# City of New York

## OFFICE OF THE COMPTROLLER

**Scott M. Stringer**
**COMPTROLLER**

## AUDITS AND SPECIAL REPORTS

## IT AUDIT

**Marjorie Landa**
Deputy Comptroller for Audit

# Audit Report on the Department of Citywide Administrative Services' Development and Implementation of the Archibus System

SI19-059A

**June 27, 2019**

**https://comptroller.nyc.gov**

THE CITY OF NEW YORK
**OFFICE OF THE COMPTROLLER**
SCOTT M. STRINGER

June 27, 2019

To the Residents of the City of New York:

My office has audited the New York City Department of Citywide Administrative Services' (DCAS') development and implementation of the Archibus system to determine whether the system meets its overall goals, and whether it has adequate functions to ensure that the information process is reliable and secure from unauthorized access. We perform audits such as this to ensure that the City agencies' systems, technology development, and resources are efficient, secure, and operate in the best interest of the public.

The audit found that although Archibus was generally meeting its overall business goals as stated in the specifications, it had not been fully utilized by the business units for which it was intended. Further, DCAS did not adequately consider and plan for certain business and security requirements, which contributed to the more than three-year delay and its increased cost. In addition, the system failed to perform input verification to ensure that the dates entered into the records it maintains correspond to a valid time frame.

DCAS has established policies and procedures to prevent unauthorized access to the system; however, we found access and security control weaknesses. Specifically, DCAS did not periodically review user account activities and did not promptly address the risks identified in the vulnerability scans. Finally, DCAS did not have a disaster recovery plan for Archibus in the event of an emergency.

The audit made 14 recommendations, including that DCAS should: ensure that the remaining Archibus modules are completed and meet the new projected timeline by November 2019; develop a date verification rule to ensure that only valid dates can be entered into the system's date fields; ensure that each user's initial password is changed immediately upon the first login and that the password is required to change every 90 days; ensure that all inactive user accounts are immediately disabled; and periodically perform vulnerability scans and promptly remediate the risks identified.

The results of the audit have been discussed with DCAS officials, and their comments have been considered in preparing this report. Their complete written response is attached to this report.

If you have any questions concerning this report, please e-mail my Audit Bureau at audit@comptroller.nyc.gov.

Sincerely,

Scott M. Stringer

# TABLE OF CONTENTS

# THE CITY OF NEW YORK
# OFFICE OF THE COMPTROLLER
# AUDITS AND SPECIAL REPORTS
# IT AUDIT

## Audit Report on the Department of Citywide Administrative Services' Development and Implementation of the Archibus System

## SI19-059A

# EXECUTIVE SUMMARY

We audited the New York City Department of Citywide Administrative Services' (DCAS') development and implementation of the Archibus system to determine whether the system meets its overall goals, and whether it has adequate functions to ensure that the information process is reliable and secure from unauthorized access.

DCAS is responsible for, among other things, procuring goods and services for City agencies and managing City-owned office buildings. DCAS' Facilities Management Division is responsible for facilities operations and management, including the provision of maintenance and construction services for the tenants in 55 DCAS-managed buildings.

To accomplish its work, the Facilities Management Division utilized multiple computer systems to process, monitor, and track work order requests. DCAS entered into a contract with Computerized Facility Integration, LLC (CFI) to implement a new commercial off-the-shelf (COTS) system, Archibus, to improve and centralize the business operations, including work requests, of the Facilities Management Division.[1] Archibus was implemented in February 2017.

## Audit Findings and Conclusions

Our audit determined that although Archibus was generally meeting its overall business goals as stated in the specifications, it had not been fully utilized by the business units for which it was intended. Further, DCAS did not adequately consider and plan for certain business and security requirements, which contributed to the more than three-year delay in the project's development and deployment and its increased cost. In addition, we found the system failed to perform input verification to ensure that the dates entered into the records it maintains corresponded to a valid time frame.

[1] Commercial off-the-shelf (COTS) refers to software or hardware products that are ready-made and available for sale to the general public.

We also found that while DCAS has established policies and procedures to prevent unauthorized access, the system nevertheless has access control weaknesses, in that: external institution users were not required to change their passwords; DCAS did not periodically review all Archibus user account activities; and DCAS did not update the list of other agencies' tenant liaisons, who are responsible for validating the identities of their agencies' users and for notifying DCAS when to create or disable their accounts. Further, our audit found that DCAS did not promptly address the risks identified in the vulnerability scans and did not have a disaster recovery plan for Archibus in the event of an emergency.

Finally, we conducted a User Satisfaction Survey and only 34 percent of respondents indicated that the Archibus is very easy to use, while 30 percent of respondents reported that the data in the system is always accurate.

## Audit Recommendations

To address the issues, we made 14 recommendations to DCAS, including the following:

- Ensure that the remaining Archibus modules are completed and meet the new projected timeline by November 2019.

- Ensure that all future system developments and enhancements are properly planned to include all business and system requirements.

- Develop a date verification rule to ensure that only valid dates can be entered into the system's date fields.

- Comply with the Department of Information Technology and Telecommunications' (DoITT's) *Password Policy* to ensure that each user's initial password is changed immediately upon the first login and that the password is required to change every 90 days.

- Enforce the policy that requires inactive user account recertification to be performed every 90 days.

- Ensure that all inactive user accounts are immediately disabled.

- Periodically perform vulnerability scans and promptly remediate the risks identified in accordance with DoITT's *Application Security Policy*.

