CITY OF NEW YORK
OFFICE OF THE COMPTROLLER

John C. Liu
COMPTROLLER

BUREAU OF FINANCIAL AUDIT

H. Tina Kim
Deputy Comptroller for Audit

Audit Report on the Security Accreditation Process at the Department of Information Technology and Telecommunications

7A10-112

October 13, 2010

http://comptroller.nyc.gov

THE CITY OF NEW YORK
OFFICE OF THE COMPTROLLER
1 CENTRE STREET
NEW YORK, N.Y. 10007-2341

John C. Liu
COMPTROLLER

October 13, 2010

To the Residents of the City of New York

My office has audited the Department of Information Technology and Telecommunications (DoITT) to determine whether the agency standards and framework provide reasonable assurance that City resources are adequately safeguarded and DoITT is adequately coordinating all City agencies to assess compliance with all its IT security policies in the in the Security Accreditation Process (SAP). We audit entities such as DoITT as a means of ensuring systems and technological resources of City agencies are cost-effective, efficient, secure, and operate in the best interest of the public.

DoITT has a policy in place for its SAP. DoITT coordinates with agencies during the SAP to ensure that all City agencies are in compliance with IT security policies. DoITT's standards and framework provide reasonable assurance that City resources are adequately safeguarded. However, DoITT lacks the necessary enforcement powers to prevent an agency from deploying a new application without submitting it to the SAP. DoITT follows the SAP to ensure that City applications are adequately safeguarded. However, we found process weaknesses for two sampled applications accredited with exceptions. In these instances, DoITT did not have all the necessary documentation required for the SAP. DoITT informed us that they accredited these two applications through its in-house certifications; but DoITT has not provided us with the formal procedure for the in-house certifications process. Additionally, DoITT indicated that when an application is accredited with exceptions, they do not have the resources to ensure the exceptions are followed up and corrected. Finally, DoITT can only decline accreditation, but it lacks the authority to enforce City agencies from deploying unaccredited applications into production.

This audit contains eight recommendations that if implemented should increase controls throughout the Security Accreditation Process.

The results of the audit have been discussed with DoITT 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,

John C. Liu

Table of Contents

AUDIT REPORT IN BRIEF 1

Audit Findings and Conclusions 1
Audit Recommendations 2

INTRODUCTION 3

Background 3
Objectives 5
Scope and Methodology 5
Discussion of Audit Results 6

FINDINGS AND RECOMMENDATIONS 7

DoITT Lacks Necessary Enforcement Powers to Provide Effective Security Accreditation 7
Review of Applications for Accreditation by DoITT 8
Agencies Deployment of Unaccredited Applications 9

APPENDIX I Security Accreditation Documentation
APPENDIX II Sample of Applications Submitted for Accreditation

ADDENDUM Department of Information Technology and Telecommunications

The City of New York
Office of the Comptroller
Bureau of Financial Audit
IT Audit Division

Audit Report on the Security Accreditation Process at the Department of Information Technology and Telecommunications

7A10-112

AUDIT REPORT IN BRIEF

The Department of Information Technology and Telecommunications (DoITT) is the City's Information Technology (IT) utility, ensuring the sustained, efficient delivery of IT infrastructure, telecommunications and IT services. It transforms the way the City interacts with its residents, businesses, visitors, and employees by leveraging technology to improve services and increase transparency, accountability, and accessibility across all agencies. DoITT supports the technical and administrative functions of the City's 311 Customer Service Center, which provides the public with information and services for more than 300 agencies and organizations; it maintains the City's official Web-site, NYC.gov, and it manages the City's television and radio stations. DoITT is home to the Citywide Geographic Information Systems Unit, which develops and hosts a digital base map used to support City operations. In June 2004, Mayor Bloomberg focused his administration's efforts on using business strategies and relevant technology to make government more accessible, responsive, and accountable to its citizens. DoITT was directed to work closely with City agencies to manage and assist in this initiative. [1]

DoITT issued its Security Accreditation Process (SAP) in July 2007, which indicates that all City-wide applications must be built in a secure fashion and is a key control in ensuring the integrity of the City's data processing systems and the security, reliability, and validity of the data contained therein. SAP outlines key steps to be followed and critical tests to be performed during the development of new City-wide systems or major changes made to any existing City-wide systems. If followed, SAP will help to ensure that the data contained in the systems is secure and protected and that the systems are working in a secure environment.

Audit Findings and Conclusions

DoITT has a policy in place for its SAP. DoITT coordinates with agencies during the SAP to ensure that all city agencies are in compliance with IT security policies. DoITT's

[1] Sister City White Paper Technology Initiatives in New York City, June 2004

standards and framework provide reasonable assurance that City resources are adequately safeguarded. However, DoITT lacks the necessary enforcement powers to prevent an agency from deploying a new application without submitting it to the SAP.

DoITT follows the SAP to ensure that City applications are adequately safeguarded. However, we found process weaknesses for two sampled applications accredited with exceptions. In these instances, DoITT did not have all the necessary documentation required for the SAP. DoITT informed us that they accredited these two applications through its in-house certifications; but DoITT has not provided us with the formal procedure for the in-house certifications process. Additionally, DoITT indicated that when an application is accredited with exceptions, they do not have the resources to ensure the exceptions are followed up and corrected. Finally, DoITT can only decline accreditation, but it lacks the authority to enforce City agencies from deploying unaccredited applications into production.

