Analysis: Compliance Enhancement System for Santam

Context

This document examines the scope and requirements for the Compliance Enhancement System at Santam. The system is intended to address compliance gaps identified in the evaluation of Santam's adherence to essential employment laws in South Africa, including the Constitution, the Labour Relations Act (LRA), the Basic Conditions of Employment Act (BCEA), and the Employment Equity Act (EEA).

Scope

The scope of the Compliance Enhancement System includes:

- Backend analysis of the Compliance Enhancement System.
- Evaluation of compliance across various dimensions
- Alignment of policies with evolving regulations, such as pay transparency and anti-discrimination protections.
- Development of updated policies and procedures to address identified compliance risks.

Required Applications

AccountPublicAPI

- This will be an API in the application virtual lan zone facing the public internet.
- This API carries out the Login and Logout operations.
- Furthermore, this API validates the request/response for the endpoint mentioned above.
- No calling API/service authentication is required for this API

AccountAPI

- This will be an API in the DMZ (Demilitarized Zone) internal network
- This API carries out the Login, GetActiveSession and Logout operations.

- Furthermore, this API validates the request/response for the endpoints mentioned above.
- Calling API authentication is required for this API. JSON Web Tokens authentication may be used to authorize the caller
- Content Type: application/json

ComplianceReportPublicAPI

- This will be an API in the application virtual lan zone facing the public internet.
- This API carries out the EvaluatePracticePolicy, UpdatePracticePolicy and CreatePracticePolicies operations.
    - Active session or account must be logged in to be able to execute these endpoints
- Furthermore, this API validates the request/response for the endpoints mentioned above.
- No calling API/service authentication is required for this API
- Content Type: application/json

ComplianceReportAPI

- This will be an API in the DMZ (Demilitarized Zone) zone in the internal network
- This API carries out the EvaluatePracticePolicy, UpdatePracticePolicy and CreatePracticePolicies operations.
    - Active session or account must be logged in to be able to execute these endpoints
- Furthermore, this API validates the request/response for the endpoints mentioned above.
- Calling API authentication is required for this API. JSON Web Tokens / basic authentication may be used to authorize the caller
- Content Type: application/json

SystemSecurityAPI

- This will be an API in the DMZ (Demilitarized Zone) zone in the internal network.
- This API will help with API authentication
- Content Type: application/json

SQL Databases

- **Santam Employees database**
    - This database will help with user account credentials verification during login.
    - This database also helps with persisting user session for a logged in account. Login time and logout time will be persisted to have history of user login events.

- **Compliance database**
    - This database persists all practices / job profiles at Santam
    - This database persists all policies associated with job profiles.
    - This database persists all procedures at Santam.

- **System security database**
    - This database will store JSON Web Token for API Authentication

Assumptions

- Infrastructure analysis has been completed and approved.
- Cloud viability matric assessment has been completed and approved.

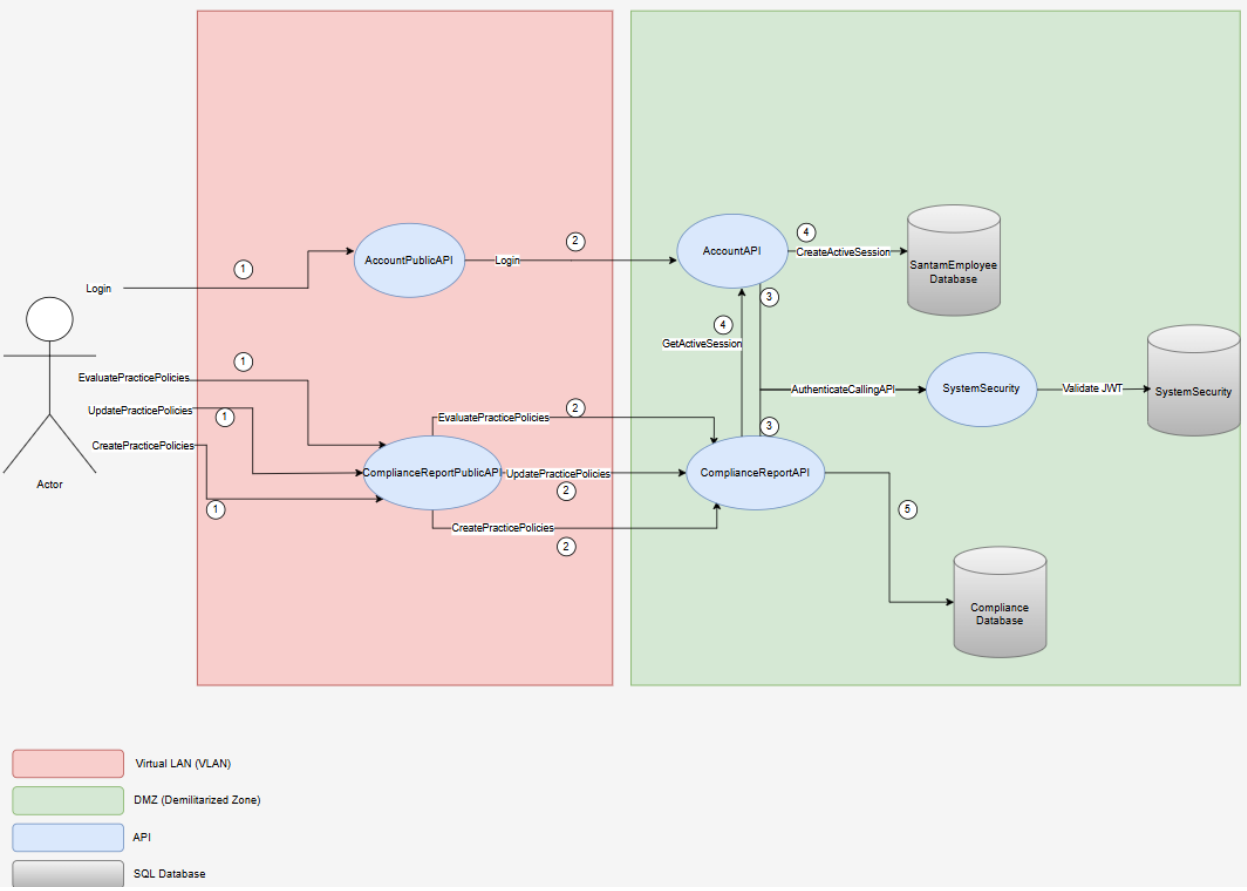
Use Cases

As a senior manager, I must be able to do the following:

- Login into the Compliance Enhancement System
    - Senior manager -> AccountPublicAPI -> AccountAPI -> SystemSecurityAPI -> SystemSecurity Database Validate JWT -> CreateSession
- Evaluate practice policies
    - senior manager -> ComplianceReportPublicAPI -> ComplianceReportAPI -> SystemSecurityAPI -> SystemSecurity Database Validate JWT -> Retrieve Policies
- Update practice policies

    - senior manager -> ComplianceReportPublicAPI -> ComplianceReportAPI -> SystemSecurityAPI -> SystemSecurity Database Validate JWT -> Update Policies
- Create practice policies
    - senior manager -> ComplianceReportPublicAPI -> ComplianceReportAPI -> SystemSecurityAPI -> SystemSecurity Database Validate JWT -> Create Policies

The diagram below outlines the use cases mentioned above



Considerations

The APIs places in the application VLan layer add security in this system.

- This prohibits public access to our critical infrastructure (applications in the DMZ).
- Also, should the applications in the DMZ get marked for upgrade or replacement, this can be done without affecting the VLan applications which are public facing