- Develop a formal Disaster Recovery Plan for Archibus to ensure the operational ability in the event of a disaster, emergency, or system failure.

## Agency Response

In its response, DCAS agreed with eight recommendations, partially agreed with one recommendation, and disagreed with the remaining five recommendations. In addition, DCAS disagreed with certain of our findings related to the system development and implementation issues including those concerning project delay, module usage, and data fields. After carefully reviewing DCAS' response, we find no basis to change any of the report's findings. The full text of DCAS' response is included as an addendum to this report.

# AUDIT REPORT

## Background

DCAS performs a wide range of administrative functions for City government and had 2,420 employees as of Fiscal Year 2018. DCAS is responsible for, among other things, procuring goods and services for City agencies and managing City-owned office buildings. DCAS' Facilities Management Division is responsible for facilities operations and management, including the provision of maintenance and construction services for the tenants in 55 DCAS-managed buildings. The Facilities Management Division is also responsible for asset acquisitions, building safety compliances, and project management.

To accomplish its work, the Facilities Management Division utilizes multiple computer systems and methods to process, monitor, and track work order requests. DCAS entered into a contract with CFI, for $996,540 (covering July 2, 2015 to July 1, 2016) that required CFI to implement a new commercial off-the-shelf system, Archibus, to improve and centralize the business operations of the Facilities Management Division. The contract was subsequently extended by DCAS to July 1, 2017 and the total cost of the application was increased to approximately $1.5 million to include additional security requirements and system enhancements.

Archibus was implemented in February 2017 to automate and centralize the work request process. The system is used by DCAS employees, employees of other City agencies, and employees of external institutions to monitor and track work order requests. DCAS' goal for Archibus is to standardize equipment and building maintenance, inventory management, and project management processes for the DCAS Facilities Management Division.

According to the DoITT's *Citywide Information Security Policy*, information stored in an agency's computer applications must be placed in a secure environment and protected from unauthorized access. To accomplish that level of security, adequate access controls, such as user-authorization, identification, authentication, access-approval, and login credentials are essential. DCAS is also responsible for ensuring that it has policies and procedures in place to protect information in the agency's computerized environment, which includes complying with DoITT's policies and standards.

## Objectives

The objectives of this audit were to determine whether Archibus:

1. Meets its overall goals as stated in the system specifications; and
2. Has adequate functions to ensure the information process is reliable and secure from unauthorized access.

## Scope and Methodology Statement

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. This audit was conducted in accordance with the audit responsibilities of the City Comptroller as set forth in Chapter 5, § 93, of the New York City Charter.

The scope of this audit was from the system development and implementation of Archibus in July 2015 through April 30, 2019. Please refer to the Detailed Scope and Methodology at the end of this report for the specific procedures and tests that were conducted.

## Discussion of Audit Results

The matters covered in this report were discussed with DCAS officials during and at the conclusion of this audit. A preliminary draft report was sent to DCAS officials and discussed at an exit conference held on May 30, 2019. On June 7, 2019, we submitted a draft report to DCAS with a request for comments. We received a written response from DCAS on June 21, 2019. In its response, DCAS agreed with eight recommendations, partially agreed with one recommendation, and disagreed with the remaining five recommendations. DCAS stated, "We are pleased that the auditors found that DCAS' Archibus system is meeting its overall business goals; however, throughout the report, there are misrepresentations that we believe require clarification."

Specifically, DCAS disagreed with our findings related to system development and implementation issues, including project delay, issues concerning module usage and data fields, and our user satisfaction survey, stating, "Some of the items listed as findings appear to be based on the auditors' opinions rather than on solid criteria (requirements)."

As discussed with DCAS officials throughout the course of the audit, the criteria we use, all of which we cite in the report, include but are not limited to the minimum requirements established by DCAS and DoITT policies. For purposes of generally accepted government auditing standards, "Criteria represent the laws, regulations, contracts, grant agreements, standards, specific requirements, measures, expected performance, defined business practices, and benchmarks against which performance is compared or evaluated." Accordingly, our use of DCAS' contract documents and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 as criteria for the development of our findings on issues such as system development and implementation and controls relating to data fields is consistent with generally accepted government auditing standards. Similarly, our user satisfaction survey, which we shared with DCAS before distributing it, was used for purposes of measuring and comparing the Archibus system's expected and actual performance as part of an assessment of whether it meets its overall goals.

We address each of DCAS' concerns in the body of the report. After carefully reviewing DCAS' response, we find no basis to change any of the report's findings.

The full text of DCAS' response is included as an addendum to this report.

# FINDINGS AND RECOMMENDATIONS

Our audit found that although Archibus was generally meeting its overall business goals as stated in the specifications, it had not been fully utilized by the business units for which it was intended. Further, DCAS did not adequately consider and plan for certain business and security requirements, which contributed to the more than three-year delay in the project's development and deployment and its increased cost. In addition, we found the system failed to perform input verification to ensure that the dates entered into the records it maintains correspond to a valid time frame.

DCAS has established policies and procedures to prevent unauthorized access to the system. However, we found access control weaknesses, in that external institution users (i.e., employees of non-profit organizations, the New York State Courts, and other organizations) were not required to change their passwords; DCAS did not periodically review all Archibus user account activities; and DCAS did not update the list of other agencies' tenant liaisons, who are responsible for validating the identities of their agencies' users and to notify DCAS when to create or disable their accounts. Further, our audit found that DCAS did not promptly address the risks identified in the vulnerability scans that DoITT conducted for the system and did not have a disaster recovery plan for Archibus in the event of an emergency.

