Minneapolis
City of Lakes

Internal Audit Department
350 South 5th Street, Suite 302
Minneapolis, MN 55415-1316
(612) 673-2056

Date: July 19, 2016

To: Mayor Betsy Hodges; City Council Members; City Coordinator Cronk; Chief Information Officer Otto Doll

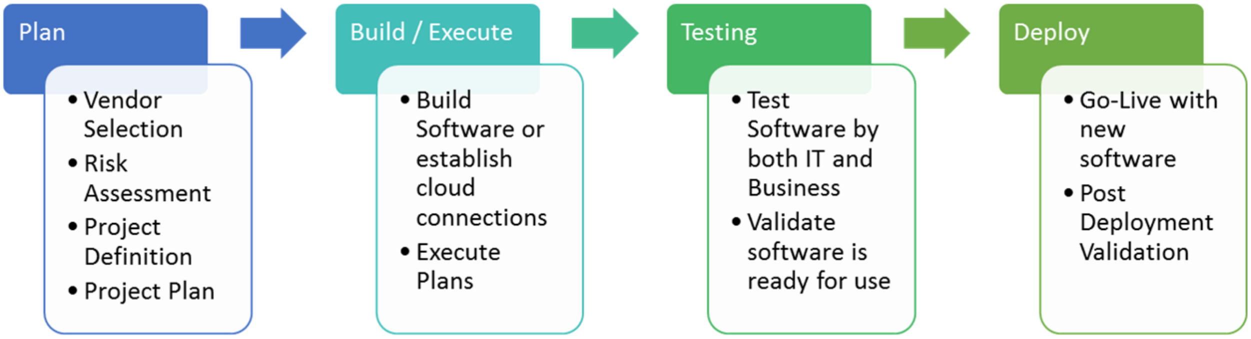
Re: IT Program and Project Management Office Review

Background

The Information Technology (IT) department's Program and Project Management Office (PMO) defines policies, procedures, guidelines and tools to be leveraged by the City of Minneapolis (City) IT Project Managers during an IT program or project lifecycle. Embedding security and privacy requirements throughout the lifecycle of an IT system implementation or upgrade helps lower the risk of unauthorized access or loss of data upon system go-live and ongoing operations support. The Internal Audit department was engaged by the IT department's PMO group to review the security and privacy considerations in their processes.

Scope and Approach

Internal Audit reviewed the PMO templates, policies, procedures, guidelines and processes to help determine when security and privacy requirements are identified, tested and implemented during the System Development Lifecycle (SDLC). The detailed phases within a SDLC vary depending on the implementation methodology selected by the project manager. However, at a high level; each SDLC methodology consists of the following phases and steps –



Plan
- Vendor Selection
- Risk Assessment
- Project Definition
- Project Plan

Build / Execute
- Build Software or establish cloud connections
- Execute Plans

Testing
- Test Software by both IT and Business
- Validate software is ready for use

Deploy
- Go-Live with new software
- Post Deployment Validation

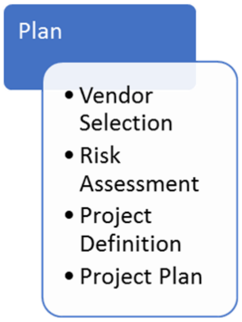
The City's practices were benchmarked against the System Administration, Audit, Network and Security (SANS) Institute security and privacy best practices for project managers to note the maturity of the City's program. The scope included:

- Security and Privacy considerations during system ideation / planning phases of the program or project.

- Development methodologies and how progress towards security or privacy objectives are being re-visited during each phase of the SDLC.

Observations

I. Request for Proposal (RFP) – Vendor Selection

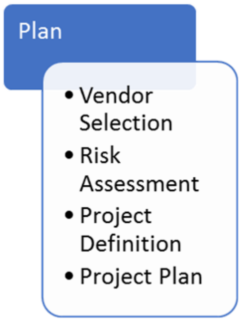


While selecting a vendor to deliver IT services, the project manager evaluates each vendor’s responses to an RFP and follows up on their references provided. The RFP vendor reference check guidelines provide potential questions to ask the vendor, such as the common challenges experienced with clients, delays in timelines, quality control, etc. but it does not provide any guidance or required questions on vendor security and privacy practices. SANS recommends inquiring about a vendor’s security practices including any past data breaches they have had at their organization. Not requesting information on how vendors secure their systems and data could result in a potentially vulnerable system design and implementation. Having a vulnerable system could result in unauthorized access or loss of sensitive and/or confidential data. This should especially be a requirement for any hosting, cloud or web-based solutions where the City would have limited to no control to the IT infrastructure (physical servers at the vendor site) as it will be outside the City network.

