AdminDroid

CJIS Compliance

with

AdminDroid Office 365 Reporter

AdminDroid

CJIS Compliance
with AdminDroid

The **Criminal Justice Information Services (CJIS)** Division under the **Federal Bureau of Investigation (FBI),** a primary law enforcement agency for the US government is widely used for safeguarding Criminal Justice Information. The **CJIS security policy v5.9** incorporated in the year 2019 has been approved by the Advisory Policy Board and Compact Council. It provides security requirements that need to be fulfilled by the **Criminal Justice Agencies, and Non-criminal Justice Agencies** for accessing the FBI CJIS Division systems and respective information.

Agencies handling the criminal justice information must provide security awareness training for all the employees, vendors, etc., and it should repeat every two years for becoming CJIS compliant. For every three years, the **CJIS Audit Unit audits** the access, usage, storage, and destruction of information in government institutions and agencies to ensure that they are fulfilling the CJIS compliance control requirements.

Also, private agencies handling the CJI must fulfill the CJIS compliance requirements and conduct an audit once in three years. To ease your CJIS auditing, we came up with two ways to make you choose the one with your comfort.

CONTROL GROUPS

The whole process of IT Operational 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 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

MAPPING OF CJIS 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 CJIS Compliance**

(AdminDroid offers CJIS 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 CONTROL GROUPS TO COBIT

Mapping of CJIS Security policy to Control Families.

CJIS Requirement	Control Family
5.1.2 Monitoring, Review, and Delivery of Services. As specified in the interagency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.	**System and Information Integrity** **Incident Response**
5.3.2.1 Incident Handling The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Incident-related information can be obtained from a variety of sources including, but not limited to audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.	**Incident Response** • Incident monitoring • Incident analysis • Info spillage response
5.3.4 Incident Monitoring The agency shall track and document security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action is complete; whichever time-frame is greater.	**Incident Response** • Incident Monitoring

5.4.1 Auditable Events and Content (Information Systems) The agency's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.	**Audit and Accountability** • Audit Events
5.4.3 Audit Monitoring, Analysis, and Reporting The management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.	**Audit and Accountability** • Audit Review, Analysis and Reporting
5.4.5 Protection of Audit Information The agency's information system shall protect audit information and audit tools from modification, deletion, and unauthorized access.	File modification, file deletion, file access Admin activity reports - report access **AdminDroid Portal Login Events** • Admin Logins • Failed Admin Logins • Admin Logouts • Login Event Summary • Login Failure Summary

Report and ReportBoard Accesses

- Reports Accessed by Admins
- Reports Access Summary
- Top Reports Accessed
- ReportBoards Accessed by Admins

Report Downloads and Emailing

- Exported from Report Page
- Report Export Summary
- Top Report Exports by Admins
- Exports from ReportBoard
- Emailed from Report Page
- Emailed from ReportBoard Page

Schedule Reports

- Created Scheduled Reports
- Edited Scheduled Reports
- Deleted Scheduled Reports
- Status Changes
- Trigger Now/Test Run Events

Report-Views Management

- Created Views
- Edited Views
- Deleted Views

Tenant Management

- Added Tenants
- Deleted Tenants
- Retained Tenants
- Force-Deleted Tenants
- Sync Pausing Events
- Sync Resuming Events
- Default Tenant Selections

Admin Management

- Added Admins
- Deleted Admins
- Admins Enabling Events
- Admins Disabling Events
- Admin and Super Admin Changes
- Tenant Delegation Changes
- Role Delegation Changes
- Invitation Mails Sent
- View As Admins

	Delegated Roles Management • Created Roles • Deleted Roles • Updated Roles • Inspect Roles **Product Settings** • Email Configured • Email Setting Changes • Beta Enabling Events • Beta Disabling Events • Data Retention Enabling Events • Data Retention Disabling Events • Disk Usage Warning Alerts Config • Disk Usage Critical Alerts Config **Alert Policies Management** • Created Alert Policies • Updated Alert Policies • Deleted Alert Policies • Status Changes • Manually Checked Alert Policies **Triggered Alerts Management** • Accessed by Admins • Status Changes • Bulk Status Changes • Deleted Alerts • Bulk Deleted Alerts
5.4.6 Audit Record Retention The agency shall retain audit records for at least one year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes.	Using AdminDroid Reporting and Auditing tool, you can retain your audit records as long as required.