Audit Recommendations

To address these issues, we make eight recommendations that DoITT should:

- Perform a Citywide risk assessment of applications that have not participated in the Security Accreditation Process.
- Contact those agencies whose systems pose the most critical risk and request that they submit applications for the Security Accreditation Process.
- Request assistance from the Mayor's Office of Operations in directing agencies to participate in the Security Accreditation Process.
- Ensure that all documentation relating to the security accreditation requests for all applications be submitted and maintained.
- Develop a formal Security Accreditation Process for in-house certifications.
- Ensure that security issues found in applications with exceptions are followed up and corrected by the agencies.
- With the assistance of the Mayor's Office of Operations, require that agencies participating in the SAP follow all Citywide security standards and security policies to ensure that applications are operating in a secure environment.
- Enhance its Security Accreditation Process procedures to ensure all agencies deploy an application only after it has been accredited by DoITT.

INTRODUCTION

Background

DoITT is the City's Information Technology utility, ensuring the sustained, efficient delivery of IT infrastructure, telecommunications and IT services. It transforms the way the City interacts with its residents, businesses, visitors, and employees by leveraging technology to improve services and increase transparency, accountability, and accessibility across all agencies. DoITT supports the technical and administrative functions of the City's 311 Customer Service Center, which provides the public with information and services for more than 300 agencies and organizations; it maintains the City's official Web-site, NYC.gov, and it manages the City's television and radio stations. DoITT is home to the Citywide Geographic Information Systems Unit, which develops and hosts a digital base map used to support City operations and several other services.

In June 2004, Mayor Bloomberg focused his administration's efforts on using business strategies and relevant technology to make government more accessible, responsive, and accountable to its citizens. DoITT was directed to work closely with City agencies to manage and assist in this initiative. Three initiatives were established: (1) using the strategic technology infrastructure and investments to ensure a high availability and resiliency of City resources; (2) securing and efficient use of these resources; and (3) monitoring how large and complex IT projects were managed to ensure their delivery was on-time and within budget thus lessening the risk associated with maintaining those projects.

In an August 8, 2006 Memo of Understanding between DoITT and Department of Investigations (DOI), DoITT became responsible for the formulation and distribution of all information security standards City-wide. All City agencies and employees and all contractors and vendors doing business with the City are required to follow these policies and standards.

DoITT issued its SAP in July 2007, which indicates that all City-wide applications must be built in a secure fashion and is a key control in ensuring the integrity of the City's data processing systems and the security, reliability, and validity of the data contained therein. SAP outlines key steps to be followed and critical tests to be performed during the development of new City-wide systems or major changes made to any existing City-wide systems. If followed, SAP will help to ensure that the data contained in the systems is secure and protected and that the systems are working in a secure environment.

DoITT informed City agencies of the SAP by posting it on the DoITT website along with a template to be used in the process. In September 2007, DoITT announced the SAP at a multi-agency meeting. DoITT also sends out a monthly Security Awareness Newsletter to keep agencies informed of relevant policies and directives for new application development.

SAP requires City agencies to submit to DoITT a template for approval of new applications. During this process there is communication between DoITT and the agency through email and by telephone. The Security Accreditation Documentation (See Appendix I) is

a template consisting of six sections that provide a description of the service or product being developed. In the template, the City agency follows the Data Classification policy by analyzing and classifying its business requirements and its data fields for the protection of business information assets. On the DoITT website, agencies are given a Security Accreditation Standard that DoITT requires them to follow for all external and internal application approval before being deployed into production.

DoITT accreditation requires that agencies follow the phases of the Software Development Life Cycle (SDLC) when developing new applications. The phases include analysis, define, design, development, test, and implementation before an application is deployed. During the define phase, the DoITT IT Security Engineering (ITSecEng) looks at functional requirements and it assists in defining technical requirements for security. During the design phase, ITSecEng can provide guidance in meeting detailed design requirements for security controls. In the development and test phases, ITSecEng assists developers with design issues. Prior to implementing a new system, DoITT reviews the documentation submitted by the agency to ensure compliance with security policies and ITSecEng then makes a final security assessment of the system.

During the SAP, DoITT reviews the documentation submitted by an agency to ensure compliance with security policies. DoITT officials informed us that they review the required Security Accreditation Documentation and communicate with the agency regarding any issues found. Furthermore, DoITT performs scans using both Appscan[2] and Qualys[3] to identify any security issues or concerns with the new applications. When a security issue is found, DoITT requests the agency to correct it. When DoITT deems an application secure, it sends the agency an e-mail indicating that the application has been accredited. After DoITT accredits the application, the agency can move it to the production environment.

If an application after review is found to have any issues, the agency can request that the application be approved with an exception for accreditation. In these instances, DoITT's Commissioner has the responsibility of reviewing the request and can provide accreditation to an application with an exception. If the Commissioner approves the request, the agency has its application accredited with an exception. If DoITT does not approve the exception, it is the agency's responsibility to fix the exception or DoITT will not accredit the application.

All applications must be reviewed and approved for accreditation by DoITT's Citywide Chief Information Security Officer. Accreditation must be achieved prior to the application's migration to the production environment.

---

[2] AppScan software from IBM is a Web based security product that identifies potential weakness in security that could pose a threat of attacks and data breaches against the application.

[3] Qualys provides on-demand IT security risk and compliance management software products and services through its QualysGuard software.

