Deloitte & Touche LLP
361 South Marine Corps Drive
Tamuning, GU 96913-3973
USA

Tel: +1 (671) 646-3884
Fax: +1 (671) 649-4265

www.deloitte.com

April 21, 2022

Mr. Rory Respicio
General Manager
Port Authority of Guam
1026 Cabras Highway, Suite 201
Piti, Guam 96925

Dear Mr. Respicio:

In connection with our audit of the financial statements of Port Authority of Guam (the Authority) as of and for the year ended September 30, 2021 (on which we have issued our report dated April 21, 2022), performed in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, we considered the Authority's internal control over financial reporting as a basis for designing audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Authority's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the Authority's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control over financial reporting. However, in connection with our audit, we identified, and included in the attached Appendix I, deficiencies related to the Authority's internal control over financial reporting as of September 30, 2021 that we wish to bring to your attention.

We have also issued a separate report to the Authority's management, also dated April 21, 2022, which includes certain deficiencies and other matters involving the Authority's internal control over financial reporting.

We have also issued a separate report to the Board of Directors, also dated April 21, 2022, on our consideration of the Authority's internal control over financial reporting and our tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements and other matters.

The definition of a deficiency is also set forth in the attached Appendix I.

Although we have included management's written response to our comments in the attached Appendix I, such responses have not been subjected to the auditing procedures applied in our audit and, accordingly, we do not express an opinion or provide any form of assurance on the appropriateness of the responses or the effectiveness of any corrective actions described therein.

A description of the responsibility of management for designing, implementing, and maintaining internal control over financial reporting and of the objectives of and inherent limitations of internal control over financial reporting, is set forth in the attached Appendix II and should be read in conjunction with this report.

Deloitte.

This report is intended solely for the information and use of management, the Board of Directors, others within the organization, the Office of Public Accountability - Guam and the Federal cognizant agency and is not intended to be and should not be used by anyone other than these specified parties.

We will be pleased to discuss the attached comments with you and, if desired, to assist you in implementing any of the suggestions.

We wish to thank the staff and management of the Authority for their cooperation and assistance during the course of this engagement.

Very truly yours,

Deloitte & Touche LLP

SECTION I – DEFICIENCIES

We identified the following deficiencies involving the Authority's internal control over its information technology (IT) environment as of September 30, 2021 that we wish to bring to your attention:

1. User Access Review (Regular and Privileged)

   Conditions: The Authority has no formal policy on periodic review of access rights given to network, operating systems, database, and application users. A user access review was performed for AS400 in FY2021; however, the review process was limited to the review of menus that the departments have access to. The review did not include verification of whether individual user accounts remain appropriate or not. No user access review was performed for NAVIS and its database and operating system and JDE EnterpriseOne. User access rights review allows management to check the appropriateness of access rights given to users to perform their duties and responsibilities. Non-performance of user access review increases risk of users having access to the system inappropriate for their job responsibilities.

   Recommendation: We recommend the Authority establish a policy on periodic user access rights review for regular and privileged users. Reviews can be quarterly, semi-annually, or annually. The IT Department should seek the involvement of department heads as they are knowledgeable as to employee job responsibilities. Review should include identification of inappropriate access granted to individual users as well as active accounts of resigned employees, unauthorized user account additions, or conflicting access. Review should include all critical systems and be properly documented.

   Management Action Response: IT & Finance will create an action plan to provide E1 access roles to business units on an annual basis. IT will create an action plan in providing NAVIS roles to business units on an annual basis. IT will also create a user access review policy and be compiled as part of the IT & cybersecurity policies.

   Target Date of Completion: September 30, 2022

SECTION I – DEFICIENCIES, CONTINUED

2. System Authentication Settings

Condition: The password system values listed below were not according to leading practices. With less than adequate system values, intruders may more easily access restricted system data.

System	Parameters	Current Settings	Industry Leading Practices
Windows and SQL	Enforce password history	0 passwords remembered	10 or greater
	Maximum Password Age	0 days	30; maximum of 90 days
	Minimum password length	0	8
	Account lockout	0	Block user access after 3 unsuccessful attempts
JDE E1	Maximum password age	N/A	30; maximum of 90 days
	Minimum password age	N/A	3
	Complexity Requirements	Only Minimum Number of Numeric is Enabled	Enabled
	Account lockout	N/A	Block user access after 3 unsuccessful attempts

We noted for Windows and SQL that passwords cannot be changed as such may negatively impact operations.