5.5.1 Account Management The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Account management includes the identification of account types (I.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges.	**Access Control** • Account Management Audit
5.5.2 Access Enforcement The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).	**Access Control** • Least privilege reporting **User License Reports** • Licensed Users • Users by Subscriptions • Unlicensed Users • Free Users • Trial Users **Admin Reports** • All Admins • Admin roles by users • User Added as Admins (25 Reports) • All Global Admins • Admins with Management Roles • Admins with Read Access Roles **Mailbox Permissions** • Access to Others Mailboxes • Mailbox Permission Summary • Mailbox Permission Detail • Mailbox with SendOnBehalf • Send As Permission • Full Permission • Read Permission • Guests’ Mailbox Permission Summary • Admins Access to Others Mailboxes • Admins with Send-on-Behalf • Admins with Send-As • Admins with Full Access • Guests Access to Others Mailboxes

5.5.2.1 Least Privilege The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know. Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.	**Access Control** • Least privilege auditing **Admin Role Changes** • Role Assignments • Role Scope Changes • Added Roles • Updated Roles **Role Configuration Changes** • Management Role • Role Assignment • Assignments Policy • Role Entry • Role Group • Role Scope **Mailbox Access** • Mailbox Non-Owner Access
5.5.3 Unsuccessful Login Attempts Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.	**Access Control** • Unsuccessful Logon Attempts

5.5.6.1 Personally Owned Information Systems A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices. This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).	**Access Control** • Access Control for Mobile Devices
5.6.1 Identification Policy and Procedures Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit	**Identification and Authentication** • Identification and Authentication (Organizational users)
5.6.2.1 Standard Authenticators Authenticators are (the something you know, something you are, or something you have) part of the identification and authentication process. Examples of standard authenticators include passwords, hard or soft tokens, biometrics, one-time passwords (OTP) and personal identification numbers (PIN). Users shall not be allowed to use the same password or PIN in the same logon sequence.	**Identification and Authentication** 1. Authenticator Management • Mfa • Users with MFA • MFA Activated Users • Users' MFA details

5.6.2.2 Advanced Authentication Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates.	**Risk Assessment** • All CA policies • Recently modified CA policies • CA policies with Grant Control details • CA policies with Session Control details • Policies with MFA • MFA policies Assignment Overview • MFA policies Assignment Details
5.6.3 Identifier and Authenticator Management The agency shall establish identifier and authenticator management processes.	**Identification and Authentication** • Identifier Management • Authenticator Management
5.7.1 Access Restrictions for Changes Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications	**Configuration Management** • Access Restrictions for changes
5.7.2 Security of Configuration Documentation The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.	**Access Control**

5.10.4.2 Malicious Code Protection The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available). The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.	Logins based on browsers, versions, OS • Organizations sign-in summary by operating system • Organizations sign-in summary by browser • User's sign-in summary by device
5.10.4.3 Spam and Spyware Protection The agency shall implement spam and spyware protection. The agency shall: 1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers). 2. Employ spyware protection at workstations, servers and mobile computing devices on the network. 3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this Policy.	**System and Information Integrity** • Spam Protection • Memory Protection

5.10.4.4 Security Alerts and Advisories The agency shall: 1. Receive information system security alerts/advisories on a regular basis. 2. Issue alerts/advisories to appropriate personnel. 3. Document the types of actions to be taken in response to security alerts/advisories. 4. Take appropriate actions in response. 06/01/2020 CJISD-ITS-DOC-08140-5.9 60 5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.	**System and Information Integrity** • Security Alerts, Advisories and Directives Using AdminDroid Alerting feature, you can issue alerts to the respective personnel in your organization. (Explore AdminDroid Alerting)
5.11.1 Audits by the FBI CJIS Division 5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies. The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities. 5.11.1.2 Triennial Security Audits by the FBI CJIS Division The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.	**Audit and Accountability** • Audit Review, Analysis and Reporting 1. Compliance search activities

5.11.2 Audits by the CSA Each CSA shall: 1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies. 2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies. 3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities. 4. Have the authority, on behalf of another CSA, to conduct a CSP compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.	**Audit and Accountability** • Audit Review, Analysis and Reporting
5.11.3 Special Security Inquiries and Audits All agencies having access to CJI shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division. All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.	**System and Information Integrity** • Information system Monitoring 1. Security Function Verification

5.12.2 Personnel Termination Upon termination of personnel by an interface agency, the agency shall immediately terminate access to local agency systems with access to CJI. Furthermore, the interface agency shall provide notification or other action to ensure access to state and other agency systems is terminated. If the employee is an employee of a NCJA or a Contractor, the employer shall notify all Interface Agencies that may be affected by the personnel change.	**Access Control**
5.12.3 Personnel Transfer The agency shall review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.	**Identification and Authentication** • Identification and Authentication (Organizational users) • Authenticator Management
5.13.2 Mobile Device Management (MDM) Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery, if so desired by the agency. Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time.	**Configuration Change Control** • Device Audit • Mobile Device
5.13.3 Wireless Device Risk Mitigations Employ malicious code protection on full-featured operating system devices or run an MDM system that facilitates the ability to provide anti-malware services from the agency level.	

