ilantus
The Cloud Identity People

مؤسسة النقد العربي السعودي
Saudi Arabian Monetary Authority

Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework

Guidelines for Identity & Access Management

inquiry@ilantus.com • www.ilantus.com

The Saudi Arabian Monitory Authority (SAMA) has mandated Banking, Insurance and Financing Companies implement a Cyber Security Framework to achieve appropriate Cyber Security governance and robust infrastructure along with necessary detective and preventive controls.

One of the components of this framework lays down the policies, oversight and governance requirements specific to Identity and Access management (IAM) - to ensure that the Member Organization only provides authorized and sufficient access privileges to approved users.

Compact Identity from Ilantus is a complete IAM solution and fulfills all the requirements needed for SAMA compliance. While several of the specifications relate to organizational policy and oversight requirements, we have detailed below how these non-product requirements are also supported as part of our well-thought-out approach to complete Cyber Security.

SAMA IAM CONTROL CONSIDERATIONS	COMPACT IDENTITY
1. The identity and access management (IAM) policy, including the responsibilities and accountabilities, should be defined, approved and implemented.	Based on the Identity and Access Management (IAM) policies defined by the organizations IT/Security team, Compact Identity can be configured to enforce those in accordance. Compact Identity collects user profile information which also includes user's application accesses and stores it within the solution's repository, thus providing a centralized view to user profile and their accesses to all authorized applications. End users can request access to the authorized applications / roles / entitlements, based on the approval workflow it is sent to the relevant authority for decision making. Administrator or Manager can view the access rights of all the users from Compact Identity's Universal Directory. Compact Identity provides an interface to the end users to login to their applications that are authorized to them based on their role. Users can access applications from their launchpad with a single click without having to enter login credentials.

Organizations can have a complete view and thus control user access to applications. Policies such as applying MFA for critical applications can be enabled.

Compact Identity thereby helps organizations define responsibilities and accountabilities.

2. The compliance with the IAM policy should be monitored.

Compact Identity generates reports that continuously helps monitor "Who has Access to What", who approved what request, various SOD violations if any and many more. This enables the compliance team to track any fraudulent activities.

Compact Identity's risk engine provides risk scores captured at various levels; user account risk score, application risk score, etc. Based on the collected risk scores, auto-actions such as sending alerts to the relevant authority (Admin, App Owner, Manager), auto-review campaigns, blocking accesses to applications are performed by the system.

Complete logs of various such activities are captured for Compliance and Monitoring.

3. The effectiveness of the cyber security controls within the IAM policy should be measured and periodically evaluated.

Compact Identity helps to configure cyber security controls defined in IAM policy by providing controlled access to critical applications by enabling Multi-factor Authentication during Single Sign On.

Compact Identity's risk engine provides risk scores at various levels such as; user risk score, account risk score, application risk score etc. Based on the threshold defined by the organization, appropriate auto-actions such as review campaigns, sending alert messages to the relevant authority are performed by the system.

This also enables Admin/IT Security to take appropriate actions and ensure organizations IAM policies are well within compliance.

Compact Identity also helps to monitor Dormant / Orphan Accounts.

Compact Identity also handles use cases such as new joiners, movers, leavers, automatically. New accesses are provisioned immediately, when a user gets promoted or transferred - his access rights across applications are automatically adjusted, when the user leaves – his accesses are disabled immediately.

With Compact Identity, administrators can configure periodic workflows for certification/review campaigns. This helps Manager continuously monitor his sub-ordinates accesses.

Inappropriate accesses if any can be removed immediately.

Compact Identity thus empowers Business and IT to measure and monitor all IAM policies.

4. IAM policy should include the following:

a. Business requirements for access control (i.e., need-to-have and need-to-know)

Compact Identity administrators can frame and configure access policies based on organization's security controls to provision user's application access based on their organizational role.

Compact Identity provides an interface to the end users to login to their applications that are authorized to them. Users can access applications from their launchpad with a single click without having to enter login credentials across applications.