In addition, we conducted a User Satisfaction Survey and only 34 percent of respondents indicated that the Archibus is very easy to use, while 30 percent of respondents reported that the data in the system is always accurate.

## System Development and Implementation Issues

DCAS followed a system development life cycle (SDLC) framework along with a project management approach when developing and implementing Archibus.[2] Nevertheless, the project was delayed by more than three years. DCAS officials stated that due to an agency reorganization, they were not able to meet the expected completion schedules. The agency provided a new estimated timeframe to fully utilize the system to all intended units by November 2019.

> ***DCAS Response***: "There are multiple references in the report to a 3 year delay in DCAS' deployment of the system. DCAS initiated a 1 year extension for the development and deployment of additional requirements identified during the requirements validation phase of the project. Archibus was deployed 1 year after original deployment date, due to an increased scope of work."
>
> ***Auditor Comment:*** Although Archibus was partially deployed one year after the original deployment date, it was not at that time available for all the intended users. Further, our audit found that as of February 2019, the Inventory Management module was used by only two of the six intended business units, and the Mobile module was still in the pilot phase. As stated in the report, DCAS provided a new estimated time frame for fully utilizing these modules for all intended business units by November 2019, three years after the original deadline of July 2016.

[2] SDLC is used during the development of an IT project, it describes the different stages involved in the project. DCAS identified six phases of the SDLC framework: planning, design, system configuration, testing, production roll-out, and maintenance support.

## System Development Issues

DCAS initially planned to implement Archibus by July 2016, a milestone that was later extended to July 2017 to enhance the system's business modules and fulfill the project's business specifications and system's security requirements. Among other things, DCAS did not have an anti-virus solution to scan documents when users uploaded them into the system. The required scan would protect against potential virus and malware threats to the system and its environment. DoITT's *Standard Requirements* states that, "[a]ll files uploaded to DoITT servers must be scanned for viruses at the time the file is uploaded." Further, the Conditional Assessment module, documented in the business requirements, was tested and implemented but was not utilized. According to DCAS officials, similar features in the Preventive Maintenance module can adequately substitute the documented needs in the Conditional Assessment module. In both of the abovementioned instances—the absence of the required anti-virus scanning solution from the system's design, and the inclusion of a reportedly unnecessary module—DCAS did not adequately consider and plan for the inclusion of the specific business and security features it needed, which contributed to the project's delay its increased cost.

## System Implementation Issues

In addition, the Archibus contract specifications states that, "[a]t the completion of this phase [Phase 5: Transition to Operations Plan for Data Collection], the system will Go-Live for all DCAS end users with all the necessary data and system enhancements identified during the previous project phases." However, as of February 2019, Archibus had not been fully utilized by the business units for which it was intended. Specifically, we found that 3 of 11 modules—Contract Management, Inventory Management, and Emergency Preparedness—were not fully used by the intended business units. These three modules were operational but lacked some of the essential data and provision for the specific training that some of the intended users would need in order to fully use them. For example, as of February 2019, the Inventory Management module was fully used by only two of the six intended business units. Without all the necessary data available, DCAS and its business units could not fully use the system to properly monitor and plan for the agency's inventory consumption and lifecycle as intended.

Furthermore, we found that 2 of the system's 11 modules—Preventive Maintenance and Mobile—were still in the pilot phase as of February 2019. The Mobile module is intended to allow the user to create, update, and close work orders at field locations. Without full roll-out of this module, the intended users will not be able to use the system to expedite the work order effectively in the field.

On April 15, 2019, DCAS officials informed us that the Contract Management, Emergency Preparedness, and Preventive Maintenance modules were being used by all intended units. However, absent proper planning throughout the SDLC, DCAS incurred increased risks of project delays and ineffective utilization of the resulting system.

> ***DCAS Response:*** "The auditors stated that without a full roll-out of Archibus' Mobile module, the intended users would not be able to use the system to expedite work orders effectively in the field. However, the auditors were advised that the mobile application was intended to be an additional tool for staff to access Archibus in the field. It was never stated that this module would be the sole means of creating work orders. Users in the field have access to computers and can process work orders without the use of the mobile app."

***Auditor Comment:*** The Mobile module is intended by DCAS to enable users to create and process work orders through a mobile device, including when computers they might otherwise use are not accessible. Without a full roll-out, users' ability to expedite work orders effectively in the field will be negated in those circumstances and diminished overall.

## Data Field Issues

The NIST SP 800-53 states, "Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content." Our tests found data input verification issues in some of the date fields that failed to automatically flag and reject impossible dates. For example, Archibus allowed a supervisor to schedule a work order for a craftsperson to start on 1/1/1800 and finish on 12/31/9999. Allowing the system to accept impossible or facially invalid dates, e.g. thousands of years in the future, can impair its ability to properly monitor work orders. Data verification is used for a system as a best practice to minimize data entry errors, ensure the dates meet certain range criteria, and improve the accuracy of the data in the system.

***DCAS Response:*** "The auditors referenced the National Institute of Standards and Technology (NIST) SP-800-53 when citing DCAS for data input verification issues; however, this is a federal standard (recommended practice) that City agencies are not mandated to follow. DCAS chose not to implement this standard, as it was not conducive to business operations."