5.13.4.3 Personal Firewall At a minimum, the personal firewall shall perform the following activities: 1. Manage program access to the Internet. 06/01/2020 CJISD-ITS-DOC-08140-5.9 71 2. Block unsolicited requests to connect to the user device. 3. Filter incoming traffic by IP address or protocol. 4. Filter incoming traffic by destination ports. 5. Maintain an IP traffic log.	**Configuration Change Control** • Mail flow configs • Transport rules • Connector configs • Hybrid configs • Federation configs • Accepted domains • Remote domain
5.13.5 Incident Response In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface. Special reporting procedures for mobile devices shall apply in any of the following situations: 1. Loss of device control. For example: a. Device known to be locked, minimal duration of loss b. Device lock state unknown, minimal duration of loss c. Device lock state unknown, extended duration of loss d. Device known to be unlocked, more than momentary duration of loss 2. Total loss of device 3. Device compromise 4. Device loss or compromise outside the United States	**Access Control** • Device audit

5.13.6 Access Control Multiple user accounts are not generally supported on limited-feature mobile operating systems. Access control (Section 5.5 Access Control) shall be accomplished by the application that accesses CJI.	**Access Control** - Access control for mobile devices
5.13.7 Identification and Authentication Due to the technical methods used for identification and authentication on many limited-feature mobile operating systems, achieving compliance may require many different components.	**Identification and Authentication** - Device Identification and Authentication

MAPPING OF CONTROL GROUPS TO REPORT COLLECTIONS

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

ACCESS CONTROL

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

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

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

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

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

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

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

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

IDENTIFICATION AND AUTHENTICATION

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

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

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

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.

SYSTEM AND INFORMATION INTEGRITY

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

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

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

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

INCIDENT RESPONSE

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

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

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

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

CONFIGURATION MANAGEMENT

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

Control	Implementation of Control in Microsoft 365	Applicable AdminDroid Report
1. Configuration Change Control Audit the changes to the configuration of your organization's information system components.	Review changes to the configuration of devices and other services in the Microsoft 365 Environment to ensure that changes are being made by authorized personnel in line with your change management procedures.	**Device Audit** • Device Config changes **Mobile Device Audit** • Mobile Device Configs • Active Sync Configs • Text Message Settings

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

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	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

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: (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].		**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 **MFA Configured Policies Analytics** • Policies with MFA • MFA policies Assignment Overview • MFA policies Assignment Details

MAPPING OF ADMINDROID REPORT CATEGORIES TO CONTROL GROUPS

The below mapping will help you to identify how various Microsoft 365 reporting fulfilling the CJIS 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 Security Function Verification	• Successful User Logins • Failed User Logins • Failed Sign-ins • Failed logins in MFA challenge • MFA Disabled • User Login Count Summary • User's First Logon Time • User's Last Logon Time • All User Logins • Users' Login Failure Summary • Users' last logon summary by users • Users' last logon summary by application • Users' last logon summary by city • Users' last logon summary by state • Users' last logon summary by country • Users' last logon summary by browser • Users' last logon summary by operating system
Password Changes (Audit.AzureAD.PasswordChanges)	Authenticator Management Account Management Audit	• User Password Changes • Password Reset by Admin • Forced/Expired Password Reset • Forced by Admin • All Password Changes
User Audit (Audit.AzureAD.UserAudit)	Account Management Audit Identifier Management	• Created Users • Updated Users • License Changes • Deleted Users • All User Events

Group Audit (Audit.AzureAD.GroupAudit)	Identifier Management	- Created Groups - Deleted Groups - Updated Groups - Group Member Changes
Admin Role Changes (Audit.AzureAD.AdminRole)	Account Management Audit Access Restrictions for Change	- All Role Member Changes - All Role Operations - Role Assignments - Role Scope Changes - Deleted Roles - Updated Roles - Added Roles
Device Audit (Audit.AzureAD.DeviceAudit)	Device Identification and Authentication Configuration Change Control	- Added Devices - Deleted Devices - Updated Devices - Config Changes - Credential Changes - Owner Changes - User Changes - All Device Operations - Sign-ins with Device details - Mobile Sign-ins - Non-compliant Device sign-ins - Unmanaged Device sign-ins