Objectives

The objectives of this audit were to determine whether:

1. DoITT's standards and framework provide reasonable assurance that City resources are adequately safeguarded, and

2. DoITT is adequately coordinating all City agencies to assess compliance with all its IT security policies.

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.

Our fieldwork was performed from January 2010 to April 2010. To achieve our audit objectives we:

- Reviewed DoITT's organizational charts;

- Interviewed DoITT officials involved in the SAP;

- Conducted a walkthrough to gain an understanding of SAP;

- Reviewed the Security Accreditation Documentation, which were submitted to DoITT by City agencies for accreditation approval;

- Reviewed and analyzed DoITT's Security Architecture Standard, which defines various security models and controls that should be functioning in applications deployed by City agencies;

- Received a list of 42 applications submitted to DoITT for accreditation. Of the 42 applications, three applications were unable to be accredited, five were accredited with exceptions and 34 received accreditation. We selected and analyzed a sample of 12 out of 42 applications (four applications that received accreditation, five applications accredited with exception, and three applications not accredited);

- Reviewed and examined the procedures for the scanning of applications to assess application vulnerabilities, which may include the data breach, malware attacks, and

notifying the user of items that do not compliance with security, privacy, or accessibility requirements;

- Reviewed e-mail approvals of accreditation and the e-mail histories between the DoITT and the respective agencies to determine whether DoITT is following the SAP for each application.

As criteria, we used the DoITT *Citywide Information Security Directives and Policies* and the National Institute of Standards and Technology *Generally Accepted Principles and Practices for Securing Information Technology System*.

Discussion of Audit Results

The matters covered in this report were discussed with DoITT officials during and at the conclusion of this audit. A preliminary draft report was sent to DoITT officials and was discussed during an exit conference held on August 9, 2010. On August 18, 2010, we submitted a draft report to DoITT officials with a request for comments. We received a written response from DoITT on September 2, 2010. In its response, DoITT officials generally agreed with the findings and recommendations of this audit.

The full text of the DoITT response is included as an addendum to this final report.

FINDINGS AND RECOMMENDATIONS

DoITT has a policy in place for its SAP. DoITT coordinates with agencies during the SAP to ensure that all city agencies are in compliance with IT security policies. DoITT's standards and framework provide reasonable assurance that City resources are adequately safeguarded. However, DoITT lacks the necessary enforcement powers to prevent an agency from deploying a new application without submitting it to the SAP.

DoITT follows the SAP to ensure that City applications are adequately safeguarded. However, we found process weaknesses for two sampled applications accredited with exceptions. In these instances, DoITT did not have all the necessary documentation required for the SAP. DoITT informed us that they accredited these two applications through its in-house certifications; but DoITT has not provided us with the formal procedure for the in-house certifications process. Additionally, DoITT indicated that when an application is accredited with exceptions, they do not have the resources to ensure the exceptions are followed up and corrected. Finally, DoITT can only decline accreditation, but it lacks the authority to enforce City agencies from deploying unaccredited applications into production.

DoITT Lacks Necessary Enforcement Powers to Provide Effective Security Accreditation

DoITT does not have the power to enforce participation by City agencies in the SAP. It also does not have a process to identify applications that have not been assessed through the SAP. As a consequence, these issues create major weaknesses in a key control over Citywide information security.

DoITT Does Not Have the Enforcement Power to Require Agencies To Submit Systems for Security Accreditation Review

DoITT asserts that it only proceeds with the SAP for an application submitted to DoITT for review. However, DoITT lacks the authority to enforce or to require agencies to submit an application for review and accreditation approval through the SAP. In fact, agency-heads are permitted to approve the deployment of an application without submitting it to DoITT for review and approval. DoITT also emphasizes that it cannot require that an agency go through the SAP for existing legacy applications. The SAP is designed for applications that are in development or undergoing a major system upgrade.

No Procedure to Identify Systems That Lack Security Accreditation

DoITT officials indicated that while they encourage all City agencies to submit their applications for review to ensure that security controls are in place; DoITT has no procedure for identifying and detecting applications, either new or that are operational, so it can properly examine them through its SAP. As a consequence, this weakness can leave these systems operating in an unsecure environment, contrary to the goal stated in DoITT's policy statement,

dated July 2007: "All externally accessible and internally accessible Citywide applications developed to support City of New York business must be built in a secure fashion."

DoITT's lack of ability to enforce its SAP is a major weakness in a key control over Citywide information security. The lack of enforcement of the SAP and of security policies leaves certain systems vulnerable to the risks of data breach and noncompliance with security, privacy, or accessibility standards.

Recommendations

DoITT should:

1. Perform a Citywide risk assessment of applications that have not participated in the Security Accreditation Process.

DoITT Response: "The Audit Report recommends that DoITT perform a Citywide risk assessment of applications that have not participated in the Security Accreditation Process. DoITT is reviewing those applications that are deemed at risk . . . The goal is to identify and migrate those hosts and applications to DoITT's centralized internet hosting environment and at the same time, perform accreditation reviews and identify risks."

2. Contact those agencies whose systems pose the most critical risk and request that they submit applications for the Security Accreditation Process.

DoITT Response: "DoITT has already directed the agencies with risk to perform a DMZ Services Assessment to gather the required information."

3. Request assistance from the Mayor's Office of Operations in directing agencies to participate in the Security Accreditation Process.

