Grant Thornton

REPORT OF INDEPENDENT CERTIFIED PUBLIC ACCOUNTANTS ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS REQUIRED BY *GOVERNMENT AUDITING STANDARDS* OVER COMPLIANCE IFORM GUIDANCE

Grant Thornton LLP
150 Almaden Boulevard, Suite 60
San Jose, CA 95113-2015

T 408-275-9000
F 408-275-0582
www.GrantThornton.com

Honorable City Council
City of San José, California

We have audited, 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, the financial statements of the Norman Y. Mineta San José International Airport (the "Airport"), a department of the City of San José, California (the "City") as of and for the year ended June 30, 2016, and the related notes to the financial statements, which collectively comprise the Airport's basic financial statements, and have issued our report thereon dated November 17, 2016.

Internal control over financial reporting

In planning and performing our audit of the financial statements, we considered the Airport's internal control over financial reporting ("internal control") to design audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of internal control. Accordingly, we do not express an opinion on the effectiveness of the Airport's internal control.

A deficiency in internal control 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 material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the Airport's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified. We did identify certain deficiencies in internal control, described in the accompanying schedule of findings as items 2016-001 to 2016-003 that we consider to be significant deficiencies in the Airport's internal control.

Compliance and other matters

As part of obtaining reasonable assurance about whether the Airport's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

City's response to findings

The City's response to our findings, which is described in the accompanying Schedule of Findings, was not subjected to the auditing procedures applied in the audit of the financial statements, and accordingly, we express no opinion on the City's response.

Intended purpose

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the Airport's internal control or on compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the Airport's internal control and compliance. Accordingly, this report is not suitable for any other purpose.

San José, California
November 17, 2016

Norman Y. Mineta San José International Airport
Schedule of Findings
Year Ended June 30, 2016

Financial Statement Findings

Finding 2016-001 Informational Technology: City-Wide Information Security Program

Criteria

Internal controls over financial reporting are reliant on information technology ("IT") controls which are designed effectively. In that regard, an effectively designed IT environment is one where an organization:

a) develops, documents, and disseminates to appropriate personnel, policies that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the policy and associated controls; and,

b) periodically reviews and updates the current policy and procedures.

Condition

Systems impacted: The specific information systems impacted by the below findings were provided separately to management. In addition, the Grant Thornton team met with individual system owners and points of contact to discuss the nuances of these findings which varied slightly based on information system use, architecture, and other factors.

An entity-wide information security management program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. Overall policies and plans are developed at the entity-wide level. System and application-specific procedures implement the entity-wide policy. Ongoing monitoring of control design, implementation, and operating effectiveness should also be applied so that the program includes continuous monitoring processes.

Critical within a well-established information security program are documented policies, procedures, and guidance, security roles and responsibilities identified and appropriately delineated across the organization, and performing ongoing evaluations to ensure that policies and controls intended to reduce risk are effective. Without these aspects, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied. Grant Thornton noted weaknesses within Management's information security program; specifically:

- Management had not assigned security responsibilities associated with its decentralized control environment. For example, there was no assignment of a centralized Chief Information Security Officer ("CISO") and/or Information Security Officer(s). Further decentralized information systems did not have a Component Security Officer ("CSO") or individual that was assigned to ensure the system/location met overarching security requirements.

- Management had not finalized, published, and communicated formal policies and procedures related to information technology ("IT") control processes. Examples of draft policies and IT controls not formally documented include:

Policies in draft	Not addressed in policy
Acceptable use	Baseline security configuration setting and monitoring
Access to network and systems	Auditable event and monitoring
Anti-virus	Application change & emergency change management
Business continuity and disaster recovery	Incident response
Data classification and handling	Vulnerability scanning
Encryption	Security training
Information security	Backup and data retention
Network security	
Password	
Secure system development	

- Management did not have a processes implemented to perform continuous monitoring. Specifically, Management did not:
  - Perform periodic risk and vulnerability assessments, penetration testing, continuous monitoring through scanning or agent-based software tools, or perform other cybersecurity activities in order to identify, track and resolve security threats.
  - Perform security configuration management processes to establish and monitor platforms and software against best practices.

