



Internal Memo.

FROM: Simon Kule, Senior Manager IT Infrastructure


Simon Kule
24/04/2023 12:43:56 PM

TO: Benoni Katende, Chief Information Officer


Approved

Benoni Katende
24/04/2023 12:46:18 PM

Edward Ssenyonjo, Head of Risk

DATE: 20th April 2023


Approved

Edward Ssenyonjo
24/04/2023 5:27:24 PM

SUBJECT: REQUEST TO MIGRATE COMPONENTS OF AVAYA CALLCENTER TO THE CLOUD

Kindly refer to the attached proposal from Sybyl (Our Avaya support provider). Avaya recently secured a license to provide cloud services in Uganda. To ensure service stability, Avaya proposes to migrate some components of the call center to the cloud as per the breakdown below.

Channels of Communication	Type	Location	Remarks
Voice	Voice	On-Premise	Delivered through MTN/AIRTEL/UTL and will use the existing setup of Avaya Aura Communication manager/session manager/system manager/experience portal and Avaya Aura Call Center Elite (part of Avaya Communication manager). Avaya Call Management System which is out of support from past 2 years have to be activated and upgraded This will provide NSSF the Voice Functionality for the Call Center
Email	Digital	Cloud	Email will be delivered through Avaya AXP CcaaS offering through direct integration with NSSF's Office 365
Website	Digital	Cloud	Chatbot which is already in cloud and integrated to your existing website will route the conversations with Avaya's agent logged into Avaya AXP CcaaS offering
Avaya Chatbot	Digital	Cloud	Avaya's Chatbot which is already in cloud will stay in cloud

Migration of the components as above will further free up resources of up to 15 servers which is worth up to USD. 100,000 in resources annually. The support for the cloud services will be covered in the current contract for the first year and will be renewed in the upcoming support provisioning for Avaya.

We hereby seek your approval of the migration as broken-down above.

Avaya Oceana Cloud migration Risk Assessment

Name	Designation	Role	Signature	Date
Hope Shaba	Information Security Specialist	Preparation		
Stephen BABIGUMIRA	Information Security Manager	Review		20 April 2023
Edward Senyonjo	Chief Risk Officer	Approval		20/04/2023

Background






National Social Security Fund uses AVAYA as the vendor to offer Unified Communications and Contact Center solution to suit to the communication and customer experience requirements of the organization. Over a Period of 5-7 years, the fund has procured the following solutions from AVAYA including Avaya Oceana. It is expected to handle the following channels of communication for customer experience team

- Inbound Voice
- Inbound Email
- Web Communications

The Fund has received a proposed from Avaya's to implement their cloud Avaya AXP CcaaS offering, This will involve migration of the Digital channels (Email, Web Communication) to Avaya's AXP Cloud freeing up all the resources consumed by Avaya Oceana.

The purpose of this risk assessment report is to identify and evaluate the potential risks associated with migration of Avaya Oceana to the Cloud. The report provides an overview of the risks, their potential impact, and recommended mitigation measures.

Avaya Cloud Migration Risk Assessment

Risk description		Recommendation	Management comment	RO
1. <u>Possible Non-Compliance to the Data Protection and Privacy</u> Processing and storing Fund Data outside Uganda poses litigation concerns especially if the destination country has different data protection and privacy regulation than Uganda. Storing Fund data in a country with less strict regulations can put the data at risk of unauthorized access, disclosure or loss which could result in violations of the Uganda Data Protection and Privacy Act 2019 hence costing the Fund in financial penalties and reputational damage.		<ul style="list-style-type: none"> Ensure that Avaya cloud service is hosted in countries that Data protection law such as the GDPR that are like Uganda's DPP Act, 2019 Obtain appropriate contractual agreements with the Avaya that include data protection and security provisions, and data sharing/processing agreements. 	<ul style="list-style-type: none"> Avaya services are hosted on Azure platform in the same location and standards as the NSSF Azure environment. 	CTESO
2. <u>Possible data breaches</u> Avaya cloud stores vast amount of data from multiple clients on the same server making it an attractive target for hackers which could result in breach of confidentiality of the Fund's sensitive data.		Ensure the contract obligations of with Avaya require them to provide evidence of having conducting comprehensive security risk assessments Or copies of compliance certificates to information security certifications such as ISO 27001 that will provide assurance to the Fund that Avaya has appropriate security controls to ensure the confidentiality, integrity and availability of the Funds data.	<ul style="list-style-type: none"> Avaya has provided documentation regarding its security posture below. <div style="text-align: center;">  Fw: EXTERNAL Fwd AXIP CCAAS Security Documents.msg </div>	CTESO
3. <u>Possible Performance degradation:</u> Cloud providers can experience downtime or latency issues. This could result in reduced productivity and loss of revenue.		Obtain Service Level Agreements contractual agreements with the Avaya to establish the performance expectations and obligations between Avaya and the Fund.	<ul style="list-style-type: none"> Will be acted upon December 2023 	CTESO
4. <u>Possible Data Loss:</u> While cloud providers generally have good backup and disaster recovery systems in place, there is still a risk of data loss due to hardware failure, human error or unforeseen events. Data loss could result in financial loss, reputational damage, and regulatory fines.		Obtain assurances/ commitments from AVAYA on testing and backup and recovery measures implemented by Avaya to minimize the risk of data loss.	<ul style="list-style-type: none"> Will be acted upon December 2023 	CTESO