***Auditor Comment:*** DCAS chose not to implement the NIST standard that would not only ensure that the data entered into the system, such as a work order date, has acceptable values, but would also help the agency maintain system security and protect its operations and functions from the negative effects of data corruption due to human error, both intentional and unintentional. Further, the NIST publication describes methods for developing specialized sets of controls tailored for specific types of missions and business functions. Data verification is a critical and widely used safeguard to minimize data entry errors, for example, by requiring dates to meet certain range criteria, and thereby improve the accuracy of the data in the system. By allowing the system to accept impossible or facially invalid dates, DCAS diminishes its ability to properly monitor work orders. Addressing security, functionality, and quality-assurance issues through the use of sound system- and security-engineering principles helps to ensure that information technology component products and the systems built from them are sufficiently trustworthy to achieve their intended purposes.

In addition, we found unused data fields in several modules. DCAS did not disable these unused fields to prevent users from entering information erroneously into them. Without disabling the unused fields, the system is at risk of containing inaccurate information that may corrupt the integrity of the data.

## Recommendations

DCAS should:

1. Ensure that the remaining Archibus modules are completed and meet the new projected timeline by November 2019.

***DCAS Response:*** DCAS disagreed with this recommendation, stating, "All of the Archibus modules are complete and available for use. DCAS will continue to utilize the modules in accordance with its business needs."

***Auditor Comment:*** As stated above in the report, as of February 2019, the Inventory Management module was used by only two of the six intended business units and the Mobile module was still in pilot phase. Therefore, we continue to recommend that DCAS complete any remaining the modules within its own projected timeline.

2. Ensure that all future system developments and enhancements are properly planned to include all business and system requirements.

***DCAS Response:*** DCAS disagreed with this recommendation, stating, "DCAS makes every effort to ensure that all system developments and enhancements are appropriately planned. The development of the Archibus system was based upon the business needs of the Agency at the time; however, as discussed with the auditors, the business needs changed due to reorganization in the Agency."

***Auditor Comment:*** Although DCAS attributes the project delay to agency reorganization, our audit found that DCAS did not adequately consider and plan for the inclusion of specific business and security features it needed, which also contributed to the project delay.

3. Develop a date verification rule to ensure that only valid dates can be entered into the system's date fields.

***DCAS Response:*** DCAS disagreed with this recommendation, stating, "The auditors did not test the validity of information entered into the system. Rather, the auditors tested the system's ability to accept backdated information. The system allows back dating to support current business practices and processes. The date fields are calendar fields where users are required to select or type month, day and year for system to save the dates. Additionally, the data goes through multiple levels of approval and validation."

***Auditor Comment:*** As stated in the report, our audit found that Archibus accepted impossible or facially invalid dates, such as 1/1/1800 and 12/31/9999, which can impair its ability to properly monitor work orders. Date verification is a best practice to minimize data entry errors, ensure dates meet certain range criteria, and improve the accuracy of the data in the system. Therefore, we continue to recommend that DCAS develop a date verification for the system.

4. Reassess and develop criteria to prevent users from erroneously inputting data into the unused fields.

***DCAS Response:*** DCAS disagreed with this recommendation, stating, "Archibus is a COTS product that provides numerous out of the box fields to provide users with the flexibility to use these fields as part of business operations, as necessary, without costly customizations. Keeping this out of the box functionality allows organizations to quickly adapt to changing business needs using the available technology and resources. The out of the box fields that are not being used in Archibus are not critical to DCAS' current business needs but may be useful in the future. Additionally, removing or updating unused fields throughout the application would require unnecessary and costly customizations."

> ***Auditor Comment:*** To minimize the risks associated with the entry of erroneous information into its system, DCAS should find alternative solutions to costly customization to prevent users from erroneously entering data into the unused fields.

## Access Control Weaknesses

DCAS has established access control policies, procedures, and guidelines for Archibus. However, we found several access control weaknesses. Specifically, DCAS failed to comply with DoITT's *Password Policy*, maintained insufficient oversight of user accounts, and its designated liaison list was not up-to-date. These issues are discussed in greater detail below.

### Password Expiration Is Not Set for External Institution Users

DoITT's *Password Policy*, states that temporary or initial user account passwords and PINs, "must be set to expire after initial use." The policy further states, "User Account passwords and/or PINS must expire at least every 90 days." However, DCAS did not enforce this policy to require their external institution users to change their passwords after their initial use; moreover, the password entered by the external institution user does not expire. DCAS officials stated that, instead, a password is assigned to each external user during the initial account creation. We found that those initial passwords do not expire, and that the users are not required to periodically change their passwords. Strongly-enforced password controls for external institution users, who are not City employees, are essential for the protection of agency information. Conversely, without enforcement of City password-control policy, DCAS incurs an increased risk of unauthorized access to its system and the data within it.

### Inadequate Oversight of User Accounts

DoITT's *Identity Management Security Policy* states that "[u]ser accounts will be created and de-provisioned in a timely manner." Currently, Archibus' provisioning policy requires a formal request from the business unit to the Archibus IT unit for creating a new user account. However, DCAS could not provide documentation for 4 out of 18 new user accounts that were created from June 1, 2018 to October 10, 2018. DCAS officials informed us that they could not find the supporting documentation to justify the creation of these accounts. Without proper documentation for tracking access requests, the agency may be at risk of granting access to users that are not authorized.

Furthermore, the system policy requires that the Archibus IT unit conduct a 90-day inactive user recertification to ensure that only authorized users have access to Archibus. However, we found that DCAS failed to have its Archibus IT unit follow that policy. Archibus IT attempted to verify 517 user accounts that had been inactive for over 6 months only after we formally initiated this audit on July 20, 2018. Subsequently, DCAS disabled 494 out of those 517 inactive user accounts.