Request for Proposal – Vendor Selection Recommendation

The IT PMO group should incorporate questions on vendor security and privacy practices in the RFP vendor evaluations. Key factors to consider are vendor access to the City network, secure data transmission protocols, independent audit reports on the vendor security and data breaches they may have had in the past. This will help the City better understand if the vendor’s security practices meet the defined internal policies. It is important to note the vendor’s policy on incident management protocols for security incidents and data breaches. Determining if the vendor has appropriately defined practices to act and communicate in a timely manner during a security incident helps note the priority they place on customer data. Instituting such a process of evaluating vendors helps better understand the risk profile of the potential future business relationship and the degree to which the vendor may potentially need to be monitored.

II. Project Definition & Risk Assessment



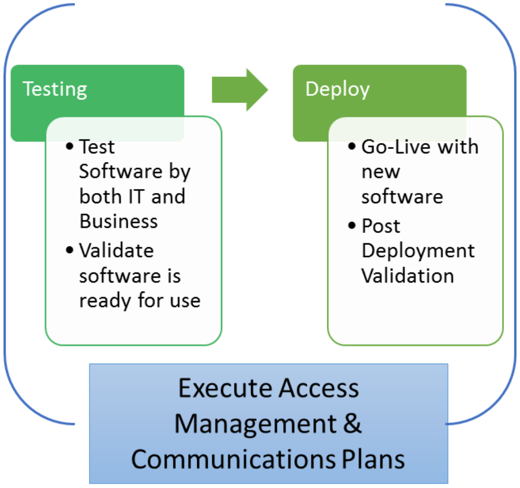
During the Plan phase of the SDLC, the project manager is responsible for creating the project plan which includes completing a project definition and a project risk assessment. The project team uses the Project Definition document to clearly define the project, including the business drivers, stakeholders, goals and objectives. The definition process facilitates agreement on the baseline scope, proposed solutions, total cost of ownership and the targeted value on investment that is expected to be realized. The IT PMO risk assessment guidelines and templates provide a framework on how to assess a risk and what risks to consider during a system implementation. The key risk areas identified to be assessed relate to innovation, backup plans and financials.

There are no formal security and privacy scoping considerations within the project definition template or a requirement for a security and privacy risk assessment for each IT project. Not being required to consider security and privacy risks within the project definition phase or risk assessment processes creates the potential risk of unforeseen budget impacts and project scope increases later on the in the project lifecycle. It also creates the risk of a potentially vulnerable system design and implementation. This could result in re-work of the system design and functionality when the risk manifests themselves during the project implementation or during ongoing operations. Such an impact causes increased costs, unauthorized system access, data breaches and loss of data.

Project Definition & Risk Assessment Recommendation

The IT PMO group should consider formalizing a section for security and privacy within the Project Definition phase and requiring a formal security and privacy risk assessment for each IT project. This will help integrate the key requirements early within a project lifecycle, lowering the risk of absent security controls upon system go-live. It would also help lower any scope creep or budget over runs as requirements for security and privacy will be defined early within the project lifecycle. The risk assessments would also help define the role IT Security should consider for the project lifecycle including a financial and human resource plan. Factors such as type of data being used for the project, hosting, production data for testing, vendor and consultant access, etc. should be included from a security and privacy perspective in the risk assessment.

III. Project Access Management and Communications Plan


Testing
Test Software by both IT and Business
Validate software is ready for use
Deploy
Go-Live with new software
Post Deployment Validation
Execute Access Management & Communications Plans

An IT project utilizes testers from multiple areas of the City such as the business teams who will be the end users of the new system, the IT team, the vendors, third party integration testers, etc. Testing is generally performed using shared IDs or non-uniquely identifying accounts as it helps expedite the testing and one tester could access multiple IDs to test the functionality assigned to each account. Who has access to these test accounts and the duration that they will need it depends on the size and complexity of the project. In addition, project teams are required to have elevated access to the live production system during the migration phase to help with troubleshooting and system stabilization. However, this access should be revoked when the system is turned over to operations support because it is no longer needed for the project team's ongoing job responsibilities. During a system implementation or services definition, there are multiple vendors and independent consultants that gain access to the City's IT resources and network. The access needed by a user during testing a new software may be different than the access they need once the system is live and in use. In order to better manage the access to these test and migration accounts and communicate how, when and where they will be utilized should be formally defined within Access Management and Communications plans. When a project contains 'non-public data' further consideration should be given to how secure communications should be conducted.

