archived Mailboxes
<p>4. Authenticator Management</p> <p>Audit the changes to authenticators by users and administrators for policy compliance and review changes to authentication policies.</p>	<p>Audit the changes to passwords effected by users and administrators to spot any unauthorized or inappropriate modifications.</p>	<p>Password Reports</p> <ul style="list-style-type: none"> • Password never expire users • Password never changed • Recent Password changers • Password not changed in 90 days • Users with weak password allowed <p>Password Changes</p> <ul style="list-style-type: none"> • User Password Changes • Password Reset by Admin • Forced/Expired Password resets • Reset Forced by Admin • All Password Changes

<p>5. Re-Authentication</p> <p>Monitor logins to your information system to identify cases such as password expiry that need action.</p>	<p>Monitor failed login attempts to your Microsoft 365 Environment to look out for issues that need administrative help.</p>	<p>User Logins</p> <ul style="list-style-type: none"> Failed User Logins Failed Sign-ins Failed in MFA challenge
---	--	--

AUDIT AND ACCOUNTABILITY

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

Control	Microsoft 365 Centric Control Implementation	Applicable AdminDroid Reports
<p>1. Audit Events</p> <p>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.</p>	<p>Collect information that answers the What, who, when and where questions about events across all services in your Microsoft 365 Environment.</p>	<p>Office 365 Workload Based Activities</p> <ul style="list-style-type: none"> Azure AD Activities Exchange Activities SharePoint Activities OneDrive Activities OneNote Activities Power BI Activities Teams Activities Stream Activities Security & Compliance Compliance Search Activities
<p>2. Audit Review, Analysis and Reporting</p> <p>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.</p>	<p>Review your audit trail across all services of your Microsoft 365 Environment.</p>	<p>Office 365 Workload Based Activities</p> <ul style="list-style-type: none"> Azure AD Activities Exchange Activities SharePoint Activities OneDrive Activities OneNote Activities Power BI Activities Teams Activities Stream Activities Security & Compliance Compliance Search Activities

		<p>Audit Settings</p> <ul style="list-style-type: none"> • Audit Enabled • Audit Disabled • Admin Audit Enabled • Owner audit Enabled • Delegate audit Enabled
	<p>Export the audit trail in a format of your choice for reporting inappropriate activity to the designated personnel.</p>	<p>Export the audit report in a range of formats including PDF and Microsoft Excel using the Export Feature.</p>
<p>3. Report Generation and Audit Reduction</p> <p>Provide summary reports to support on demand audit review, analysis and reporting requirements and investigation requirements without altering the audit log.</p>	<p>Review detailed visualizations of audit trail data to easily spot anomalous behaviour without having to go through the raw audit information.</p>	<ul style="list-style-type: none"> • Dashboard.Audit • Dashboard.AzureAD • Dashboard.Security • Dashboard.Exchange • Dashboard.UsageandAdoption
<p>4. Non-Repudiation</p> <p>Monitor and record user activity in your information system to counter claims of repudiation.</p>	<p>Configure alerts on suspicious user activity in your Microsoft 365 Environment to ensure non-repudiation.</p>	<p>All User Summary</p> <ul style="list-style-type: none"> • All user summary by activity

<p>5. Cross-organizational Auditing</p> <p>Audit the activity of extra- or cross-organizational users and processes in your Microsoft 365 Environment.</p>	<p>Audit the activity of external users across Microsoft 365 services to look out for any suspicious events.</p>	<p>Overall External user summary</p> <ul style="list-style-type: none"> • External User summary by activity • External User summary by activity type • External User summary by alert policy name • External User summary by security • External User summary by category • External User summary by policy type • External User summary system alerts
---	--	--

SYSTEM AND INFORMATION INTEGRITY

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

Control	Microsoft 365 Centric Control Implementation	Applicable AdminDroid Reports
<p>1. Flaw Remediation</p> <p>Identify, report, and correct the flaws in software and firmware for the organizations' Security.</p>	<p>Monitor the added or updated applications in your organization to test and remediate the flaws.</p>	<p>Application Audit</p> <ul style="list-style-type: none"> • Added Applications • Updated Applications
<p>2. Software, Firmware, and Information Integrity</p> <p>Employ integrity verification schemes to detect unauthorized changes to your information system.</p>	<p>Review the secure score of Microsoft 365 services to understand the security and integrity status of your Microsoft 365 Environment.</p>	<p>Overall (Secure score)</p> <p>AdminDroid offers more detailed Secure Score Reports for each Microsoft 365 service.</p> <ul style="list-style-type: none"> • 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