Without periodically reviewing users' activities and promptly disabling the accounts of users who no longer need access to the system, DCAS may be at risk of an unauthorized user's accessing the system.

## Outdated List of Tenant Liaisons

DoITT's *Identity Management Standard* states, "[a]ll non-employee accounts (both onsite and offsite) must be reviewed periodically by the authorizing employee/manager to ensure access rights are still appropriate and the account is still needed." Our audit found that DCAS did not have an up-to-date list of Archibus's external tenant liaisons—individuals employed by other City agencies and by institutions who are authorized to request that DCAS provide access to the Archibus system for individuals working for their organizations.

To use the system, employees of other City agencies and external institutions must request access through their designated tenant liaisons. DCAS depends on these external liaisons to validate the identities of their organizations' users and to notify DCAS when to create or disable their accounts. Our analysis of the current list of 70 City agency tenant liaisons found that as of October 23, 2018, 5 liaisons no longer worked for their agencies and 4 of those 5 had left their agencies over a year earlier. However, those five individuals were still authorized, as far as DCAS was concerned, to request access for employees of the agencies where the liaisons no longer worked. Furthermore, we found that six City agencies and two external institutions did not have tenant liaisons responsible to notify DCAS to create or disable user accounts when warranted. Without maintaining a complete and accurate list to ensure that only authorized individuals can request access to Archibus, DCAS incurs an increased risk that unauthorized users may be given access to the system.

In addition, DoITT's *Identity Management Security Policy* states that "[u]ser accounts will be created and de-provisioned in a timely manner." Our audit found that two users were no longer working for their assigned agencies. They included one user whose account was used on October 5, 2018 had been on childcare leave since July 2015—more than three years earlier. Without proper monitoring to ensure that only authorized users have access to Archibus system, DCAS will incur an increased the risk of unauthorized access.

> ***DCAS Response:*** "The auditors told DCAS staff that they had conducted a search for Archibus users and their employment statuses in the City's Payroll Management System. In the report, the auditors stated that they found that one Archibus user, whose account was used on October 5, 2018, had been on childcare leave since July 2015, more than three years earlier. However, DCAS staff confirmed, through the user's agency, that the staff person had not been on child care leave. Rather, another employee with the same last name (who did not have access to Archibus) was actually on leave."
>
> ***Auditor Comment:*** As stated in the report, we found that one user was on child care leave since July 2015, and the user's account was last used in October 2018. We performed a PMS match based on the user profile provided by DCAS, which included the user's *full* name and the corresponding agency. We found that only one person within that agency matched the user profile we received from DCAS. We provided this information to DCAS officials in a preliminary draft report and thus, if the agency believed there to be an error, it had ample opportunity to alert us to it and provide us with documentation to support its claim. Therefore, we cannot credit DCAS' recent, contrary, unsupported assertion regarding the user's identity.

## Recommendations

DCAS should:

5. Comply with DoITT's *Password Policy* to ensure that each user's initial password is changed immediately upon the first login and that the password is required to change every 90 days.

   ***DCAS Response:*** DCAS partially agreed with this recommendation, stating, "All users will now be able to self-manage their passwords. For internal users, passwords have always been managed through LDAP user account management procedures.[3] This has forced users to change their passwords every 90 days. External users must now self-manage their passwords through NYC ID or LDAP. According to DoITT's external ID management and password policy, these passwords need not expire."

   ***Auditor Comment:*** We are pleased that DCAS has revised its policy to allow users to self-manage their passwords. However, DCAS' response does not state whether it will also ensure that each user's initial password is changed immediately upon the first login as required by DoITT's *Password Policy*. We urge DCAS to implement that portion of the recommendation.

6. Enforce the policy that requires inactive user account recertification to be performed every 90 days.

   ***DCAS Response:*** DCAS agreed with this recommendation, stating, "DCAS will review account activity every 90 days and deprovision users that did not log into the system during that period."

7. Ensure that all inactive user accounts are immediately disabled.

   ***DCAS Response:*** DCAS agreed with this recommendation, stating, "For internal users, deprovisioning has occurred primarily through LDAP user account management procedures. As part of these procedures, when users leave the City or have not logged into the network in the last 90 days, the users were deprovisioned from any systems on the network, including Archibus. Because the external users are tenants that may periodically request maintenance work, DCAS would only disable external users upon receipt of a request. DCAS will now deprovision all users (whether internal or external) that have been inactive for 90 days. DCAS will also continue to disable user accounts upon request."

8. Ensure that accounts are created only for authorized users and that all account creations are properly documented.

   ***DCAS Response:*** DCAS agreed with this recommendation, stating, "DCAS has implemented a formal policy for user access requests which includes each user's completion of a signed access request form."

9. Promptly communicate with each City agency and external entity to update their tenant liaison information.

[3] LDAP (Lightweight Directory Access Protocol) refers to an Internet protocol for accessing distributed directory services. LDAP is used to manage user accounts, track login information, establish access permissions, and enable applications to authenticate users.

***DCAS Response:*** DCAS agreed with this recommendation, stating, "DCAS has contacted the City agencies and other external entities that use Archibus to request updates to their liaison information."

10. Develop a procedure to ensure that the City agencies' and external entities' designations for their authorized liaisons are promptly updated when changes occur.

    ***DCAS Response:*** DCAS agreed with this recommendation, stating, "Previously, DCAS relied on City agencies and other external entities to provide updates to liaison information when staffing changes occurred. DCAS will now periodically contact City agencies and other external entities and request that they confirm or update this information."