An Access Management Plan defining authentication protocols, password management and authorizations (roles for system access) for the project team during its lifecycle does not exist at the City. A communication plan that helps define the different types of communication needs, audience, type (formal or informal) and mode of communication for a project does exist but it doesn't explicitly consider secure communication channels. The City's IT Project Plan template does not identify secure communication methods and channels available for the project team to share 'non-public data'.

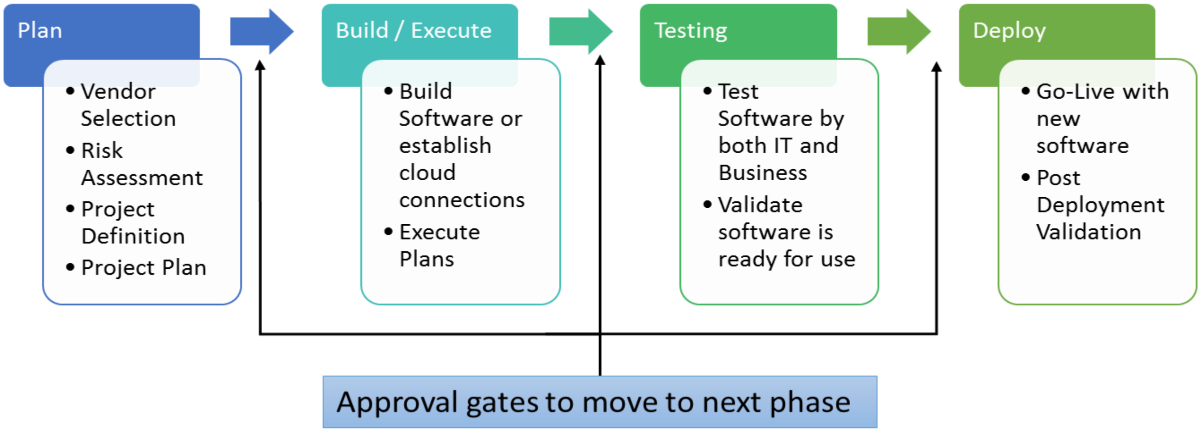
This lack of an Access Management plan creates a risk of not knowing who had or continues to have access to what data within the City's network and IT landscape. Risk of data manipulation or loss due to unauthorized access increases significantly when the project team's access is not formally defined for the entire project lifecycle including after system go-live. Not defining secure communication methods available to the teams increases the risk of loss of sensitive or confidential information via data breach or accidental loss. Defining secure communication routes lowers the risk of losing sensitive or confidential information in addition to potential intellectual property.

Project Access Management Plan Recommendation

IT Project Managers, in collaboration with the business lines should be required to define an access management plan for a project team for the entire project lifecycle. Shared, vendor and contractor accounts should be well managed in order to help ensure authorized access to the system, especially after contract termination. The IT PMO group should also define a formal secure communication protocol that enables a secure mode for data transmission among team members and vendors. Steps on encrypted emailing and other secure communication methods that can be leveraged by the project team should be defined and documented. Consideration should also be given as to how communications with vendors or contractors will be impacted if non-City provided IT assets are used for communications.

IV. Approval Gates

There are multiple project implementation methodologies that can be leveraged for a system implementation. Each methodology has its pros and cons with respect to how it impacts scope, timing and funding. However, one aspect common among the methodologies is the use of a forum to gain approval on what could or couldn't be completed, outstanding risks, budget, scope and team member impacts within a phase before moving to a different phase of the project (example would include moving a project from the development to testing phase). A gate provides the forum for formal approval by the project's key stakeholders to move forward to the next phase of the SDLC in the project.


Plan
• Vendor Selection
• Risk Assessment
• Project Definition
• Project Plan
Build / Execute
• Build Software or establish cloud connections
• Execute Plans
Testing
• Test Software by both IT and Business
• Validate software is ready for use
Deploy
• Go-Live with new software
• Post Deployment Validation
Approval gates to move to next phase

The City's approval gates do not require a formal approval or consultation from the security team to pass each phase of a project. Change in scope, timing or budget could impact the security considerations in a project. Not having security embedded as part of the project phase approvals, creates the risk of missing security needs that may have risen after initial risk assessment and could result in increased costs, unauthorized access and / or loss of data from the network.

Approval Gates Recommendation

The IT PMO group should consult the IT Security team after the completion of key milestones within a project. This will help to note if there have been any changes to project scope or risk profile from the initial security and privacy risk assessment performed. If such changes do occur, it would potentially require a modification to the security and privacy strategy of the project including but not limited to system design, funding and delivery timing.