<p>3. Information System Monitoring</p> <p>Monitor your information system to detect indicators of potential attacks and unauthorized activity.</p>	<p>Review audit data in your Microsoft 365 Environment across services with a focus on the risk laden areas to detect any anomalies.</p>	<p>All Low-Level Reports (The Advanced Search Tool helps you in zeroing in on the exact report you need)</p> <p>Overall Activities</p> <ul style="list-style-type: none"> • Admin Activities • All Failed Activities • All Activities <p>Office 365 Workload Based Activities</p> <ul style="list-style-type: none"> • Azure AD Activities • Exchange Activities • SharePoint Activities • OneDrive Activities • OneNote Activities • Power BI Activities • Teams Activities • Stream Activities • Security and Compliance • Compliance Search Activities
<p>4. Security Alerts, Advisories and Directives</p> <p>Receive, generate, and disseminate alerts and advisories on your information system whenever deemed necessary.</p>	<p>Configure alerts and review them based on their severity in your Microsoft 365 Environment whenever and wherever they come up.</p>	<p>Alert Severity</p> <ul style="list-style-type: none"> • High severity • Medium severity • Low Severity <p>Alert Category</p> <ul style="list-style-type: none"> • Data Loss Prevention • Threat Management • Information Governance • Permissions • Mail Flow • Others
<p>5. Security Function Verification</p> <p>Verify the security operation of your information system and notify whenever any security verification test failure takes place.</p>	<p>Monitor for and review security verification failures such as failed login attempts in your Microsoft 365 Environment.</p>	<p>User Logins</p> <ul style="list-style-type: none"> • Failed User Logins • Users' Login Failure Summary <p>MFA Reports</p> <ul style="list-style-type: none"> • MFA Non-Activated Users • Failed Sign-ins • Failed in MFA challenge • MFA Disabled

<p>6. Spam Protection</p> <p>Employ and regularly update spam protection features in your information system.</p>	<p>Monitor and regularly review the quantity and content of spam mail received by your Microsoft 365 Environment.</p>	<p>Advanced Threat Protection</p> <ul style="list-style-type: none"> • Anti-Spam • Spam Mails Received • Spam Mails Sent/Received
<p>7. Memory Protection</p> <p>Identify any malware or phishing attacks in your organization to protect the memory locations.</p>	<p>Track and review the malware and phishing details regularly in your Microsoft 365 environment.</p>	<p>Advanced Threat Protection</p> <ul style="list-style-type: none"> • Anti-Malware • Phishing filter • Anti-Phishing • Malware Mails Received

INCIDENT RESPONSE

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

Control	Implementation of Control in Microsoft 365	Applicable AdminDroid Reports
<p>1. Incident Monitoring</p> <p>Monitor and detect security incidents in your information system in a timely manner.</p>	<p>Review user and administrator activity such as login failures to spot any suspicious events which could lead to a security incident.</p>	<p>Risky Login Attempts</p> <ul style="list-style-type: none"> • 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 <p>Risky Sign-ins</p> <ul style="list-style-type: none"> • Confirmed Risky Sign-ins • Open Risky Sign-ins <p>Password Changes</p> <ul style="list-style-type: none"> • User password changes • Self-service password resets

		<p>Risky Sign-ins by Risk Level</p> <ul style="list-style-type: none"> • High Risky Sign-ins • Medium Risky sign-ins • Low Risky sign-ins • Hidden Risky sign-ins <p>Sign-ins with Prompts</p> <ul style="list-style-type: none"> • Strong Auth Enrollment Prompted Sign-ins • Signed-in via Alternate Auth Method • Password reset Prompts • Multiple O365 Accounts Prompts • Keep Me Signed-in Prompts <p>Administrative Users Reports</p> <ul style="list-style-type: none"> • User added as admins
	<p>Identify information security hazards to your Microsoft 365 Environment and review their status until closure.</p>	<p>Advance Threat Protection</p> <ul style="list-style-type: none"> • Safe Attachment • Safe Link • Anti-Spam • Anti-Malware • Phishing Filter • Junk Email • DKIM Config • All ATP Activities • Anti-Phishing • ATP Config
<p>2. Incident Analysis</p> <p>Analyse and investigate the events and activity deemed anomalous in your information system.</p>	<p>Analyse the security incident to understand its impact on your Microsoft 365 Environment and determine the appropriate response.</p>	<p>Overall Activities</p> <ul style="list-style-type: none"> • All Activities • Admin Activities • All Failed Activities <p>Sharing & Access</p> <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • Azure AD Activities • Exchange Activities • SharePoint Activities • OneDrive Activities • OneNote Activities • Power BI Activities • Teams Activities • Stream Activities • Security and Compliance • Compliance Search Activities
3. Information Spillage Response Identify, alert, isolate and eradicate the contamination in your information system.	Configure alerts in your Microsoft 365 Environment to identify any suspicious activity that may lead to an information breach.	Alert Category <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • Device Config changes Advance Threat Protection <ul style="list-style-type: none"> • Safe attachment • Safe link • Anti-Spam • Anti-Malware • Phishing Filter • Junk Email • DKIM Config • All ATP Activities • Anti-phishing • ATP config