Cause

Due to budget constraints and significant reductions in ITD, Management has not developed or resourced an IT governance structure and processes that appropriately support the risks and threats associated with an organization of the City's size and with the added complexities of decentralization. Furthermore, while Management was in the process of finalizing and implementing City-wide policies and procedures over IT systems, they had not developed ongoing monitoring procedures to protect the integrity of financial data, nor were appropriate processes in place in order to monitor potential security threats.

Effect or Potential Effect

A lack of formal security responsibilities, as well as, policies and procedures related to security controls increases the risk that implementation of control activities may not be consistent throughout the divisions / components within the City.

Failure to perform network security vulnerabilities and penetration assessments increases the risk that the information system's security weaknesses are not identified and investigated in a timely fashion.

Failure to implement and monitor recommended security configuration and best practice settings increases the likelihood of misconfigurations that may be exploited.

Inadequate information security frameworks may lead to lapses in security requirements and consistent implementation across decentralized locations.

This could lead to errors, data loss, inappropriate access, and other risks with the potential to impair the confidentiality, integrity, and availability of systems and data. These issues may result in unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems, which may lead to misstatements on the financial statements.

Management Response

The audit identifies significant resource needs that Management concurs with. In August 2016, the City recognized increasing cybersecurity risks affecting its functions and operations. The City is in the process of developing its first dedicated Cybersecurity function to confront emerging risks associated with data exfiltration, malware, social engineering, denial-of-service attacks, and advanced persistent threats. Management recognizes the importance of information and systems security to the organization's fiscal status, insurability, compliance with laws and regulations, and overall wellbeing.

The City is currently building the cybersecurity program around the NIST Cybersecurity Framework. The model addresses the following critical functions to adequately address the security of information and electronic assets: Identify, Protect, Detect, Respond, Recover. Policies in draft are being modified to include feedback from this audit and the work on the Office of the City Auditor. Management will focus more heavily on the Identify and Protect functions initially per the recommendations of this audit.

Finding 2016-002 Information Technology: Account Management, Password Configuration, Broad Privileged Access, Password Configuration, Shared Accounts, and Audit Logging/Monitoring

Criteria

Internal controls over financial reporting are reliant on information IT controls which are designed effectively. In that regard, an effectively designed IT environment is one where an organization maintains the following:

Account Management includes the following criteria:

a) Identifies and selects the types of information system accounts needed to support organizational missions/business functions;
b) Assigns account managers for information system accounts;
c) Establishes conditions for group and role membership;
d) Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e) Requires approvals by appropriate personnel for requests to create information system accounts;
f) Creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions;
g) Monitors the use of information system accounts;
h) Notifies account managers when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes;
i) Authorizes access to the information system based on a valid access authorization, intended system usage, and other attributes as required by the organization;

j) Reviews accounts for compliance with account management requirements periodically; and,

k) Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

l) Restrictions on the use of shared accounts such as defining the specific criteria that must be met in order to use a shared account and termination of the shared account credentials when members leave the group.

Password Strength the organization employs the principle of strong passwords, requiring credentials of reasonable complexity and inactivity-based log-out.

Separation of Duties the organization documents separation of duties of individuals and defines information system access authorizations to support separation of duties. Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.

*Least Privileg*e the organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Access Restrictions for Change the organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Organizations should maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes.

Audit Events the organization:

a) Determines that the information system is capable of auditing organization-defined auditable events;

b) Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

c) Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and,

d) Determines that the organization-defined audited events are to be audited within the information system along with the frequency of (or situation requiring) auditing for each identified event.

Audit Review, Analysis, and Reporting the organization reviews and analyzes information system audit records periodically for indications of inappropriate or unusual activity and reports findings to the appropriate personnel or role within the organization. Information security-related auditing performed by organizations can include, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP.

Condition

Systems impacted: The specific information systems impacted by the below findings were provided separately to management. In addition, the Grant Thornton team met with individual system owners and points of contact to discuss the nuances of these findings which varied slightly based on information system use, architecture, and other factors.