# System Vulnerability Issues

DoITT's *Vulnerability Management Standard* requires that, "[a]ll City of New York information systems must be monitored for vulnerabilities to maintain their operational availability, confidentiality, and integrity." A vulnerability scan can help analyze, identify, and classify security weakness and threats.

The *McAfee Vulnerability Manager Reports* for October 2018 provided by DCAS identified high and medium risks in Archibus servers, such as several missing security updates and patches. However, we found that DCAS did not immediately address and resolve those vulnerabilities. We discussed these issues with DCAS officials, and they provided documentation to show that these risks were resolved three months later in February 2019.

DoITT's *Vulnerability Management Standard* requires that, "[s]cans will open tickets for identified vulnerabilities with severity level 4 or 5, and assign them to the business unit manager. These vulnerabilities tickets should be resolved and the asset re-scanned within seven days." Without periodically conducting vulnerability scans and promptly addressing the risks identified in the scans, DCAS may be at risk of security breaches from internal and external sources.

## Recommendation

11. DCAS should periodically perform vulnerability scans and promptly remediate the risks identified in accordance with DoITT's *Application Security Policy*.

    ***DCAS Response:*** DCAS agreed with this recommendation, stating, "DCAS has had several safeguards in place to protect the Agency from security breaches. The application's servers are hosted at DoITT's Data Center, which are monitored and protected by DoITT. Additionally, DCAS utilizes several host-based and network-based intrusion detection and intrusion prevention systems to protect against attacks. DCAS has now additionally appointed a windows security administrator to periodically scan this application. Any risks identified in the scans will be addressed promptly."

# Lack of Disaster Recovery Plan

DoITT's *Application Security Policy* mandates that "[a]pplication business owners must ensure that each application has a defined Business Continuity Plan and a Disaster Recovery Plan to ensure its readiness to respond to events that could disrupt the application's service continuity."

Although DCAS provided a Business Continuity Plan for its Archibus system, it did not have a Disaster Recovery Plan. Such a plan should specify the steps that need to be taken to quickly resume operations without material loss of computer data in the event of emergency or system failure. Without such plan, DCAS is vulnerable to the loss of information and the system operational ability should such an event occur.

### Recommendation

12. DCAS should develop a formal Disaster Recovery Plan for Archibus to ensure the operational ability in the event of a disaster, emergency, or system failure.

    ***DCAS Response:*** DCAS agreed with this recommendation, stating, "DCAS has been working with DoITT to secure a formal Disaster Recovery Plan for Archibus and will continue to do so until a plan is in place."

## User Satisfaction Survey

We conducted a user satisfaction survey to determine whether Archibus was meeting the users' needs, and whether it has adequate functions to ensure the information processing performed through the system is reliable. We distributed the survey to all 496 users DCAS identified as of October 10, 2018. As of February 8, 2019, we received 149 responses (30 percent). In the survey, 73 percent of respondents indicated that the layout of the information displayed on the Archibus screens is easy to work with.[4] However, only 34 percent of respondents felt that the system is very easy to use. The survey also found:

- 30 percent of respondents reported that the system does not have all the functions they need to complete their job responsibilities;
- 30 percent of respondents reported that they were very happy with the system;
- 30 percent of respondents reported that the data in the system is always accurate; and
- 51 percent of respondents reported that the process of entering the data into the system is easy.

We forwarded our survey results to DCAS officials and recommended that they review the issues reported by the respondents.

### Recommendations

DCAS should:

13. Ensure that the user concerns identified in the report are addressed.

    ***DCAS Response:*** DCAS disagreed with this recommendation, stating, "It is not clear that the survey provides useful feedback. For example, one of the questions in the survey asks whether the system has all the functions for the users to complete their job duties. However, it is unclear if the responsibilities of the responders relate to functions that exist in Archibus."

[4] The percentage is calculated according to the number of responses to each individual question.

***Auditor Comment:*** To ensure that our survey questions and survey goal were clear, we discussed the survey with, and forwarded it to, DCAS officials prior to its distribution. The agency did not raise any concerns at that time. The survey results contain useful information and user feedback that DCAS can utilize to improve the system.

14. Periodically conduct a survey to receive feedback from the users.

    ***DCAS Response:*** DCAS agreed with this recommendation, stating, "DCAS will work on a survey to receive user feedback periodically."

# DETAILED SCOPE AND METHODOLOGY

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. This audit was conducted in accordance with the audit responsibilities of the City Comptroller as set forth in Chapter 5, § 93, of the New York City Charter.

The scope of this audit covered the period from the system development and implementation of Archibus in July 2015 through April 30, 2019. To achieve our audit objectives, we:

- Reviewed the DCAS agency-wide organization chart, Facilities Management, and Information Technology (IT) divisions' organization charts to gain an understanding of the management and administration structure of DCAS and the divisions related to Archibus;
- Interviewed various DCAS officials in the agency's Facilities Management Division, Archibus IT unit, and DCAS IT unit to understand their roles and responsibilities;
- Reviewed Archibus system user manuals, training documents, Archibus work request process flowcharts, module description, and functional design document to gain an understanding of the system's usage and functionalities;
- Conducted system walk-through of Archibus to gain an understanding of how DCAS' business units and the personnel performed their tasks and operations;
- Reviewed Comptroller's Directive #1, DoITT's *Password Policy*, DoITT's *Identity Management Security Policy*, DoITT's *Identity Management Standard*, DoITT's *Vulnerability Management Policy and Standard,* and DoITT's *Security Architecture Standard,* DoITT's *Standard and Requirements*, and the NIST Special Publication 800-53 Revision 4 *Security and Privacy Controls for Federal Information Systems and Organizations* to determine the controls that should be in place;
- Reviewed the contract and amendments for Archibus to understand the project scope and contractor's responsibilities;
- Reviewed and analyzed business specification requirements and system specifications stated in the original Request For Proposal for Archibus as a basis to determine whether system deliverables were implemented and completed according to contract plan;
- Reviewed the *Archibus Technical Policies and Procedures* and system security document to understand the internal controls and security configuration that exist in Archibus;
- Reviewed the Archibus user access security matrix to understand the users' roles and accessibilities;
- Reviewed test plans and user acceptance testing sign-off documentation for Archibus to determine whether DCAS had quality assurance controls in place;
- Reviewed data collection plan to verify whether DCAS had processes and procedures in place to protect the data integrity for Archibus;
- Reviewed Archibus' implementation timelines and current modules' usage to determine whether DCAS managed the project accordingly;

- Reviewed and analyzed the security accreditation documentation for Archibus to determine whether DCAS had adequate controls for system operations, data integrity, and data confidentiality in Archibus;
- Performed system function tests in the staging environment to determine whether Archibus fulfilled the business specification requirements;
- Conducted system validation tests to determine whether Archibus had data input checks to prevent incorrect and invalid entries;
- Analyzed and tested the list of 496 active users as of October 10, 2018 against the City's Payroll Management System to determine whether the users were active City employees;
- Reviewed and examined the Archibus user list to determine whether DCAS provided a reasonable assurance to prevent unauthorized access;
- Reviewed account provisioning and de-provisioning procedures to determine whether DCAS had sufficient controls for managing the user accounts;
- Reviewed Archibus user provision and de-provision requests from June 1, 2018 to December 14, 2018 to determine whether DCAS had sufficient access controls to monitor Archibus users;
- Reviewed the Archibus user recertification documentation to determine whether DCAS had adequate access controls in user account management;
- Examined the Archibus tenant liaison list to determine whether DCAS maintained an accurate list;
- Compared the current tenant liaisons for the City agency with PMS to determine whether they were active employees;
- Reviewed the Archibus *IBM AppScan* Report to determine whether DCAS performed system security reviews;
- Analyzed the *McAfee Vulnerability Management Reports* to determine whether DCAS had monitored and addressed the potential risks; and
- Reviewed DCAS' *Archibus Business Continuity Plan* to determine whether DCAS had adequate policies to recover data and continue operations within a reasonable time after disastrous events.

In addition, to determine whether Archibus improved the reliability of information and whether users were satisfied with the system, we conducted a user satisfaction survey. We distributed the surveys to all 496 Archibus users on January 17, 2019 and received 149 responses as of February 8, 2019. The survey also provided information on users' feedback regarding Archibus' usability, information accuracy, sufficiency in training, and effectiveness of troubleshooting.

The results of the above tests, while not projectable to their respective populations, provided a reasonable basis for us to evaluate and support our findings and conclusion about DCAS' development and implementation of Archibus.

NYC DCAS
Citywide Administrative Services

Lisette Camilo
Commissioner

June 21, 2019

Ms. Marjorie Landa
Deputy Comptroller for Audit
Office of the New York City Comptroller
1 Centre Street, RM 1100
New York, NY 10007

RE: Comptroller's Audit on New York Department of Citywide Administrative Services' Development and Implementation of the Archibus System.

Dear Deputy Comptroller Landa:

Thank you for the opportunity to respond to the audit report on the New York Department of Citywide Administrative Services' Development and Implementation of the Archibus System.

We are pleased that the auditors found that DCAS' Archibus system is meeting its overall business goals; however, throughout the report, there are misrepresentations that we believe require clarification. These issues were brought to the auditors' attention at the Exit Conference, but the appropriate changes were not made in the report. I have addressed the most significant misrepresentations below.

- There are multiple references in the report to a 3 year delay in DCAS' deployment of the system. DCAS initiated a 1 year extension for the development and deployment of additional requirements identified during the requirements validation phase of the project. Archibus was deployed 1 year after original deployment date, due to an increased scope of work.

- The auditors stated that without a full roll-out of Archibus' Mobile module, the intended users would not be able to use the system to expedite work orders effectively in the field. However, the auditors were advised that the mobile application was intended to be an additional tool for staff to access Archibus in the field. It was never stated that this module would be the sole means of creating work orders. Users in the field have access to computers and can process work orders without the use of the mobile app.

- The auditors referenced the National Institute of Standards and Technology (NIST) SP-800-53 when citing DCAS for data input verification issues; however, this is a federal standard (recommended practice) that City agencies are not mandated to follow. DCAS chose not to implement this standard, as it was not conducive to business operations.

- The auditors told DCAS staff that they had conducted a search for Archibus users and their employment statuses in the City's Payroll Management System. In the report, the auditors stated that they found that one Archibus user, whose account was used on October 5, 2018, had been on childcare leave since July 2015, more than three years earlier. However, DCAS staff confirmed, through the user's agency, that the staff person had not been on child care leave. Rather, another employee with the same last name (who did not have access to Archibus) was actually on leave.