DoITT Response: "DoITT will invite the Mayor's Office of Operations to participate in cases where agencies are not voluntarily compliant with this process. DoITT is also seeking support with other oversight agencies."

Review of Applications for Accreditation by DoITT

DoITT follows the procedures in the SAP for the accreditation of applications. We sampled 12 applications for review, which included the following: four applications accredited, five applications accredited with exceptions and three applications not accredited by DoITT.

DoITT provided all documentation for the four sampled applications accredited by DoITT. We found process weaknesses for two sampled applications accredited with exceptions. In these instances, DoITT did not have all the necessary documentation required for the SAP. Specifically, the agency did not submit a template to DoITT and there was no sign-off approval sent to the agency for these two applications. DoITT informed us that they accredited these two applications through its in-house certifications; however, DoITT does not have a formal

procedure for in-house certifications process, which creates the potential for DoITT to overlook security issues. Also, DoITT indicated that when an application is accredited with exceptions, they do not have the resources to ensure the exceptions are followed up and corrected. This creates the potential for security issues to be unresolved by city agencies.

Recommendations

DoITT should:

4. Ensure that all documentation relating to the security accreditation requests for all applications be submitted and maintained.

DoITT Response: "DoITT agrees, and is keeping full documentation for each application reviewed. This includes the accreditation template, any additional system documentation reviewed, and the email records of all conversations around the process. We are implementing an annotation tool, in conjunction with Sharepoint, which we will maintain and file the history of each project."

5. Develop a formal Security Accreditation Process for in-house certifications.

DoITT Response: "DoITT acknowledges that in the early days of the process that certain critical steps were missed, but has been remedied by following the documentation collection detailed in Section 4."

6. Ensure that security issues found in applications with exceptions are followed up and corrected by the agencies.

DoITT Response: "You have also requested that DoITT ensure that security issues found in applications with exceptions are followed up and corrected by the agencies. Typically, exceptions will be granted for medium and low risk issues where there is specific acknowledgement of intent to remediate by a specific date. DoITT will continue to follow up in cases where exceptions have been granted until such time as the exceptions can be cleared."

Agencies Deployment of Unaccredited Applications

DoITT was unable to accredit: the Electronic Death Registration System (EDRS), the Achievement Reporting and Innovation System (ARIS), and the Customer Resource Management System of the New York Department of Cultural Affairs (DCLA) because they did not comply with DoITT standards and security policies. For two sampled applications that were not accredited by DoITT, EDRS and ARIS, the agencies did not provide all necessary documentation. Despite these issues, these applications were all deployed without meeting the SAP.

The Department of Health and Mental Hygiene (DoHMH) requested accreditation for the EDRS but did not submit the necessary template to DoITT. DoITT did not perform any security scans on the application to allow for accreditation. The EDRS application submitted by DoHMH did not meet the Citywide security architecture standard. This standard defines various security models and controls that should be included in applications deployed by City agencies.

The security scans of the DOE's ARIS were performed by a third party, but DoITT stated that it had no documentation of those scans. In that regard, DOE did not follow the Citywide security architecture standard and violated the Citywide security policy during its development of ARIS.

In the case of DCLA's Customer Resource Management System, DoITT stated that DCLA did not receive accreditation of the system because DCLA sent clear-text passwords via e-mail to system users who forgot their existing passwords. DoITT policy indicates that clear-text passwords are not to be sent through an e-mail since doing so represents weak controls over account management. DoITT declined to accredit the application and recommended that the agency not deploy it. However, DCLA disregarded DoITT's recommendation and deployed the application, assuming the inherent security risk. We found that DoITT needs to enhance its SAP procedures to ensure all agencies deploy an application only after it has been accredited by DoITT.

Recommendations

DoITT should:

7. With the assistance of the Mayor's Office of Operations, require that agencies participating in the SAP follow all Citywide security standards and security policies to ensure that applications are operating in a secure environment.

DoITT Response: "DoITT will work with the Mayor's Office of Operations along with other oversight agencies in order to secure the operating environment."

8. Enhance its Security Accreditation Process procedures to ensure all agencies deploy an application only after it has been accredited by DoITT.

DoITT Response: "For those applications which require accreditation, DoITT will facilitate deploying only those applications which are accredited at go-live or appear likely to be accreditable within a short time thereafter."

THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY &TELECOMMUNICATIONS

Security Accreditation Documentation

(Replace Document Title with Project Name Here)

Authors: Names of authors of this document
Contributors: Names of contributors to this document

Date: October 12, 2010
Version: 1.5

Contents

1 Introduction 3
1.1 Project Ownership 3
1.2 References 4
1.3 Change History 4
1.4 Glossary 4
2 Architectural Analysis 5
2.1 Business View 5
2.2 Functional Use View 5
2.3 Data View 5
2.3.1 Privacy 6
2.4 High Level Architectural View 7
3 Architectural Topology 8
3.1 Product Summary 8
3.2 Logical Architecture View 8
3.3 Application Dependencies 9
3.4 Database View 9
4 Security Controls 10
4.1 Authentication 10
4.2 Authorization 10
4.3 Audit 10
5 Physical Architecture 12
5.1 Infrastructure 12
5.2 Protocols 13
5.2.1 Non Standard Protocols 13
5.3 Servers 13
6 Risks 14

1 Introduction

This section needs to provide a brief description of the service or product being developed. What business purpose will it serve? Include any high level points that are relevant. If product/service is deployed in multiple phases, keep the document relevant to the current phase, however also include relevant information for other phases.