Where password controls are not sufficiently robust and enforced in the system, there is a risk of user passwords being compromised; hence, unauthorized access could be gained more easily, leading to unauthorized disclosure, creation, modification or deletion of sensitive financial information or transactions in the system.

Recommendation: Password parameters should be set according to industry leading practices. The Authority should clearly define security settings in information security policy, with consideration of current leading practices.

Management Action Response: The NAVIS Windows & SQL 24 servers are configured to systematically communicate with each other, using administrator & sql access. Changing the passwords is not recommended as this will impact the system functionality and its operation.

IT will inform Oracle to change the E1 authentication settings as recommended by the auditor.

Target Date of Completion: May 15, 2022

SECTION I – DEFICIENCIES, CONTINUED

3. Lack of Backup Documentation

Condition: We noted that the Authority's backup monitoring logs or documentation consists only of dates of backups and specific tapes backups are stored on. Although we noted that the backups were up to date at the date of fieldwork, some of the dates on the backup logs were skipped and the tapes were not switched during certain days. In addition, backup tapes for AS400 backups are kept inside the data center, which is within the same potential quarantine zones, access routes or environmental disaster belts as production servers. As of May 18, 2021, JDE World/AS400 has already been migrated to JDE E1; hence, an AS400 back-up would no longer be needed.

We also noted that the vendor, Oracle, is performing the backup procedures for Oracle database; however, there is no monitoring in place performed by IT to ensure successful backups occur. Per further inspection of the SOC 1 Type II Report provided by the vendor, we noted that under the "Complementary User Entity Controls Description - Availability, Physical Security and Environmental Safeguards" section of the report: 'Customers are responsible for implementing a backup and/or replication process in line with their requirements and policies'.

Without proper documentation of backup monitoring there is a chance that backups are not performed on certain days. Also, as the storage site and production site are exposed to similar risks, data availability could be compromised after an occurrence of a disaster and or terrorism.

Recommendation: The Authority should improve their backup monitoring log to include columns indicating the names of who performed the back up and monitoring, the resolution of errors encountered during the backup process, if any and the results. Backup off-site storage should be moved to a location not exposed to the same risks as the data center.

Management Action Response: IT will ask Oracle if there are any backup monitoring module in E1.

Target Date of Completion: IT will inform Oracle by May 22, 2022. Implementation will be tentative.

SECTION II – DEFINITION

The definition of a deficiency is as follows:

A deficiency in internal control over financial reporting exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A deficiency in design exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective would not be met. A deficiency in operation exists when (a) a properly designed control does not operate as designed, or (b) the person performing the control does not possess the necessary authority or competence to perform the control effectively.

MANAGEMENT'S RESPONSIBILITY FOR, AND THE OBJECTIVES AND LIMITATIONS OF, INTERNAL CONTROL OVER FINANCIAL REPORTING

The following comments concerning management's responsibility for internal control over financial reporting and the objectives and inherent limitations of internal control over financial reporting are included in generally accepted auditing standards.

Management's Responsibility

The Authority's management is responsible for the overall accuracy of the financial statements and their conformity with accounting principles generally accepted in the United States of America. In this regard, the Authority's management is also responsible for designing, implementing and maintaining effective internal control over financial reporting.

Objectives of Internal Control over Financial Reporting

An entity's internal control over financial reporting is a process effected by those charged with governance, management, and other personnel, designed to provide reasonable assurance regarding the preparation of reliable financial statements in accordance with accounting principles generally accepted in the United States of America. An entity's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the entity; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with accounting principles generally accepted in the United States of America, and that receipts and expenditures of the entity are being made only in accordance with authorizations of management and those charged with governance; and (3) provide reasonable assurance regarding prevention, or timely detection and correction, of unauthorized acquisition, use, or disposition of the entity's assets that could have a material effect on the financial statements.

Inherent Limitations of Internal Control over Financial Reporting

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct, misstatements. Also, projections of any assessment of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.