NYC Department of Information Technology & Telecommunications

Guidance for Audit Readiness

Risk Management & Compliance Division

Linda Mercurio, Director

Table of Contents

Introduction to Audit Readiness

Chapter 1 – Project Oversight and Audit Readiness

1) *Requirements for all projects*
2) *Additional areas to be reviewed*
3) *Access to and use of confidential information*
4) *Mobile computing and storage devices*
5) *Access controls*
6) *Personnel needed to support assessment*

Chapter 2 – Internal Controls

1) *Benefits of internal controls*
2) *Who is responsible for internal control?*
3) *Internal assessments*
4) *Benefits of internal assessments*
5) *What does the Risk Management and Compliance Division do?*
6) *Risk assessment*

Chapter 3 – Types of Government Audits

Sample Internal Assessment Projects
What Risk Management and Compliance means to you?

Introduction to Audit Readiness

Auditors look for documentation of every decision that is made over the course of a project, from project conception to project completion. Auditors want documentation of the big decisions, like whether to go forward with the project in the first place, which vendor to use, whether to pay a vendor's invoice, and whether to accept a vendor's deliverable. Auditors also want documentation of the smallest, day-to-day decisions, like the approval of a subcontractor, the approval of a consultant's time sheet, or the approval of extension of time for contract performance.

In examining this documentation, auditors are asking whether the project met its expectations. Did the deliverables comply with contract requirements? Did the cost fall within budgetary and contractual maximums? Perhaps most importantly, does the product work as claimed when the project was proposed?

The ideal state of audit readiness is to have complete documentation (digital, paper, or both) for every decision that is made in the course of a project. The documentation is organized and maintained in a way that makes it readily accessible to auditors when the time comes, and the documentation clearly and completely explains the reasons for each project decision. Finally, the documentation demonstrates contract compliance and budgetary compliance.

Of course, good audit readiness practices help us avoid embarrassing second-guessing by outside auditors. But more importantly, the discipline of audit readiness helps us to ensure that we think through the decisions we make on a project, from project development to project implementation to completion, acceptance, and final payment. If we can't document a decision in a way that is clear to an auditor, we probably shouldn't make that decision in the first place.

The purpose of this document is to provide guidance in audit readiness for project managers and support teams, and to inform them about the availability of Risk Management and Compliance Division as a resource.

Chapter 1 - Oversight of Project and Readiness for an audit

1) Requirements for all projects - All projects should have the following:

1. General Preparation

- Organizational Chart
- Project Charter
- Work Breakdown Structure
- Governance Plan
- Steering Committee Org Chart and schedule regular Steering Committee Meetings

2. Staff (Including Consultants)

- Job descriptions and skill sets/qualifications required
- Review Resumes of consultants to ensure they are qualified in accordance with the terms of the contract.
- Are there clearly defined job descriptions for all staff and consultants?

3. Project Plans

- Project plan and kick-off
- Is there a business case or project charter for the project?
- Was the project incorporated into the agency Disaster Recovery Plan (for mission criticalapplication)?
- Follow DoITT PMO Methodology

4. Data Collection

- Is data regularly collected and analyzed in the development of long-term (strategic) and short term (tactical) plans and are forecasts meeting the division's and the agency's mission, including such activities as succession planning, leadership development, and recruitment schedules?
- Create Project Sharepoint Site for documentation
- Change Control Process/ Change Management Plan
- Risks + Issues Log
- Review and Sign-off by the Business and PM all project documentation
- SOW from Vendor
- Lessons Learned

5. Policies & Procedures

- Comply with all City Policies and Procedures for Contracts, Security, Legal, etc...
- Define Data classification; ensure proper security controls are in place for development and infrastructure
- Security accreditation for all public facing and/or internal facing multi agency applications
- Request Vendor run security background checks on their project staff
- Identify mission critical applications; plan for disaster recovery

6. Financials

- Manage Project budget and track spending
- Review invoicing for proper billing rates and hours

7. Deliverables

- Define clear acceptance Criteria for each deliverable
- Ensure deliverables are delivered on time within scope and budget meeting quality criteria
- Do not pay Vendor for deliverables until they are accepted
- For large projects, break scope and delivery into smaller multiple releases to reduce risk

8. Vendor Performance

- Monitor performance of Vendor
- Raise issues immediately to Vendor when staff is not meeting performance expectations; request fire and new hire
- Raise issues immediately to DoITT Senior Management when PMQA or SI Vendors are not meeting performance expectations
- Ensure Vendor has proper Leadership in place for their project team and the staff is qualified to do the work they are tasked to do

9. Security

- All public facing and/or internal facing multi agency applications are required to go through a Security Accreditation process and complete deliverables to satisfy IT Sec.
- Even if the city application doesn't require going through the Security Accreditation process - at a minimum, all applications must comply with City IT Security procedures and policies.