		<p>Mobile Device Audit</p> <ul style="list-style-type: none"> • Mobile Device Configs • Active Sync Configs • Text Message Settings <p>Data Loss Prevention</p> <ul style="list-style-type: none"> • DLP Configs <p>Mail Flow</p> <ul style="list-style-type: none"> • Mail Flow Configs • Connector Configs • Accepted Domains • Remote Domain • Hybrid Configs • Federation Configs <p>Add On Management</p> <ul style="list-style-type: none"> • Bots • Connectors • Tabs • All Activities <p>Site Collections</p> <ul style="list-style-type: none"> • SharePoint Sharing Configs • SharePoint DLP Actions
<p>2. Access Restrictions for Change</p> <p>Establish and enforce logical access restrictions associated with changes to the information system.</p>	<p>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.</p>	<p>Admin Reports</p> <ul style="list-style-type: none"> • All admins • Admin Roles by Users • All Global Admins • Admins with Management Roles • Admins with Read Access Roles <p>Overall Activities</p> <ul style="list-style-type: none"> • All activities • Admin Activities • All Failed Activities <p>Admin Role Changes</p> <ul style="list-style-type: none"> • All Role Member Changes • Role Assignments • Role Scope Changes • All Role Operations

<p>3. Configuration Settings</p> <p>Monitor for changes to the configuration settings of the IT Products within your information system.</p>	<p>Monitor and identify the changes to the configuration of your Microsoft 365 Environment to make sure that no unauthorized changes are made.</p>	<p>Device Audit</p> <ul style="list-style-type: none"> • Device Config Changes <p>Directory Audit</p> <ul style="list-style-type: none"> • Directory Setting Changes • Domain Changes
<p>4. Software Usage Restrictions and User Installed Software</p> <p>Enforce software installation policies and monitor their effective implementation in your information system.</p>	<p>Monitor applications added through Azure Active Directory to ensure that they follow your organization's software installation policies.</p>	<p>Software Installs</p> <ul style="list-style-type: none"> • Office activations • Project client • Visio client • Activations user Counts • Activation Counts <p>Application Audit</p> <ul style="list-style-type: none"> • Added applications • Consent to applications • OAuth2 permission grant

RISK ASSESSMENT

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

Control	Implementation of Control in Microsoft 365	Applicable AdminDroid Report
<p>1. Policy and Procedures</p> <p>a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:</p> <p>(i) [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that</p> <p>a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</p> <p>b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and</p> <p>(ii) Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;</p> <p>b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and</p> <p>c. Review and update the current risk assessment:</p>	<p>Monitor all the security related policies and its conditions configured in your Microsoft 365 environment.</p>	<p>CA Policy Configuration Analytics</p> <ul style="list-style-type: none"> • All CA policies • Recently modified CA policies • CA Policies with Grant Control details • CA Policies with Session Control details <p>CA Policy Assignment Details analytics</p> <ul style="list-style-type: none"> • 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

<p>(i) Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and</p> <p>(ii) Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].</p>		<p>MFA Configured Policies Analytics</p> <ul style="list-style-type: none"> • Policies with MFA • MFA policies Assignment Overview • MFA policies Assignment Details
<p>2. Risk Assessment</p> <p>a. Conduct a risk assessment, including:</p> <p>(i) Identifying threats and vulnerabilities in the system.</p> <p>b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments.</p> <p>c. Review risk assessment results [Assignment: organization-defined frequency].</p> <p>d. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles].</p> <p>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</p>	<p>Review all the risky logins with its details detected by the security policies.</p>	<p>Risky Sign-ins by Risk Level</p> <ul style="list-style-type: none"> • High Risky Sign-ins • Medium Risky Sign-ins • Low Risky Sign-ins • Hidden Risky Sign-ins <p>Risky Sign-ins by Detection Timing</p> <ul style="list-style-type: none"> • Real Time Risk Detections • Near Real Time Risk Detections • Offline Risk Detections <p>Risky Sign-ins by Risk Event Type</p> <ul style="list-style-type: none"> • 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