Indicate the following:

- Is the application home grown, commercial of the shelf (COTS), or customized COTS?
- Is this an Internet facing application?

PLEASE NOTE:
At one time, some agencies were permitted to terminate dedicated T1 connections to a router in the 2 Tier DMZ. This was for the purpose of supporting a local DMZ and for Internet access. This architecture was designed before DoITT had the capability to host internet facing applications for City agencies. While existing connections are grandfathered, new connections will not be approved, nor will significant expansion of existing agency DMZs be approved. In order to strengthen perimeter security, all internet facing applications which require public access will be hosted in a DoITT managed datacenter. All agencies currently hosting such applications should begin a migration project immediately in order to adopt the new, more secure architecture. (From section 12 of the Citynet Architecture Standard)

- What type of data does it collect?
- What is the anticipated user community (Including admin and internal staff)?
- How will users access the application (Web, Thick client or other)?
- Will any portion of the project require the use of outside 3rd party? If so, which parts and has the 3rd party been selected?

- Does the requesting agency have citynet access?

- Does the agency have its own DMZ?
- What are the anticipated project costs?

1.1 Project Ownership

List all respective entities below. Include an appendix A with contact details for names below.

Project Stakeholders:

Include names of business and technical project stakeholders.

Steering Committee:

Include names of people on the project steering committee if such exists.

Project Business Owner

Project Technology Owner

Hosting Owner – if applicable

Data Owner

Data Steward

Project Manager

1.2 References

Include any references to other documentation that may be relevant.

	Document	Version	Date	Author
1				
2				

1.3 Change History

State major changes from previous versions of this document

Version	Date	Author	Key Changes
0.1			
0.2			

1.4 Glossary

Provide a glossary of terms that may not be otherwise known but are referred in the document.

Term	Definition
Platform	Collection of systems and components
RAID	Redundant Array of Independent Disks
PII	Personal Identifiable Information
PHI	Personal Health Information
COTS	Commercial Off-The-Shelf

2 Architectural Analysis

2.1 Business View

Describe the business purpose for this product/service. What is the particular business problem that is being solved? How will this product enable the resolution of the business problem or enhance user experience?

2.2 Functional Use View

Describe the intended users of this service/product. List all types of users that will be using the application and their respective user scenarios. What will be the responsibility of each role? Document what each user role will be capable of doing in the application. Define the level of access each user role requires. Include the consumers, back end processing roles, reporting and 3rd party access if required.

2.3 Data View

What types of data are collected, stored, and/or processed by the application?
What is the data classification level of the data sets? (If more than one data set exists then describe all of the data sets) according to the Citywide Information Security Data Classification Policy?

- What are the origins of the data? How is it collected?
- What are the access methods (services) to access/modify/delete data?
- Is data accessed from any other data store(s)?
- Who has rights to access the data?

Will the data that is collected, stored or processed by the application be shared with (accessed by, or provided in any form) to a 3rd party entity such as another City agency, members of the public, or entities other than the data owner or data steward?

Provide a clear explanation on the ownership of the data. Who ultimately owns the data? Which entity is responsible for the appropriate use of the data? Describe any data stewards? Document any transmission and/or aggregation points. Who has ownership of these transmission and aggregation points?

According to City of New York Security policies all data that is classified as private or higher needs to be encrypted in transit and at rest. PII and PHI is automatically classified as private. Not all fields need to be encrypted, but only fields that make the data PII such as a social security number.

All passwords are classified as private and have to be protected when passed across the network in such a way that if intercepted, they cannot be used to authenticate. For example some technological solutions are encryption, or hashing in conjunction with appropriate challenge response protocol.

2.3.1 Privacy

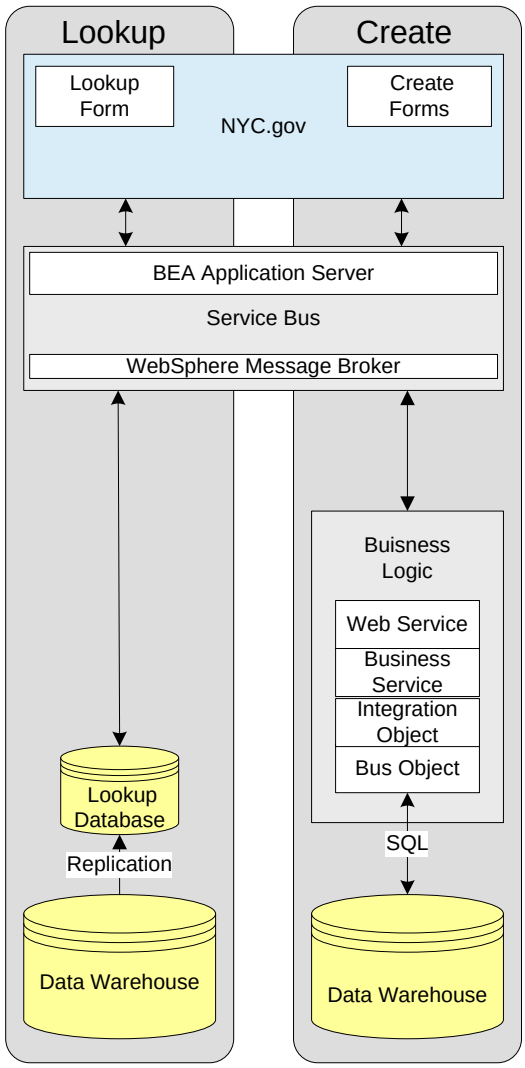
Describe the privacy implications of the data being used.