10. Timesheets (Required for T&M Only)

- Sample the timesheets and make sure they are signed off and the tasks being performed are indicated on the timesheet and appear reasonable.
- The timesheet should be signed by the individual, the vendor project manager and the City project manager. Make sure overtime has prior written approval
- Timeliness of approval - Comptroller expects 60 days or less. If there is a delay in approval, it should be noted with reasons in the project files.
- Separate timesheets for FFP and Time and Materials.

11. Deliverables

- Deliverables approved and paid for by the city have been received and are readily accessible and kept in a shared drive.
- Timeliness of deliverables.

12.Invoices

- Vendor costs and service levels are materially accurate. This is demonstrated by maintaining documentation which has the proper reviews and approvals.
- Invoices for payments are allowable, reflect the amounts that are contractually agreed upon, which may include amendments and task orders.
- Costs are within contract and within budget.

13.Compliance

- Ensure we are in compliance with the City's procurement rules.
- For example: pay OGS rates if we are using a NY State contract.
- Ensure we are in compliance with all City directives – especially Directive #1 (Principles of Internal Controls) and Directive #5 (Audits of Agency Programs and Operations).
- For example: demonstrate that there is segregation of duties in our cash receipt functions (Directive #1).

14.Finished Products

- Product meets goals stated in the project justification and allows for future enhancements and upgrades.
- Product adheres to the project's mission plan.

15.Copies of the Systems Policies and Procedures, including:

- Back-up and disaster recovery.
- Security.
- Data entry and verification.
- Program change controls.
- How the source documents are reconciled to system files.

16. Travel Rate Requirements

- If the Project Manager is using a vendor that has travel rate requirements in their contract - they need to ensure that each of the consultants that charge the travel rate are actually living 100 miles from the facility. It is recommended that from time to time a roll-on form or resume be reviewed for those individuals charging this rate.
- "Travel" charges consist of a supplement of $50 per hour for any person that qualifies as a "Travel" resource, but there also is a "Travel Cap" of 20%. A contract may have a true-up at the end of the term to the extent that the Travel Cap is exceeded.
- Travel cap of 20% applies to both FFP and T&M.
- For T&M task orders, travel hours cannot exceed 20% of the total hours billed over the term of the contract. This is for each task order and **not to be aggregated together**.
- For FFP task orders, the contractors estimate the number of Travel hours needed cannot exceed the 20% of the total hours estimated for all fixed price Task Orders. The 20% of the total hours is for each of the Task Orders individually and **not the total** of the FFP task Orders.

17.Implementation Plans

- Development and implementation plans.
- Copies of any plans and implementation schedules for any changes to the project (i.e. adding new features, adding capacity, introducing new technology).
- Cost estimates and actual costs incurred to date.