<p>3. Risk Response</p> <p>Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.</p>	<p>Monitor all the responses taken by the users for the risky activities detected in the organization.</p>	<p>Risky Sign-ins by Risk Resolved Method</p> <ul style="list-style-type: none"> • 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 <p>Risky Sign-ins by Risk Status</p> <ul style="list-style-type: none"> • Marked As Safe • Marked As Remediated • Marked As Dismissed • Marked As Compromised
<p>4. Criticality Analysis</p> <p>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].</p>	<p>Identify and analyse all the critical resources to secure your organization from unauthorized access or data breach.</p>	<p>Risky Sign-ins</p> <ul style="list-style-type: none"> • Confirmed Risky Sign-ins • Open Risky Sign-ins • Admin Confirmed User Compromised • Risk Status Marked as Compromised <p>Sign-ins with Prompts</p> <ul style="list-style-type: none"> • Strong Auth Enrollment Prompted Sign-ins • Signed-in Via Alternate Auth Method • Password reset Prompts • Multiple O365 Accounts Prompts • Keep Me Signed-in Prompts

MAPPING OF ADMINDROID REPORT CATEGORIES TO CONTROL GROUPS

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

Report Category	Control Groups	Applicable AdminDroid Reports
<p>User Logins (Audit.AzureAD.UserLogins)</p>	<p>Unsuccessful Logon Attempts Previous Logon (Access) Notification Re-Authentication Security Function Verification</p>	<ul style="list-style-type: none"> • 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
<p>Password Changes (Audit.AzureAD.PasswordChanges)</p>	<p>Authenticator Management Account Management Audit</p>	<ul style="list-style-type: none"> • User Password Changes • Password Reset by Admin • Forced/Expired Password Reset • Forced by Admin • All Password Changes
<p>User Audit (Audit.AzureAD.UserAudit)</p>	<p>Account Management Audit Identifier Management</p>	<ul style="list-style-type: none"> • Created Users • Updated Users • License Changes • Deleted Users • All User Events

<p>Group Audit (Audit.AzureAD.GroupAudit)</p>	<p><u>Identifier Management</u></p>	<ul style="list-style-type: none"> • Created Groups • Deleted Groups • Updated Groups • Group Member Changes
<p>Admin Role Changes (Audit.AzureAD.AdminRole)</p>	<p><u>Account Management Audit</u> <u>Access Restrictions for Change</u></p>	<ul style="list-style-type: none"> • All Role Member Changes • All Role Operations • Role Assignments • Role Scope Changes • Deleted Roles • Updated Roles • Added Roles
<p>Application Audit (Audit.AzureAD.ApplicationAudit)</p>	<p><u>Software Usage Restrictions and User Installed Software</u></p>	<ul style="list-style-type: none"> • Added applications • Consent to Applications • OAuth2 Permission grant
<p>Directory Audit (Audit.AzureAD.DirectoryAudit)</p>	<p><u>Configuration Settings</u></p>	<ul style="list-style-type: none"> • Domain Changes • Setting Changes
<p>Device Audit (Audit.AzureAD.DeviceAudit)</p>	<p><u>Device Identification and Authentication</u> <u>Configuration Change Control</u> <u>Configuration Settings</u></p>	<ul style="list-style-type: none"> • 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

<p>Risky Login Attempts (Audit.Security.RiskyLoginAttempts)</p>	<p>Incident Monitoring Unsuccessful Logon Attempts</p>	<ul style="list-style-type: none"> Failed to Pass MFA Legacy/Basic Auth Attempt Challenge Expired Password Login Attempts Admin's Login Failures Admin's Login Failure Summary Disabled User Login Attempts Failed Sign-ins Failed in MFA challenge
<p>Administrative Users Reports (Audit.Security.UserAddedAsAdmins)</p>	<p>Least Privilege</p>	<ul style="list-style-type: none"> User added as admins <i>(25 reports)</i>

<p>Mailbox Access (Audit.Exchange.MailboxAccess)</p>	<p>Least Privilege</p>	<ul style="list-style-type: none"> MFA Non-owner access
<p>Mailbox Permissions (Audit.Exchange.MailboxPermissions)</p>	<p>Least Privilege</p>	<ul style="list-style-type: none"> 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