- Are there policies/laws/regulations that govern the use and storage of the data?
- Is the data critical to the subsistence and successful operation of any government agency? For example, does it include the names of police officers, agents etc.
- Does the data include financial information?
- Does the data include PII or PHI?

2.4 High Level Architectural View

Provide a high level view of the components of the product/service and its supporting infrastructure. (Below is a sample diagram for reference)

Include a global view any services or applications new or existing that this service/product will depend on. Include 3d party or external data sources, administration access etc.



3 Architectural Topology

In this section describe in detail the overall logical architecture of the product/service. Describe all high level components of the system. Describe any architectural dependencies. State any architectural assumptions.

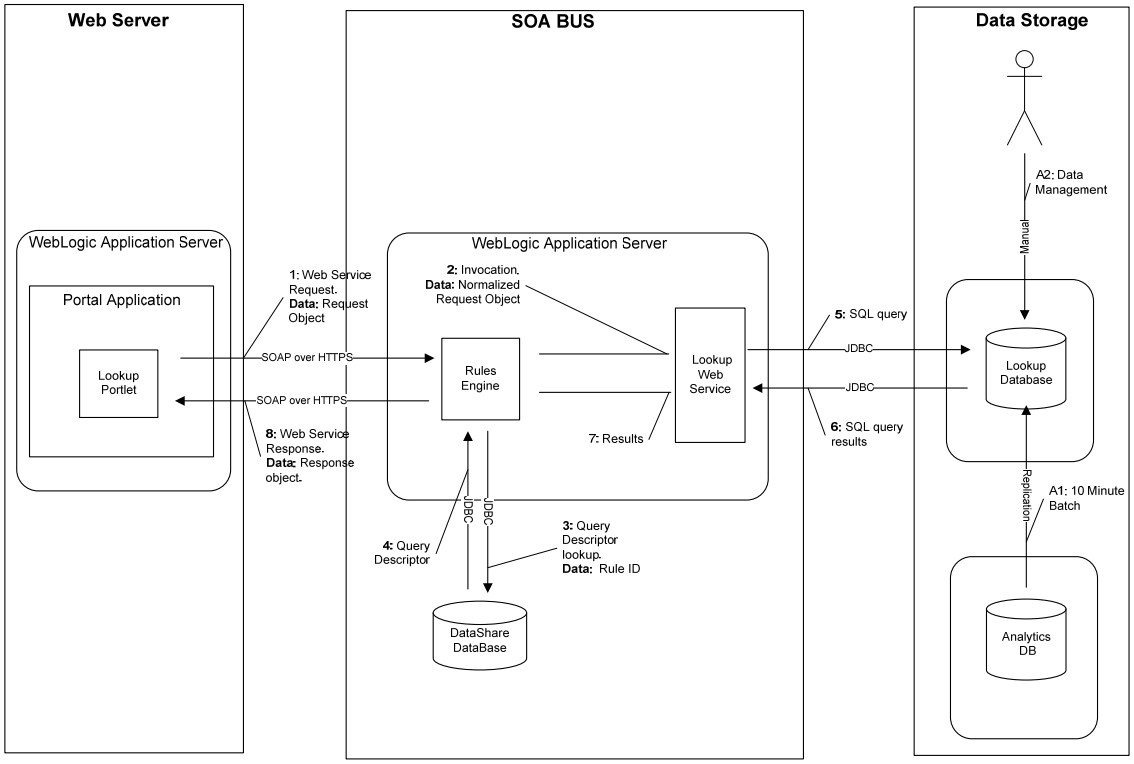
3.1 Product Summary

Where it will be deployed, how many environments will be required and what other underlying software infrastructure (such as MS SQL, Oracle, Apache, Web Logic) will be used. What operating system(s) will be required? What development language(s) (if applicable) will be utilized?

3.2 Logical Architecture View

Provide logical architecture diagrams. Describe in detail logical components. Outline the operation of the system in a Disaster Recovery/Business Continuity Planning situation if such is provided for. Below is a sample Logical Diagram.

Lookup Application Architecture



3.3 Flow diagram

Provide a diagram that identifies all the data flows between the components of the application. Include internal as well as external data flows.

3.4 Application Dependencies

Describe any other existing or future applications/services that this service/product will depend on. Describe how the interconnection will be established, how data will be accessed. Provide a flow diagram similar to above depicting use of other applications.

3.5 Database View

Provide a database schema or the number of tables. Define what type of information will be stored in the tables. Describe the database controls that will be in place to protect the data. For example: "Only store procs will be used to insert data, data will be validated for valid characters only, the account used will only have insert permissions on tables a,b,c."

Include in the schema the relationship of tables to permissions of database users. (The schema needs to clearly describe proper database permissions for each database user.)

4 Security Controls

Describe security controls that will be used to protect access to the data and the integrity of the system. Describe each control and how it fits in each of the logical components. Describe which controls exist to prevent privilege escalation and ensure that each user modality is only capable to perform tasks as required by the business process described above.