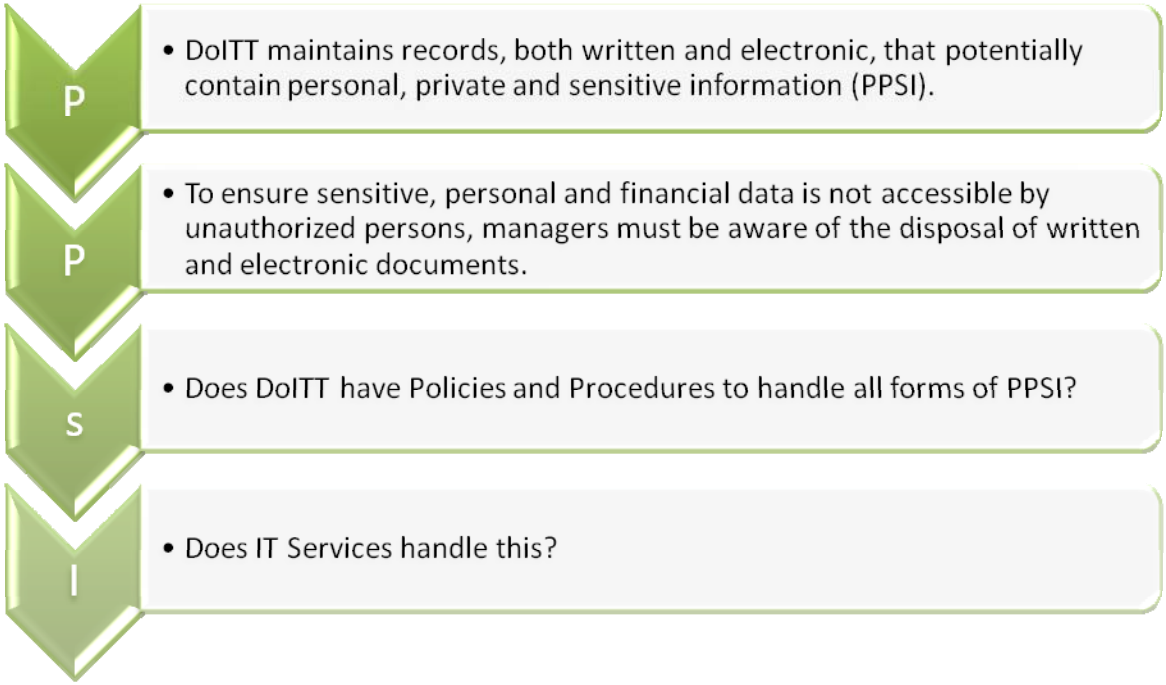
18.Vendor Management

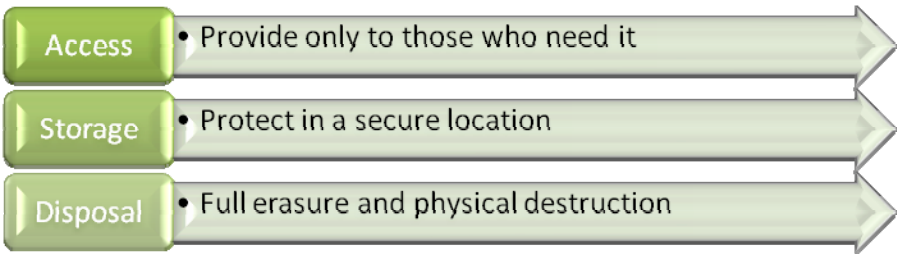
- Project functions reliably and information kept in the data and tracking systems is accurate and secure from unauthorized access.
- Equipment procured in accordance with the Procurement Policy Board rules.
- Prompt vendor payments.
- Signed NDAs are kept for all consultants working on the project.
- Does the Project Manager look at Vendex before choosing the Vendor?
- Acceptance Criteria - Is stated clearly and the course of action is understood by both the City and the Vendor?
- Is the PMQA taken to task for their job performance and is this stipulated in the Contract? Are they closely monitoring the System Integrator and is the City taking the necessary action when needed?
- Clearly defined job requirements for both the PMQA and the System Integrator should be part of every contract.
- Is there a clearly defined course of action if a System Integrator is not performing?
- The Project Management team should utilize the Vendor Management Office.
- VMO is responsible for the Performance Metrics on Vendors. A vendor management system has been rolled out that includes a new database for managing and reviewing vendor relationships and contracts across city agencies.
- Project Managers should periodically request VMO to send the roll-up reports from vendors (as required by contract) which will have detailed information such as the names of the consultants, hours worked and project costs charged.
- Ensure that the Business Sponsor is engaged in the Project.
- Review Vendor resumes/roll-on forms carefully
- Avoid Time and Material contracts
- Do not start a contract without the necessary resources available.
- Ensure that the Evaluation criteria and justification for picking a vendor makes sense.