<p>Advanced Threat Protection (Audit.Exchange.ATP)</p>	<p><u>Incident Monitoring</u> <u>Configuration Change Control</u> <u>Spam Protection</u> <u>Memory Protection</u></p>	<ul style="list-style-type: none"> • Safe Attachment • Safe Link • Anti-Spam • Anti-Phishing • Anti-Config • Spam Mails Received • Spam Mails Sent/Received • Anti-Malware • Phishing Filter • Junk Email • DKIM Config • All ATP Activities
<p>Role Changes (Audit.Exchange.RoleChanges)</p>	<p><u>Least Privilege</u></p>	<ul style="list-style-type: none"> • Management • Role Assignments • Assignments Policy • Role Entry • Role Scope • Role group
<p>Mail Flow (Audit.Exchange.MailFlow)</p>	<p><u>Configuration Change Control</u></p>	<ul style="list-style-type: none"> • Mail Flow Configs • Transport Rules • Connector Configs • Accepted Domains • Remote Domain • Hybrid Configs • Federation Configs
<p>Mobile Device Audit (Audit.Exchange.MobileDevice)</p>	<p><u>Access Control for Mobile Devices</u> <u>Configuration Change Control</u></p>	<ul style="list-style-type: none"> • Mobile Device Configs • Active Sync Configs • Text Message Configs
<p>Data Loss Prevention (Audit.Exchange.DataLossPrevention)</p>	<p><u>Configuration Change Control</u></p>	<ul style="list-style-type: none"> • DLP Configs • Rule Matches

<p>Access Requests (Audit.SharePoint.AccessRequests)</p>	<p>Information Sharing Audit</p>	<ul style="list-style-type: none"> • Requests Created • Requests Accepted • Requests Denied • Modified Files
<p>Sharing Invitations (Audit.SharePoint.SharingInvitations)</p>	<p>Information Sharing Audit</p>	<ul style="list-style-type: none"> • Invites Created • Invites Accepted • Invites Revoked • All Events • External User Invites
<p>File Activities (Audit.SharePoint.FileActivities)</p>	<p>Information Sharing Audit</p>	<ul style="list-style-type: none"> • All Events

<p>Teams (Audit.Teams.Teams)</p>	<p>Unsuccessful Logon Attempts</p>	<ul style="list-style-type: none"> • Login Activities
<p>Add On Management (Audit.Teams.AddOnManagement)</p>	<p>Configuration Change Control</p>	<ul style="list-style-type: none"> • Bots • Connectors • Tabs • All Activities

<p>All User Summary (Audit.Alerts.AllUserSummary)</p>	<p>Non-Repudiation</p>	<ul style="list-style-type: none"> • All user summary by activity
--	--	--

<p>External User Summary (Audit.Alerts.ExternalUserSummary)</p>	<p>Cross-organizational Auditing</p>	<ul style="list-style-type: none"> • 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 category • External user summary by policy type • External user summary system alerts
<p>Alert Severity (Audit.Alerts.AlertSeverity)</p>	<p>Security Alerts, Advisories and Directives</p>	<ul style="list-style-type: none"> • High severity • Medium severity • Low severity
<p>Alert Category (Audit.Alerts.AlertCategory)</p>	<p>Security Alerts, Advisories and Directives Information Spillage Response</p>	<ul style="list-style-type: none"> • Data Loss Prevention • Threat Management • Information Governance • Permissions • Mail flow • Others
<p>Overall (Audit.SecureScore.Overall)</p>	<p>Software, Firmware and Information Integrity</p>	<ul style="list-style-type: none"> • 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

<p>Overall Activities (Audit.General.Overall)</p>	<p><u>Account Usage Monitoring</u> <u>Information System Monitoring</u> <u>Incident Analysis</u> <u>Access Restrictions for Change</u></p>	<ul style="list-style-type: none"> • Admin Activities • All Failed Activities • All Activities • Top Activity Summary • Daily activity summary • Activity by Department • Activity by City • Activity by State • Activity by Country • Activity by JobTitle • Activity by Company
<p>Office 365 Workload Based Activities (Audit.General.O365WBA)</p>	<p><u>Audit Events</u> <u>Audit Review Analysis & Reporting</u> <u>Information System Monitoring</u> <u>Incident Analysis</u></p>	<ul style="list-style-type: none"> • Azure AD Activities • Exchange Activities • SharePoint Activities • OneDrive Activities • OneNote Activities • Power BI Activities • Teams Activities • Stream Activities • Security and Compliance • Compliance Search Activities
<p>Sharing & Access Audit.General.SharingAndAccess</p>	<p><u>Incident Analysis</u> <u>Information Sharing Audit</u></p>	<ul style="list-style-type: none"> • 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