Describe the process of keeping these controls current and up to date with relevant policies, include management of controls. Outline who will be responsible for ensuring these controls are operating correctly and updating policies.

4.1 Authentication

Describe how all components within the system will be authenticated. Where are the user accounts stored? How are authentication credentials stored? (This should include not only physical user authentication but component to component authentication as well. For example, how does the application authenticate to the database? How are web services authenticated to each other?

Where and how is the authentication credentials stored? Are these credentials stored in an encrypted form?

Is there a self registration option for the system? If so how the authenticity of a user be identified (i.e. how do we know that Joe Smith is really Joe Smith). Is there ability for the end-user to reset his account credentials? If so how is this accomplished?

4.2 Authorization

Describe what process controls authorization of users. Where in the system is authorization information stored? How is it enforced? What are the controls in place to prevent privilege elevation (i.e. what prevents a user from gaining more access then he/she has)?

How is initial user provisioning done?

4.3 Audit

Describe how the system audits events. Who performed which actions and when?

4.4 Data Transit

If the data classification is sensitive or higher, describe how the data is protected during its transmission to insure its confidentiality and integrity.

4.5 Data at Rest

If the data classification is sensitive or higher, describe how the data is protected at rest. Stored in a database, a file or in cache.

4.5.1 Cached data

Describe if data is cached any where, including the browsers cache and what steps are taken ensure data classified is sensitive or higher is not stored in the cache or the cache is properly cleared.

4.6 Access Control

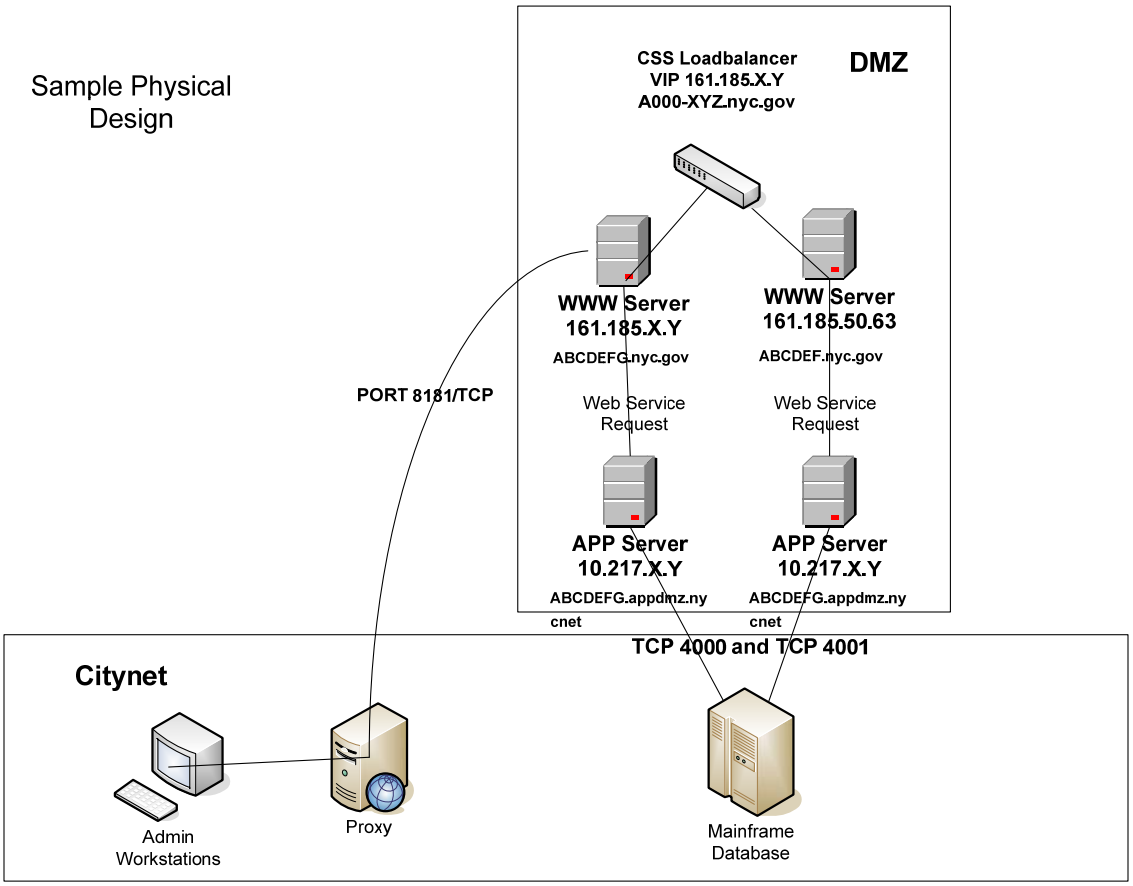
Describe what controls are in place to prevent unauthorized access to different system components. For example, what prevents someone from accessing a web service? Accessing a database?

5 Physical Architecture

5.1 Infrastructure

Describe the physical infrastructure of the system/product and how it will fit into the existing environment. Describe all environments that relate to this service/product including development, staging, pre-production QA etc. Describe where each environment will be located and who will be hosting it. Provide a physical diagram of production and pre-production (staging) environments at minimum. Describe where each server will be connected and how it will communicate with the rest of the environment. Describe any external connectivity requirements, including internet, intranet, extranet. Include any disaster recovery and business continuity environments.

Below is a sample physical diagram.