- Some of the items listed as findings appear to be based on the auditors' opinions rather than on solid criteria (requirements). Specifically, although requested by DCAS, the auditors were not able to provide DCAS with any relative criteria for the observations they included as findings in the following sections:
  - System Development and Implementation Issues
  - System Development Issues
  - System Implementation Issues
  - Data Field Issues
  - User Satisfaction Survey

The audit resulted in fourteen recommendations. Responses to each of the recommendations are provided below.

**Recommendation 1:** Ensure that the remaining Archibus modules are completed and meet the new projected timeline by November 2019.

**Agency Response: Disagree**
All of the Archibus modules are complete and available for use. DCAS will continue to utilize the modules in accordance with its business needs.

**Recommendation 2:** Ensure that all future system developments and enhancements are properly planned to include all business and system requirements.

**Agency Response: Disagree**
DCAS makes every effort to ensure that all system developments and enhancements are appropriately planned. The development of the Archibus system was based upon the business needs of the Agency at the time; however, as discussed with the auditors, the business needs changed due to reorganization in the Agency.

**Recommendation 3:** Develop a date verification rule to ensure that only valid dates can be entered into the system's date fields.

**Agency Response: Disagree**
The auditors did not test the validity of information entered into the system. Rather, the auditors tested the system's ability to accept backdated information. The system allows back dating to support current business practices and processes. The date fields are calendar fields where users are required to select or type month, day and year for system to save the dates. Additionally, the data goes through multiple levels of approval and validation.

**Recommendation 4:** Reassess and develop criteria to prevent users from erroneously inputting data into the unused fields.

**Agency Response: Disagree**
The auditors did not find that users were erroneously inputting data into unused data fields. The auditors found that there were unused data fields in the applications. Archibus is a COTS product that provides numerous out of the box fields to provide users with the flexibility to use these fields as part of business operations, as necessary, without costly customizations. Keeping this out of the box functionality allows organizations to quickly adapt to changing business needs using the available technology and resources. The out of the box fields that are not being used in Archibus are not critical to DCAS' current business needs but may be useful in the future. Additionally, removing or updating unused fields throughout the application would require unnecessary and costly customizations.

**Recommendation 5:** Comply with DoITT's Password Policy to ensure that each user's initial password is changed immediately upon the first login and that the password is required to change every 90 days.

**Agency Response: Partially Agree**
All users will now be able to self-manage their passwords. For internal users, passwords have always been managed through LDAP user account management procedures. This has forced users to change their passwords every 90 days. External users must now self-manage their passwords through NYC ID or LDAP. According to DoITT's external ID management and password policy, these passwords need not expire.

**Recommendation 6:** Enforce the policy that requires inactive user account recertification to be performed every 90 days.

**Agency Response: Agree.**
DCAS will review account activity every 90 days and deprovision users that did not log into the system during that period.

**Recommendation 7:** Ensure that all inactive user accounts are immediately disabled.

**Agency Response: Agree.**
For internal users, deprovisioning has occurred primarily through LDAP user account management procedures. As part of these procedures, when users leave the City or have not logged into the network in the last 90 days, the users were deprovisioned from any systems on the network, including Archibus. Because the external users are tenants that may periodically request maintenance work, DCAS would only disable external users upon receipt of a request. DCAS will now deprovision all users (whether internal or external) that have been inactive for 90 days. DCAS will also continue to disable user accounts upon request.

**Recommendation 8:** Ensure that accounts are created only for authorized users and that all account creations are properly documented.

**Agency Response: Agree**
DCAS has implemented a formal policy for user access requests which includes each user's completion of a signed access request form.

**Recommendation 9:** Promptly communicate with each City agency and external entity to update their tenant liaison information.

**Agency Responses: Agree**
DCAS has contacted the City agencies and other external entities that use Archibus to request updates to their liaison information.

**Recommendation 10:** Develop a procedure to ensure that the City agencies' and external entities' designations for their authorized liaisons are promptly updated when changes occur.

**Agency Responses: Agree**
Previously, DCAS relied on City agencies and other external entities to provide updates to liaison information when staffing changes occurred. DCAS will now periodically contact City agencies and other external entities and request that they confirm or update this information.

**Recommendation 11:** DCAS should periodically perform vulnerability scans and promptly remediate the risks identified in accordance with DoITT's Application Security Policy.

**Agency Response: Agree**
DCAS has had several safeguards in place to protect the Agency from security breaches. The application's servers are hosted at DoITT's Data Center, which are monitored and protected by DoITT. Additionally, DCAS utilizes several host-based and network-based intrusion detection and intrusion prevention systems to protect against attacks. DCAS has now additionally appointed a windows security administrator to periodically scan this application. Any risks identified in the scans will be addressed promptly.

**Recommendation 12:** DCAS should develop a formal Disaster Recovery Plan for Archibus to ensure the operational ability in the event of a disaster, emergency, or system failure.

**Agency Response: Agree**
DCAS has been working with DoITT to secure a formal Disaster Recovery Plan for Archibus and will continue to do so until a plan is in place.

**Recommendation 13:** Ensure that the user concerns identified in the report (survey) are addressed.

**Agency Response: Disagree**
It is not clear that the survey provides useful feedback. For example, one of the questions in the survey asks whether the system has all the functions for the users to complete their job duties. However, it is unclear if the responsibilities of the responders relate to functions that exist in Archibus.

**Recommendation 14:** Periodically conduct a survey to receive feedback from the users.

**Agency Response: Agree**
DCAS will work on a survey to receive user feedback periodically.

DCAS is committed to ensuring the protection and control of its data and its information processing resources. We will use the information provided by this audit to further strengthen DCAS' internal control environment.

Respectfully,

Lisette Camilo