<p>User Reports (Stat.AzureAD.UserReports)</p>	<p><u>Account Management Audit</u> <u>Identification and authentication</u> <u>(Organizational Users)</u></p>	<ul style="list-style-type: none"> • 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
<p>License Reports (Stat.AzureAD.LicenseReports)</p>	<p><u>Least Privilege</u></p>	<ul style="list-style-type: none"> • Licensed Users • Users by Subscriptions • Unlicensed Users • Free Users • Trial Users
<p>Group Reports (Stat.AzureAD.Group)</p>	<p><u>Account Type Monitoring</u></p>	<ul style="list-style-type: none"> • All Groups • Group Members • Cloud Groups • Nested Groups • Synced Groups • Deleted Groups
<p>Manager Reports (Stat.AzureAD.ManagerReports)</p>	<p><u>Account Details Monitoring</u></p>	<ul style="list-style-type: none"> • Managers & Direct Reports • Users with Manager • Users without Manager
<p>License & Subscription Usage (Stat.AzureAD.LicenseReports)</p>	<p><u>Account Usage Monitoring</u></p>	<ul style="list-style-type: none"> • Daily Activities • Subscription Usage • Unused Subscriptions • Licensed Users • Regain Licenses

<p>MFA Reports (Stat.Security.MFAReports)</p>	<p>Identification and Authentication (Organizational Users) Security Function Verification</p>	<ul style="list-style-type: none"> • User with MFA • Users without MFA • MFA Enabled • MFA Enforced Users • MFA Activated Users • MFA Non-Activated User • MFA Device Details
<p>Password Reports (Stat.Security.PasswordReports)</p>	<p>Identification and Authentication (Organizational Users) Authenticator Management</p>	<ul style="list-style-type: none"> • 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
<p>Admin Reports (Stat.Security.AdminReports)</p>	<p>Access Restrictions for Change Least Privilege</p>	<ul style="list-style-type: none"> • All Admins • Admin Roles by Users • All Global Admins • Admins with Management Roles • Admins with Read Access Roles
<p>External User Reports (Stat.Security.ExternalUserReports)</p>	<p>Account Management Audit</p>	<ul style="list-style-type: none"> • All External Users
<p>Mailbox Info (Stat.Exchange.MailboxInformation)</p>	<p>Identifier Management</p>	<ul style="list-style-type: none"> • All Mailboxes • Shared Mailboxes • Archived Mailboxes

<p>Shared Mailbox Info (Stat.Exchange.SharedMailboxInfo)</p>	<p>Account Usage Monitoring</p>	<ul style="list-style-type: none"> • Shared mailbox size over time
<p>Mailbox Usage (Stat.Exchange.MailboxUsage)</p>	<p>Account Usage Monitoring</p>	<ul style="list-style-type: none"> • Mailbox size over time • Daily mailbox quota status • Archived mailbox over warning quota • Daily Site Storage
<p>Audit Settings (Stat.Exchange.AuditSettings)</p>	<p>Audit Review, Analysis and Reporting</p>	<ul style="list-style-type: none"> • Audit enabled mailboxes • Audit disabled mailboxes • Admin Audit enabled • Owner audit enabled • Delegate audit enabled
<p>Mobile Devices (Stat.Exchange.MailboxInfo)</p>	<p>Access Control for Mobile Devices Device Identification and Authentication</p>	<ul style="list-style-type: none"> • 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

<p>Site Collections (Stat.SharePoint.Site)</p>	<p>Configuration Change Control</p>	<ul style="list-style-type: none"> • Sharing Configs • SharePoint DLP Actions
<p>Inactive Users (Stat.SharePoint.InactiveUsers)</p>	<p>Inactive Users</p>	<ul style="list-style-type: none"> • By Last File Accessed • By Last File Synced • By Last External Share • By Last Internal Share • By Last Page Access

<p>Daily Activation Summary (Stat.SharePoint.DailySummary)</p>	<p>Account Usage Monitoring</p>	<ul style="list-style-type: none"> • 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
---	---	--