Risky Login Attempts (Audit.Security.RiskyLoginAttempts)	Incident Monitoring Unsuccessful Logon Attempts	- Failed to Pass MFA - Legacy/Basic Auth Attempt Challenge - Expired Password Login Attempts - Admin’s Login Failures - Admin’s Login Failure Summary - Disabled User Login Attempts - Failed Sign-ins - Failed in MFA challenge

Administrative Users Reports (Audit.Security.UserAddedAsAdmins)	Least Privilege	• User added as admins *(25 reports)*

Mailbox Access (Audit.Exchange.MailboxAccess)	Least Privilege	• MFA Non-owner access
Mailbox Permissions (Audit.Exchange.MailboxPermissions)	Least Privilege	• Access to Others Mailboxes • Mailbox Permission Summary • Mailbox Permission Detail • Mailbox with Send on Behalf • Send as Permission • Full Permission • Read Permission • Guests' Mailbox Permission Summary • Admins Access to Others Mailboxes • Admins with Send-on-Behalf • Admins with Send-As • Admins with Full Access • Guests Access to Others Mailboxes
Advanced Threat Protection (Audit.Exchange.ATP)	Incident Monitoring Configuration Change Control Spam Protection Memory Protection	• Safe Attachment • Safe Link • Anti-Spam • Anti-Phishing • Anti-Config • Spam Mails Received • Spam Mails Sent/Received • Anti-Malware • Phishing Filter • Junk Email • DKIM Config • All ATP Activities

Role Changes (Audit.Exchange.RoleChanges)	Least Privilege	• Management • Role Assignments • Assignments Policy • Role Entry • Role Scope • Role group
Mail Flow (Audit.Exchange.MailFlow)	Configuration Change Control	• Mail Flow Configs • Transport Rules • Connector Configs • Accepted Domains • Remote Domain • Hybrid Configs • Federation Configs
Mobile Device Audit (Audit.Exchange.MobileDevice)	Access Control for Mobile Devices Configuration Change Control	• Mobile Device Configs • Active Sync Configs • Text Message Configs
Data Loss Prevention (Audit.Exchange.DataLossPrevention)	Configuration Change Control	• DLP Configs • Rule Matches

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

File Activities (Audit.SharePoint.FileActivities)	Information Sharing Audit	• All Events

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

Alert Severity (Audit.Alerts.AlertSeverity)	Security Alerts, Advisories and Directives	• High severity • Medium severity • Low severity
Alert Category (Audit.Alerts.AlertCategory)	Security Alerts, Advisories and Directives Information Spillage Response	• Data Loss Prevention • Threat Management • Information Governance • Permissions • Mail flow • Others

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

Overall Activities (Audit.General.Overall)	Account Usage Monitoring Information System Monitoring Incident Analysis Access Restrictions for Change	• Admin Activities • All Failed Activities • All Activities • Top Activity Summary • Daily activity summary • Activity by Department • Activity by City • Activity by State • Activity by Country • Activity by JobTitle • Activity by Company
Office 365 Workload Based Activities (Audit.General.O365WBA)	Audit Events Audit Review Analysis & Reporting Information System Monitoring Incident Analysis	• Azure AD Activities • Exchange Activities • SharePoint Activities • OneDrive Activities • OneNote Activities • Power BI Activities • Teams Activities • Stream Activities • Security and Compliance • Compliance Search Activities

Sharing & Access Audit.General.SharingAndAccess	Incident Analysis Information Sharing Audit	• Anonymous User Activities • External User Activities • Guest User Activities • All File/Folder Sharing Activities • All File/Folder Access Activities • Files shared by External users • Files shared to External users • File/Folder accesses by External Users • File Deletion • Anonymous link creation • Anonymous link accessed • Files shared via Teams Channels • Files shared by External Users in Channels • Files shared via 1:1 chat • Files shared to External Users 1:1 chat

User Reports (Stat.AzureAD.UserReports)	Account Management Audit Identification and authentication (Organizational Users)	• All Users • Disabled Users • Enabled Users • Recently Created • Deleted Users • Users not in any Group • Cloud Users • Synced Users • Release Track Users • All Contacts • Users with Errors • Internal Guest Users
License Reports (Stat.AzureAD.LicenseReports)	Least Privilege	• Licensed Users • Users by Subscriptions • Unlicensed Users • Free Users • Trial Users