2) Access to confidential information

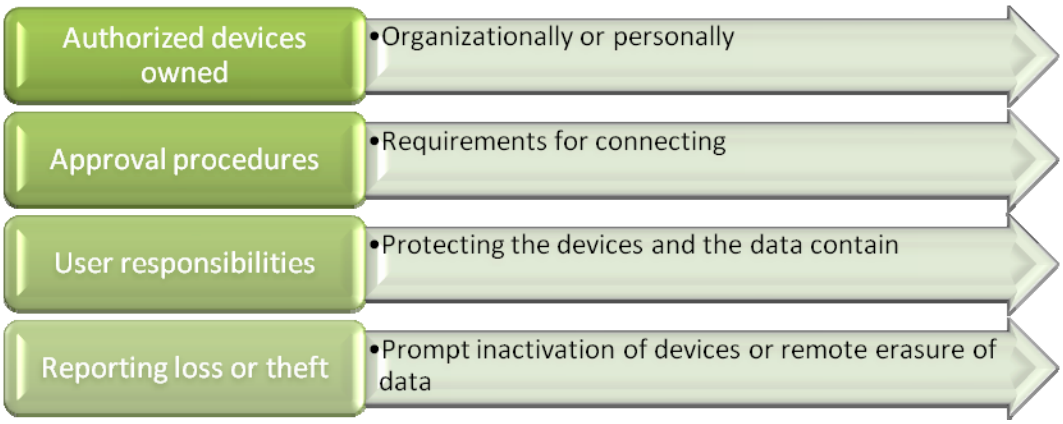
Confidential information consists of:

a. Confidential project information and other confidential DoITT information
b. Confidential personal information





3) *Mobile Computing and storage devices*



4) *Access Controls*

- Written procedures for granting, changing, and terminating access.
- Update rights as necessary (e.g., retirements, terminations).
- Each user should have his or her own network and application account and password.
- Assign access based on what users need to complete their jobs.
- User should set their own passwords.
- Hold passwords to complexity requirements to make them more difficult to crack or be easily guessed.
- Periodically compare employee master list to list of network and application user accounts.

5) *Personnel needed to support audit*

- Contracts Personnel-both on the Project and in the Contracts Unit
- Legal Counsel-on the Project
- Accounts Payable—both on the Project and the Accounts Payable Unit under John Winker
- Project Manager
- Risk Management and Compliance Unit- (Ensures that all documentation is readily available and performs a random sampling of documentation).

- ★ Administrative Staff-to help ensure that all documentation is readily available and is in order-(proper signatures and deliverables in place).

Chapter 2 – Internal Controls

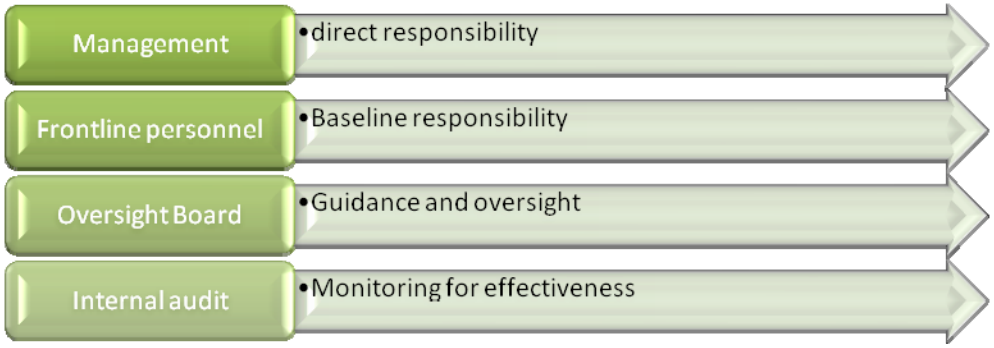
1) *What are internal controls?*

Internal controls, often referred to as management controls, in the broadest sense include the plan of organization, methods, and procedures adopted by management to meet its missions, goals, and objectives.

Internal controls also serve as the first line of defense against fraud and violations of law, regulations and provisions of contracts and grant agreements.

- Internal controls help protect assets and reduce the possibility for a fraud.
- Establish monitoring procedures.
- Improves efficiency of operations.
- Increase financial reliability and integrity.
- Helps compliance with laws and regulations.