<p>Inactive Users (Stat.OneDrive.InactiveUsers)</p>	<p>Inactive Users</p>	<ul style="list-style-type: none"> • By Last File Accessed • By Last File Synced • By Last External Share • By Last Internal Share
--	---------------------------------------	--

<p>Daily Summary (Stat.OneDrive.DailySummary)</p>	<p>Account Usage Monitoring</p>	<ul style="list-style-type: none"> • Daily Activities • User Activities • Active Users
--	---	---

<p>User Activities (Stat.Teams.UserActivities)</p>	<p>Account Usage Monitoring</p>	<ul style="list-style-type: none"> • Daily Activities • Overall Activities
---	---	--

<p>Inactive Users (Stat.Teams.InactiveUsers)</p>	<p>Account Management Audit Inactive Users</p>	<ul style="list-style-type: none"> • By Last Team Chat • By Last Private Chat • By Last Call Activity • By Last Meeting Activity
---	--	--

<p>Inactive Users (Stat.Yammer.InactiveUsers)</p>	<p><u>Inactive Users</u></p>	<ul style="list-style-type: none"> • By Last Post Liked • By Last Post Posted • By Last Post Read • By Last Activity
<p>User Activities (Stat.Yammer.UserActivities)</p>	<p><u>Account Management Audit</u></p>	<ul style="list-style-type: none"> • Daily Activities • Overall Activities
<p>User Activities (Stat.Skype.UserActivities)</p>	<p><u>Account Usage Monitoring</u></p>	<ul style="list-style-type: none"> • Peer to peer Sessions • Organized Conference • Participated Conference • File Transfer • Instant Messages
<p>Active Users (Stat.General.ActiveUsers)</p>	<p><u>Account Management Audit</u></p>	<ul style="list-style-type: none"> • 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
<p>Office 365 Group Creations (Stat.General.Office365GroupCreations)</p>	<p><u>Account Management Audit</u></p>	<ul style="list-style-type: none"> • Groups created via Teams • Groups created via Yammer • Groups created via SharePoint • Empty Groups • Groups with Hidden membership
<p>Software Installs (Stat.General.SoftwareInstalls)</p>	<p><u>Software Usage Restrictions and User Installed Software</u></p>	<ul style="list-style-type: none"> • Office activations • Project client • Visio client

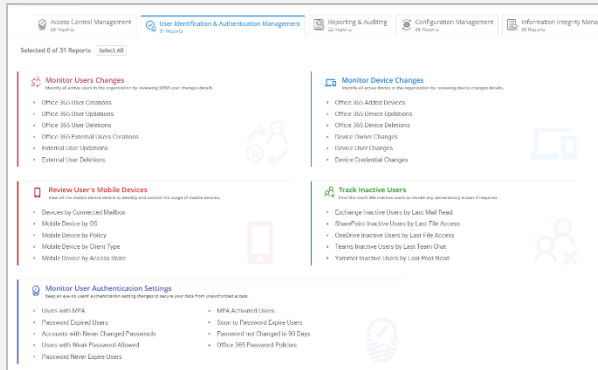
<p>Risky Sign-ins (Anal.Sign-inAnal.RiskySign-Ins)</p>	<p>Criticality Analysis Incident Monitoring</p>	<ul style="list-style-type: none"> • Confirmed Risky Sign-ins • Open Risky Sign-ins • Admin Confirmed User Compromised • Risk Status Marked as Compromised
<p>Sign-ins with Prompts (Anal.Sign-inAnal.Sign-InsWithPrompt)</p>	<p>Criticality Analysis Incident Monitoring</p>	<ul style="list-style-type: none"> • Strong Auth Enrollment Prompted Sign-ins • Signed-in Via Alternate Auth Method • Password reset Prompts • Multiple O365 Accounts Prompts • Keep Me Signed-in Prompts
<p>Risky Sign-ins by Risk Level (Anal.Sign-InAnal.ByRiskLevel)</p>	<p>Risk Assessment Incident Monitoring</p>	<ul style="list-style-type: none"> • High Risky Sign-ins • Medium Risky Sign-ins • Low Risky Sign-ins • Hidden Risky Sign-ins
<p>Risky Sign-ins by Detection Timing (Anal.Sign-InAnal.ByDetectTiming)</p>	<p>Risk Assessment</p>	<ul style="list-style-type: none"> • Real Time Risk Detections • Near Real Time Risk Detections • Offline Risk Detections
<p>Risky Sign-ins by Risk Status (Anal.Sign-InAnal.ByRiskStatus)</p>	<p>Risk Response</p>	<ul style="list-style-type: none"> • Marked As Safe • Marked As Remediated • Marked As Dismissed • Marked As Compromised