Group Reports (Stat.AzureAD.Group)	Account Type Monitoring	• All Groups • Group Members • Cloud Groups • Nested Groups • Synced Groups • Deleted Groups
Manager Reports (Stat.AzureAD.ManagerReports)	Account Details Monitoring	• Managers & Direct Reports • Users with Manager • Users without Manager
License & Subscription Usage (Stat.AzureAD.LicenseReports)	Account Usage Monitoring	• Daily Activities • Subscription Usage • Unused Subscriptions • Licensed Users • Regain Licenses

MFA Reports (Stat.Security.MFAReports)	Identification and Authentication (Organizational Users) Security Function Verification	• User with MFA • Users without MFA • MFA Enabled • MFA Enforced Users • MFA Activated Users • MFA Non-Activated User • MFA Device Details
Password Reports (Stat.Security.PasswordReports)	Identification and Authentication (Organizational Users) Authenticator Management	• Password Policies • Password Expired Users • Password soon to Expire Users • Password Never Expire Users • Users with Password Expiry • Password never changed • Password not changed in 90 days • Recent password changers • Users with weak password allowed

Admin Reports (Stat.Security.AdminReports)	Access Restrictions for Change Least Privilege	• All Admins • Admin Roles by Users • All Global Admins • Admins with Management Roles • Admins with Read Access Roles
External User Reports (Stat.Security.ExternalUserReports)	Account Management Audit	• All External Users

Mailbox Info (Stat.Exchange.MailboxInformation)	Identifier Management	• All Mailboxes • Shared Mailboxes • Archived Mailboxes
Shared Mailbox Info (Stat.Exchange.SharedMailboxInfo)	Account Usage Monitoring	• Shared mailbox size over time
Mailbox Usage (Stat.Exchange.MailboxUsage)	Account Usage Monitoring	• Mailbox size over time • Daily mailbox quota status • Archived mailbox over warning quota • Daily Site Storage
Audit Settings (Stat.Exchange.AuditSettings)	Audit Review, Analysis and Reporting	• Audit enabled mailboxes • Audit disabled mailboxes • Admin Audit enabled • Owner audit enabled • Delegate audit enabled

Mobile Devices (Stat.Exchange.MailboxInfo)	Access Control for Mobile Devices Device Identification and Authentication	• All Mobile Devices • Devices by Connected Mailbox • Mobile Device by OS • Mobile Device by Policy • Mobile Dives by Client Type • Mobile Devices by Access State

Site Collections (Stat.SharePoint.Site)	Configuration Change Control	• Sharing Configs • SharePoint DLP Actions
Inactive Users (Stat.SharePoint.InactiveUsers)	Inactive Users	• By Last File Accessed • By Last File Synced • By Last External Share • By Last Internal Share • By Last Page Access
Daily Activation Summary (Stat.SharePoint.DailySummary)	Account Usage Monitoring	• Daily Active users • Users File Access Summary • Users File Synced Summary • Users Internal File Sharing Summary • Users External File Sharing Summary • Users Page Visit Summary • Daily Summary of Users by Activity

Inactive Users (Stat.OneDrive.InactiveUsers)	Inactive Users	• By Last File Accessed • By Last File Synced • By Last External Share • By Last Internal Share

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

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

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

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

Active Users (Stat.General.ActiveUsers)	Account Management Audit	- Last Active Time - Daily Active Users - Exchange Last Active Time - SharePoint Last Active Time - OneDrive Last Active Time - Teams Last Active Time - Yammer Last Active Time
Office 365 Group Creations (Stat.General.Office365GroupCreations)	Account Management Audit	- Groups created via Teams - Groups created via Yammer - Groups created via SharePoint - Empty Groups - Groups with Hidden membership

Risky Sign-ins (Anal.Sign-inAnal.RiskySign-Ins)	Incident Monitoring	- Confirmed Risky Sign-ins - Open Risky Sign-ins - Admin Confirmed User Compromised - Risk Status Marked as Compromised
Sign-ins with Prompts (Anal.Sign-inAnal.Sign-InsWithPrompt)	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)	Incident Monitoring	- High Risky Sign-ins - Medium Risky Sign-ins - Low Risky Sign-ins - Hidden Risky Sign-ins

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

How can AdminDroid help implement other Security and Compliance requirements?

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

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

Explore >

AdminDroid

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

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

Live Demo Download

Connect with us

linkedin.com/company/admindroid/	reddit.com/r/AdminDroid/	twitter.com/admiindroid
facebook.com/admindroid	youtube.com/admindroid	admindroid.com
github.com/admindroid-community		