2) *Who is responsible for internal control?*



3) *Internal assessments*

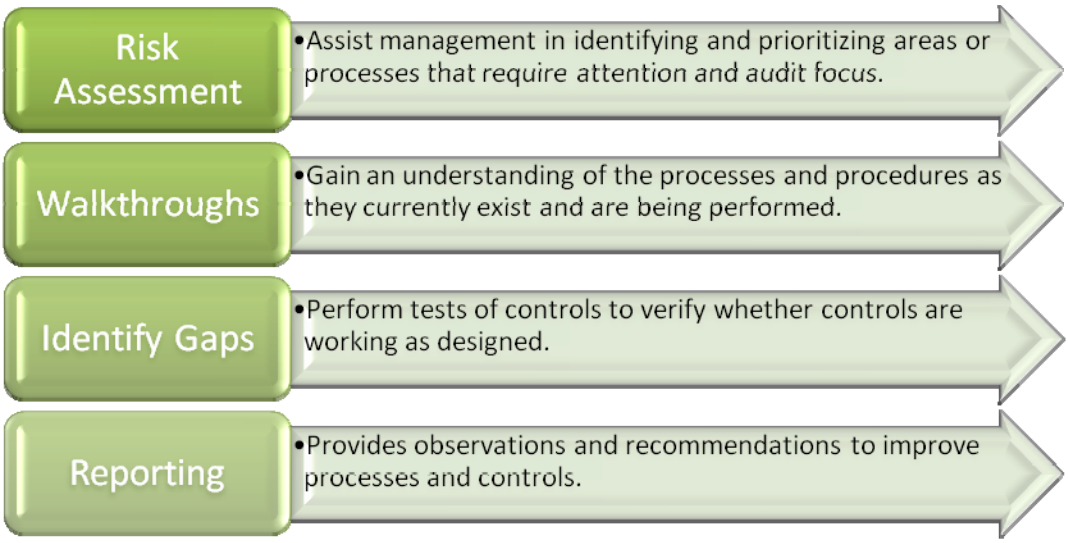
Internal assessments can be performed at the request of executive management.

Internal assessments are an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

4) *Benefits of Internal Assessments*

- Improves the "control environment" within the organization.
- Makes organization process-dependent instead of person-dependent.
- Indentifies redundancies in operational and control procedures.
- Provides recommendations to improve procedures.
- Serves as an early warning system, identifying deficiencies for timely remediation.
- Increases accountability.

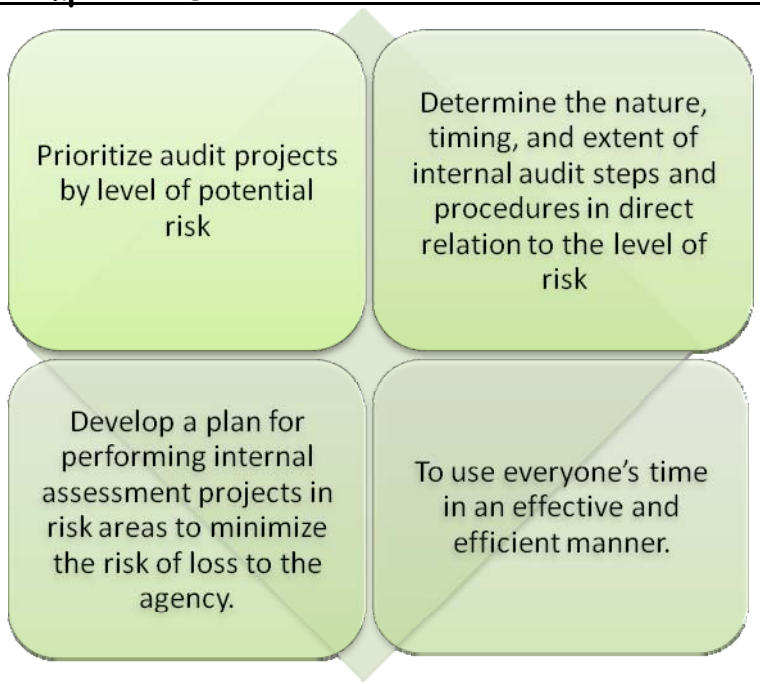
5) *What does the Risk Management and Compliance Division do?*



6) *Risk assessment*

Definition of "Risk": Risk is the probability that an event or action may adversely affect the organization or activity under audit. Examples of risks are performing work without funding, cost overruns, and lack of city oversight.