<p>Risky Sign-ins by Risk Event Type (Anal.Sign-InAnal.ByRiskEventType)</p>	<p><u>Risk Assessment</u></p>	<ul style="list-style-type: none"> • 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
<p>Risky Sign-ins by Risk Resolved Method (Anal.Sign-InAnal.ByResolvedMethod)</p>	<p><u>Risk Response</u></p>	<ul style="list-style-type: none"> • 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
<p>CA Policy Configuration (Anal.CAP.PolicyConfiguration)</p>	<p><u>Policy and Procedures</u></p>	<ul style="list-style-type: none"> • All CA policies • Recently modified CA policies • CA Policies with Grant Control details • CA Policies with Session Control details

<p>CA Policy Assignment Details (Anal.CAP.AssignmentDetails)</p>	<p><u>Policy and Procedures</u> <u>Identification and Authentication</u> <u>(Organizational Users)</u></p>	<ul style="list-style-type: none"> • 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
<p>MFA Configured Policies (Anal.CAP.MFAConfigPolicies)</p>	<p><u>Policy and Procedures</u> <u>Identification and Authentication</u> <u>(Organizational Users)</u></p>	<ul style="list-style-type: none"> • Policies with MFA • MFA policies Assignment Overview • MFA policies Assignment Details

Pre-compiled Report Bundle for FISMA Compliance

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



[Explore FISMA Report Board](#)

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

Outline of FISMA Compliance Report Categorization

Access Control Management

Monitor and control the user access privileges in your organization by tracking user activities, failed logins, privilege changes, etc.

- [Detect Anomalies in User Activity \(8 Reports\)](#)
- [Check Users, Groups & Device Details \(6 Reports\)](#)
- [Monitor User Activities \(5 Reports\)](#)
- [Monitor and Control User Access Rights \(10 Reports\)](#)
- [Keep Track of Failed Logins \(4 Reports\)](#)

User Identification & Authentication Management

Review the user identity changes, authentication setting changes, device details, and more to identify the updates made in the organizational users.

- [Monitor Users Changes \(6 Reports\)](#)
- [Monitor Device Changes \(6 Reports\)](#)
- [Review User's Mobile Devices \(5 Reports\)](#)
- [Track Inactive Users \(5 Reports\)](#)
- [Monitor User Authentication Settings \(9 Reports\)](#)

Reporting & Auditing

Audit various activities to efficiently manage your organization like mailbox auditing, user activities, and more.

- [User Activities by Resources \(10 Reports\)](#)
- [Verify Mailbox Auditing \(5 Reports\)](#)
- [Analyze User Activities \(8 Reports\)](#)

Configuration Management

Verify the configuration changes made by the users to prevent any security risks.

- [Review Security Configurations \(12 Reports\)](#)
- [Monitor Configuration Changes \(16 Reports\)](#)
- [Sharing Configuration Changes \(6 Reports\)](#)
- [Access Permission Changes \(4 Reports\)](#)

Information Integrity Management

Trace the risky activities such as risky logins, alerts, ATP changes, secure scores to maintain data security and to avoid any risks in the organization.

- [Track Risky Logins \(17 Reports\)](#)
- [Monitor System Alerts \(10 Reports\)](#)
- [Verify Application Details \(4 Reports\)](#)
- [Track ATP activities \(3 Reports\)](#)
- [Review Integrity and Security Scores \(5 Reports\)](#)

Incident Analysis

- [Monitor File Sharing and Access Activity \(4 Reports\)](#)
- [DLP Rule Matches & Alerts \(4 Reports\)](#)
- [Ensure Data Recovery \(6 Reports\)](#)

How can AdminDroid help implement other Security and Compliance requirements?

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

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



Explore >

AdminDroid

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

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

Live Demo

Download

Connect with us

[in linkedin.com/company/admindroid/](https://www.linkedin.com/company/admindroid/)

[reddit.com/r/AdminDroid/](https://www.reddit.com/r/AdminDroid/)

[X twitter.com/admiindroid](https://twitter.com/admiindroid)

[f facebook.com/admindroid](https://www.facebook.com/admindroid)

[youtube.com/admindroid](https://www.youtube.com/admindroid)

[ad admindroid.com](https://admindroid.com)

github.com/admindroid-community