Organizations can have a control of user access to applications. Policies such as applying MFA for critical applications can be enabled.

Compact Identity helps to run periodic access review so that manager can monitor or review user's subordinate's accesses and revoke all inappropriate access in accordance to the job role.

b. User access management (e.g., joiners, movers, leavers)

Compact Identity allows you to provision new users by any or all the following:

- Admin initiated manual add (Use case for external vendors and contractors)
- Import user information from a csv file (Use case for external vendors and contractors)
- Any HR System (SAP HRIS, Workday HR and many more)
- AD/LDAP

Joiner: When a user in imported from ANY of the above, his accounts in target applications are automatically provisioned based on the rules configured in Compact Identity as per organization's policy and the app icon is made visible in the end user launchpad.

Mover: When user undergoes a change in role (Transfer), the information is updated in HR system based on the reconciliation in Compact Identity. Users access rights across applications are automatically adjusted by Compact Identity based on the new role.

	Leaver: When user leaves the Organization, the information is updated in HR system and based on the reconciliation in Compact Identity - users accounts in target applications are auto disabled ensuring the user no longer has access to organization resources. Thus, enabling organizations be Audit ready at any time and remain Compliant.
B1. All identified user types should be covered (i.e., internal staff, third parties)	Compact Identity supports any types of users, it can be internal staff (Employees, Contractors, Consultants) or third parties (Vendors, Business Partners).
B2. Changes for third parties should be instigated by the appointed accountable party	Appointed accountable party can communicate to the admin requesting to make changes to any third parties. It will be recorded in audit logs and can be submitted for compliance requirements.
B3. User access requests are formally approved in accordance with business and compliance requirements (i.e., need-to-have and need-to-know to avoid unauthorized access and unintended data leakage)	Compact Identity ensures right users have right set of accesses based on their job role, with properly monitored approval process. When an end user requests for an access, it is sent to the relevant authority for approval based on the workflow configuration which is in accordance to the business rules. The relevant authority has the rights to Approve or Reject the request. For business-critical applications, multi-level with/without delegated approval can be configured. All these transactions can be monitored real-time from the dashboard, reports for the same can also be availed.

B4. Changes of job status or job positions for internal staff (e.g. joiner, mover and leaver) should be instigated by the human resources department;	Compact Identity can be integrated with any HR system. Based on scheduled reconciliation in Compact Identity, all the user information including job status, job position for internal staff will be periodically updated in the solution. Any changes of job status or job positions can be tracked from the Dashboard in real-time, dashboards can be made available to the Human Resource department.
B5. Changes in access rights should be processed in a timely manner;	Changes in Access rights are handled in real time. If end user requests are approved by the manager, automatic provisioning of accounts in target applications are processed immediately. In similar manner, during termination, end user accounts are disabled with immediate effect ensuring the user no longer has access to organizational resources.
B6. Periodically user access rights and profiles should be reviewed	Admins can configure access review/certification workflows for Roles, Applications, Entitlements, and set up a campaign based on organization's security policy. These campaigns can be scheduled to be run for weekly, monthly, quarterly, half early, yearly basis (customizable). This result is then notified to the Manager for his action, enabling a Manager to periodically review user access rights. Right set of accesses can be Retained while un-authorized access if any can be Revoked by a single click (disable/delete user account). This information is captured and can be made available to the compliance team for Audit.
B7. An audit trail of submitted, approved and processed user access requests and revocation requests should be established	Reports of submitted, approved and processed user access requests and revocations are available OOTB, and can be made available at any time for Audit and Compliance.