The purpose of a risk assessment is to enable the organization to:



Chapter 3 – Types of Government Audits

We have been audited by the Federal, State and City governments.

The scope of government audits may involve multiple objectives, including a review of the efficiency and effectiveness of programs and services, in addition to an examination of traditional matters such as financial statements and fiscal operations.

Government Auditing Standards issued by the US General Accountability Office define the different types of government audits as follows and provide a framework to help ensure professional, high quality work.

1.Financial Audits

- Provide and independent assessment of and reasonable assurance about whether an entity's reported financial conditions, results and use of resources are presented fairly in accordance with recognized criteria. Reporting on financial audits performed in accordance with GAGAS also includes reports on internal control, compliance with laws and regulations, and provisions of contracts and grant agreements as they relate to financial transactions, systems and processes.

2.Attestation Engagements

- "can cover a broad range of financial or non-financial objectives and may provide different levels of assurance about the subject matter or assertion depending on the users' needs. Attestation engagements results in an examination, a review or an agreed-upon procedures report on a subject matter or on an assertion about a subject matter that is the responsibility of another party."

3.Performance Audits

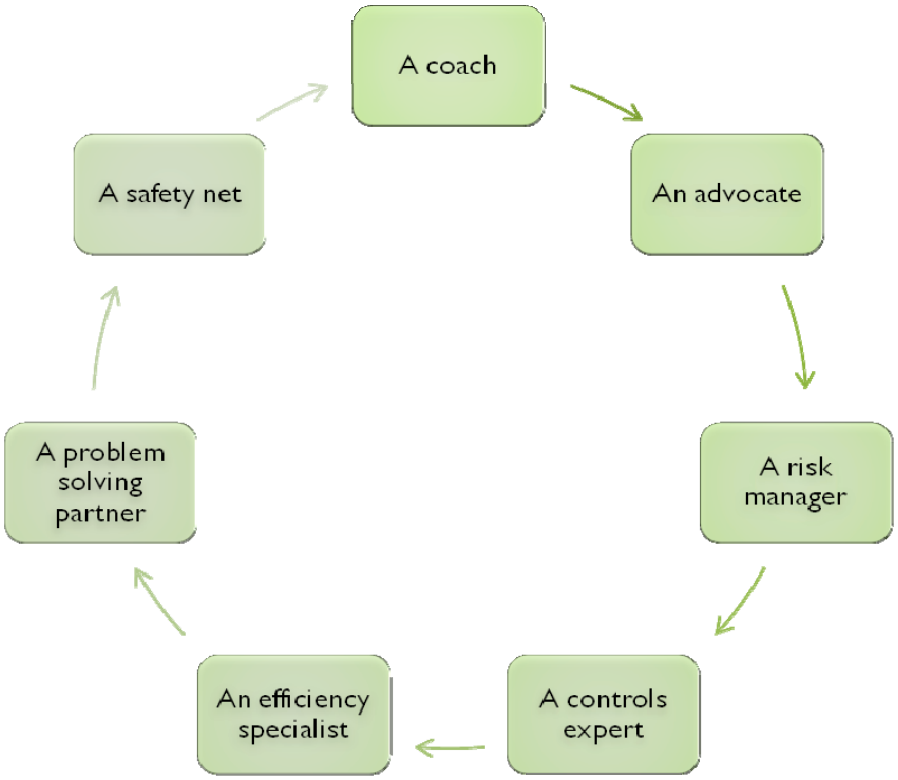
- Are engagements that provide assurance or conclusions based on an evaluation of sufficient, appropriate evidence against stated criteria, such as specific requirements, measures or defined business practices. Performance audits provide objective analysis so that management and those charged with governance and oversight can use the information to improve program performance and operations, reduce costs, facilitate decision making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability.

Performance audit objectives may vary significantly and "include assessments of program effectiveness, economy and efficiency; internal control; compliance; and prospective analyses" Moreover, a performance audit may incorporate one of more of these objectives.

Sample Internal Assessment Areas

What Risk Management and Compliance means to you?

You have, at your fingertips –


A coach
An advocate
A risk manager
A controls expert
An efficiency specialist
A problem solving partner
A safety net