System authorization, access, and account management controls must be used to limit system activities to ensure legitimate use, least privilege, and segregation of duties. Access controls provide assurance that critical systems assets are safeguarded and that logical access to sensitive applications, system utilities, and data is provided only when authorized and appropriate. Further, broad or special (privileged) access privileges, such as those associated with operating /database system software, administrative accounts, and /or superusers, may allow normal controls to be overridden or otherwise circumvented. Additionally, a lack of logging and monitoring broad or privileged access may result in unusual or suspicious activity going unidentified. Grant Thornton noted the following. Grant Thornton noted Management should address the following:

Account Management

- Management did not have a process to consistently document and retain approvals related to initial authorization and ongoing changes to user's access for seven systems tested.
- Management did not perform periodic access recertification for users (including privileged users) and system accounts for 11 systems tested.
- Management did not define the timeframe in which a separated employee or contractor's access from the Network must be disabled after separation and the timeframe in which a reassigned employee's access must be reviewed and updated after reassignment.

Password Configuration

Grant Thornton noted that there was no consistent password policy City-wide for the systems identified above. As a result we noted that password security configuration settings were not consistently aligned with best practices across the network, platforms, and devices. Specifically, we noted information systems did not meet some or all of the following:

- Minimum length requirements
- Enforce the use of alpha numeric characters
- Restrict the use of common words; and,
- Apply password expiration

In addition, we noted that information systems did not log users out after a period of inactivity or lock users out after a set number of failed password attempts.

Broad / Privileged User Accounts

- For one system tested we noted the IT team had access to the operating system and the database.
- Management did not consistently segregate system management functions such as user and system administration from functional responsibilities for seven systems tested. Further system users had IT administrative responsibilities.
- We noted that a system / tool was utilized to make direct changes to production data for a system tested. This tool enables users to bypass transactions made via the applications in the normal course of business, circumvent manual controls in place and update data directly in the database. Per discussion with Management, users require approvals before making changes to data via this tool; however; there were no systematic restrictions that required approvals prior to the updates being made.

Shared Accounts

- We noted instances where systems utilized shared accounts which negate accountability of use. Specifically a shared account was used to make direct data changes via the tool described above and to transfer information into systems.

Audit Logging and Monitoring

- Management did not log and/or monitor activities associated with privileged user accounts (e.g. system administrators, user administrators, network administrators, operators, and developers) for four systems tested. Further one system had limitations which did not allow it to log activities.
- We noted a lack of formally defined auditable events (such as privileged use, invalid password attempts, key configuration changes, or changes made directly to financial data), investigation and analysis processes.

Cause

- Management had not implemented a policy and procedures that appropriately documents account management requirements as part of their internal control framework.
- Management had not defined City-wide password security configurations. Additionally, some information systems did not have the technical capability to enforce password configuration best practices.
- Management had not defined requirements for privileged user accounts, shared accounts, logging/ monitoring, and segregation of duties in policy and procedures.

Effect or Potential Effect

Account Management

- Without formally completing or approving access requests, changes or timely terminations of access, there is an increased risk of inappropriate or unauthorized access to information systems and financial data.
- Without a periodic review of user and system accounts, there is a greater probability that an access change made in error would not be identified in a timely manner.
- Without defining the requirements around logical and physical access removal for separated or reassigned employees and contractors, there is an increased risk that access will not be removed or will not be removed in a timely manner. This access may allow inappropriate access to execute system functions. This could also lead to a license violation issue.

<u>Password Configuration</u>
Failure to implement recommended security settings and best practices for passwords increases the likelihood of account compromise by malicious users

<u>Broad / Privileged User Accounts</u>

- Failure to effectively restrict access to applications based on job function and employ adequate segregation of duties increases the risk for abuse of system privileges, fraud, and inappropriate activity without collusion.
- Direct data changes bypass system transactions and controls and therefore increase the risk of inappropriate updates to data. This may impact the organization's ability to rely on the completeness, accuracy, and validity of financial data. Further, the use of shared user accounts on a production system reduces the audit and accountability of users within the system and password security. In other words, there is no traceability of user's activity to perform these changes to production data.