C. User access management should be supported by automation	User access rights are automatically handled based on the organizational roles that have been set.
D. Centralization of the IAM function	Compact Identity collects all the user profile information and stores it in a centralized repository. It also collects all the application access information that are mapped to a user. Thus, providing a centralized view for all users and their accesses.
E. Multi-factor authentication for sensitive and critical systems and profiles	Multi-factor authentication at application level and end user launchpad (across all users in the solution) is currently available. MFA for systems and profiles level are in road-map.
F. Privileged and remote access management, which should address the following requirements:	Saudi Arabian Monitory Authority's guidance for Identity Access Management measures aligns closely with Ilantus's Privileged Access Management (PAM) best practices:
F1. The allocation and restricted use of privileged and remote access, specifying:	Compact Identity Privileged Access Management can be used to control, define, and manage access on a need-to-know and need-to-have basis. Depending on the users' roles, responsibilities, PAM can enable controlled, password-less access to important IT systems such as RDP, SSH and others. This ensures that only designated users can access with their authorized user IDs and passwords of these privileged accounts and these identities are not shared among multiple users.

F1a. Multi-factor authentication should be used for all remote access;

Compact Identity PAM can force users to enter another form of authentication on login, such as a pin or token. PAM comes with its own built-in email two-factor authentication and supports the existing infrastructure to make use of RADIUS two-factor systems. PAM can also integrate with TOTP authenticators to step up the authentication process.

F1b. Multi-factor authentication should be used for privilege access on critical systems based on a risk assessment;

Using two-factor authentication helps prevent a scenario where a user might walk away from a workstation while logged in and an attacker could walk up to it and login to PAM. For critical systems, Access-Request workflows can be included.

With Access-Request Workflow Templates one can:

- Require that multiple people approve a request before access is granted
- Require multiple workflow steps, each with different reviewers and number of required approvers, if desired.
- Select “Owners” as a review group

This can enhance the security for critical systems

F2. The periodic review of users with privileged and remote accounts;

Identify all privileged accounts and resources and vault away those privileged credentials so that they are properly managed. Organizations can leverage the Privileged Access Service to establish the core privileged access controls across your growing attack surface.

F3. Individual accountability;

Compact Identity PAM can force users to enter another form of authentication on login, such as a pin or token. PAM comes with its own built-in email two-factor authentication and supports the existing infrastructure to make use of RADIUS two-factor systems. Along with credential vaulting, it is important to establish an identity for users via HR-vetted enterprise directory identities like Active Directory, meaning these identities are automatically disabled when the person's employment is terminated. Instead of logging into a server with a shared account, superusers would leverage their individual identity to authenticate to the system. Compact Identity PAM can integrate with the organization's Active Directory and

F4. The use of non- personal privileged accounts, including:

F4a. Limitation and monitoring.

F4a. CI PAM can document record of all actions performed, audit logs not only can be used in forensic analysis to find exactly the issue but also to attribute actions taken by a specific user, also the sessions are so critical it is also best practice to keep a video recording of the session that can be reviewed or used as evidence for your most critical assets or in highly regulated industries. CI PAM session monitoring along with User Audit Report can help customers fulfil their compliance requirements.

F4a. Confidentiality of passwords.

F4b. Privileged account passwords need to be changed on an ad-hoc basis whenever an admin leaves or if a security breach occurs, it's critical to automate this process to ensure that your security team can move quickly to address threats. Using CI PAM password management feature, you can easily automate privileged password changes on a schedule to meet compliance mandates. The built-in password changing, and expiration schedules ensure that critical passwords are changed automatically, without manual intervention.

F4c. Changing passwords frequently and at the end of each session.

F4c. Remote Password Changing (RPC) allows properly configured Secrets to automatically update a corresponding remote account. Compact Identity PAM allows Secrets to be set for enable change password on Check-in so that whenever any privilege user checks into a secret, PAM will change the password at the end of his session and will automatically generate a new strong password and change the remote password to keep all the account synchronized.

Note: The above SAMA IAM Control Considerations have been taken from Section 3.3.5 Identity and Access Management of SAMA Cyber Security Framework.

20+ Years in IAM

18+ Fortune 100 Customers

10M+ Identity Lifecycles Managed

2M+ Logins Everyday