5.2 Logical and Physical overlay

Provide a diagram which clearly identifies all the logical components and their respective physical location.

5.3 Protocols

Describe all the communications protocols used by the product/service. Outline which components communicate with other components in the product/service. Identify which protocols are being used and include how these protocols are secured.

5.3.1 Non Standard Protocols

Describe any non standard communication protocols that will be used if any.

5.4 Servers

Describe servers used in each environment

Server:
Network location-
Where is it placed in the infrastructure?
Hardware /VM -
What hardware is required?
Storage –
- How much storage is required?
Operating system-
- What is the operating system?
Security –

What security products/configurations are in place to ensure the server is not compromised?

6 Risks

Summarize and quantify any known or anticipated risks to the confidentiality and integrity of the data. Identify any product or service that is used for this purpose.

Appendix A – Project Team Contact List

Name	Company Affiliation	Title	Phone Number	Email Address

Appendix II

Sample of Applications
Submitted for Accreditation

Agency Application	TEMPLATE	SCANS	SIGN-OFF	EMAIL HISTORY
Accredited Applications				
311 Online/Universal Intake	Y	Y	Y	Y
SCOUT on the Web (Street Conditions Observation Unit)	Y	Y	Y	Y
OEM COOP Living Disaster Recovery Planning System	Y	Y	Y	Y
DoHMH, Environmental Public Health Tracking Portal	Y	Y	Y	Y
Exceptions				
Financial Information Services Agency Employee Self- Service (ESS)	Y	Y	Y	Y
311 Online	Y	Y	Y	Y
Cityhall Graffiti Waiver	N	Y	N	Y
Cityhall WTC Registry	N	Y	N	Y
311 PICTURE/VIDEO (Citizens Pictures & Video Project)	Y	Y	Y	Y
Unable to be Accredited				
Department of Cultural Affairs Customer Resource Management System	Y	Y	Y	Y
DOE Achievement Reporting and Innovation System	Y	N	Y	Y
DoHMH Electronic Death Registration System	N	N	N	Y

Y - Documentation Received
N - Documentation Not Received

Information Technology & Telecommunications

Carole Post
Commissioner
75 Park Place
New York, NY 10007
212-788-6600

September 2, 2010

Honorable Tina Kim
Deputy Comptroller
Audits and Accountancy
1 Centre Street
New York, New York 10007-2341

Re: Draft Audit Report on the Security Accreditation Process at the Department of Information Technology and Telecommunications-7A10-112 dated August 18, 2010

Dear Ms. Kim:

Below please find the Department of Information Technology and Telecommunications' comments on the recommendations made in the above referenced report.

1) The Audit Report recommends that DoITT perform a Citywide risk assessment of applications that have not participated in the Security Accreditation Process. DoITT is reviewing those applications that are deemed at risk. These are agency hosted internet facing applications that are not compliant with the current Security Architecture Standard and therefore cannot be accredited. The goal is to identify and migrate those hosts and applications to DoITT's centralized internet hosting environment and at the same time, perform accreditation reviews and identify risks.

2) The Report also recommended contacting those agencies whose systems pose the most critical risk and request that they submit applications for the Security Accreditation Process. DoITT has already directed the agencies with risk to perform a DMZ Services Assessment to gather the required information.

3) Your office has also indicated that DoITT should request assistance from the Mayor's Office of Operations in directing agencies to participate in the Security Accreditation Process. DoITT will invite the Mayor's Office of Operations to participate in cases where agencies are not voluntarily compliant with this process. DoITT is also seeking support with other oversight agencies. We encourage agencies to take another look at Section J (Internet Connectivity) of Directive 1. This section emphasizes utilizing the DoITT Security Accreditation Process.

4) The Report further recommends that DoITT should ensure that all documentation relating to the security accreditation requests for all applications be submitted and maintained. DoITT agrees, and is keeping full documentation for each application reviewed. This includes the accreditation template, any additional system documentation reviewed, and the email records of all conversations around the process. We are implementing an annotation tool, in conjunction with Sharepoint, which we will maintain and file the history of each project.

5) Your office would like DoITT to develop a formal Security Accreditation Process for in-house certifications. DoITT acknowledges that in the early days of the process that certain critical steps were missed, but has been remedied by following the documentation collection detailed in Section 4.

6) You have also requested that DoITT ensure that security issues found in applications with exceptions are followed up and corrected by the agencies. Typically, exceptions will be granted for medium and low risk issues where there is specific acknowledgement of intent to remediate by a specific date. DoITT will continue to follow up in cases where exceptions have been granted until such time as the exceptions can be cleared.

7) The Report also recommends that with the assistance of the Mayor's Office of Operations, DoITT must require that agencies participating in the SAP follow all Security standards and security policies to ensure that applications are operating in a secure environment. DoITT will work with the Mayor's Office of Operations along with other oversight agencies in order to secure the operating environment.

8) Lastly, in your final recommendation you ask DoITT to enhance its Security Accreditation Process procedures to ensure all agencies deploy an application only after it has been accrecited by DoITT. For those applications which require accreditation, DoITT will facilitate deploying only those applications which are accredited at go-live or appear likely to be accreditable within a short time thereafter.

DoITT would like to thank the Comptroller's office for this audit and trying to ensure agency wide compliance with the security accreditation process.

Sincerely,

Carole Post

Carole Post

Cc: M.Bimonte, D. Srebnick, L. Mercurio, file