<u>Shared Accounts</u>
Shared accounts negate accountability of use in that Management is not able to identify the user that made changes.

<u>Audit Logging and Monitoring</u>
Failure to maintain adequate logging and monitoring of higher risk application events and privileged access increases the risk that suspicious activities may not be identified and investigated.

This could lead to errors, data loss, inappropriate access, and other risks with the potential to impair the confidentiality, integrity, and availability of systems and data. These issues may result in unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems, which may lead to misstatements on the financial statements.

Management Response

Individual items are accurate and Management concurs with the Audit Criteria. Nonetheless, overall risk of occurrence and impacts of occurrence are most probably minor in the context of financial reporting—e.g. limits on network access restrict non-employee access; database edits would cause anomalies that would evidence elsewhere in reporting; small staff sizes extant in the City demands some roles be combined; and no evidence has emerged of any malicious activity.

Management agrees with the need to develop mature Access Control processes and Awareness and Training.

Finding 2016-003 Information Technology: Change Management

Criteria

Internal controls over financial reporting are reliant on IT controls which are designed effectively. In that regard, an effectively designed IT environment is one where an organization:

a) Determines the types of changes to the information system that are configuration-controlled;

b) Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;

c) Documents configuration change decisions associated with the information system;

d) Implements approved configuration-controlled changes to the information system;

e) Retains records of configuration-controlled changes to the information system for an organization-defined time period;

f) Audits and reviews activities associated with configuration-controlled changes to the information system; and,

g) Coordinates and provides oversight for configuration change control activities through an organization-defined configuration change control element (e.g., committee, board).

Condition

Systems impacted: The specific information systems impacted by the below findings were provided separately to management. In addition, the Grant Thornton team met with individual system owners and points of contact to discuss the nuances of these findings which varied slightly based on information system use, architecture, and other factors.

Change management processes provide assurance that software, data, and other changes associated with information systems are approved and tested so they do not introduce functional or security risks. A disciplined process for testing, approving, and migrating changes between environments, including into production, is essential to ensure that systems operate as intended and that no unauthorized changes are implemented.

Grant Thornton noted that Management did not have a process to consistently document and retain evidence related to change management activities including change request and approval, scheduling, initiation, testing, implementation approvals and post-implementation review for eight systems tested. In addition, we noted that City personnel do not have access to source code for one system tested, which is handled by the vendor, but were responsible for user acceptance testing and certain approvals, which were not consistently documented and retained.

Cause

As part of the internal controls framework, management has not incorporated a policy and procedure to periodically monitor and review the configuration items that are migrated to production. Additionally, IT personnel did not consistently document and retain evidence related to change management activities (e.g. change request and approval, scheduling, initiation, testing, implementation approvals and post-implementation review).

Effect or Potential Effect

Without formally completing or approving change management activities for system changes, patches and modifications, there is an increased risk that change management controls will not be completed. Without effective control over changes that are migrated to the production environment, there is an increased risk that an inappropriate code change could be introduced into the production environment, potentially impacting the financial statement and related processes (i.e. cash accountability, financial reporting, etc.).

Norman Y. Mineta San José International Airport
Schedule of Findings
Year Ended June 30, 2016

Inappropriate code change could have a negative impact on system functionality, availability, or ability to produce complete and accurate financial data. These issues may result in unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems, which may lead to misstatements on the financial statements.

Management Response

Comments are accurate and Management concurs with the Audit Criteria. However, overall risk of occurrence and impacts are most probably minor in the context of financial reporting—e.g. change controls occur on a technical level across system and application teams for major changes; backups are available in the event a critical restore of data is required; erroneous changes would likely cause data anomalies elsewhere in financial reports that would trigger review; and no evidence has emerged of any malicious activity.

Management agrees with the need to develop mature Information Protection Processes and Procedures and Awareness and Training. The City will commence implementation of appropriate tools, controls, and training of essential personnel.