Security Accreditation Process

Scope

All externally accessible, public facing applications and internally accessible, multi-agency applications developed to support City of New York business must be built in a secure fashion. These applications must successfully complete the security accreditation process to ensure compliance with security policies, standards and best practices. Successful completion is acknowledged by the Citywide Chief Information Security Officer (CISO) and must be achieved prior to launch in production.

Accreditation Process Overview

The Accreditation process is an oversight or overlay process on top of the Software Development Life Cycle. It is designed to integrate into specific areas of the SDLC and build security into the project from the beginning, avoiding costly re-design or resolution of security issues in later stages. The role of the IT Security Engineering team in the process is to partner with the project team, enabling secure, feature rich and timely development of applications where risks are appropriately understood and addressed.

It is important to note that while projects require many meetings and discussions, the actual assessment process will use the security accreditation document as the authoritative source for information. ***Clearly written and detailed documentation is the key to ensuring an efficient and timely assessment.***

Security Accreditation Document

The artifact of the security accreditation process is the Security Accreditation Document. This is a living document that facilitates communications between the project team and the IT Security Engineering team. The document is a multi-part template. Each part gets completed by the project team and subsequently reviewed by the IT Security team at various stages of the process. At the end of the project the completed Security Accreditation Document will contain all the relevant information about the project from a security perspective. The information will range from high level business requirements all the way down to IP Addresses and class names. It is important to note that each review may take multiple iterations and/or meetings, until both the project team and IT Security team are on the same page about the relevant content and all security questions have been addressed. A successful accreditation process can be ensured by starting the process during planning stage and before requesting funding. If the process is not started in the planning stage, it may be too late and will jeopardize the project.

Security Resourcing

Just like any other part of the project, such as infrastructure, hardware, software, development time, QA etc, IT Security is an integral part of the project and should be included in project cost calculations. Each large or complex project should dedicate from 10-15% of the total project budget for IT Security.

Agile and Waterfall Development Methodologies

The accreditation process is equally adaptable to both the Waterfall and Agile development methodologies. The activities depicted in the Agile Model diagram below correspond roughly to the plan, design, build, test and deploy phases of the Waterfall model. Please note that in an Agile model, these activities are intended to be shorter in duration. Also note that Agile methodology requires a resource to be an integral part of the project team at the scrum level and participate in stand-up meetings and facilitate "on-the-ground" security decisions.

Software Development Life Cycle (SDLC)

The following diagrams depict the Software Development Life Cycle and appropriate checkpoints for information security assurance. Please note that these are also available as a checklist to facilitate smooth a smooth flight through the accreditation process.

Agile Model

Accreditation Process Details

The following steps describe the accreditation process:

1. **Planning / Analysis:** Determine the data classification and determine identify the business functions the application will address.

   - Define project objectives.
   - Complete Intake process and assign business owner/project manager (where appropriate).
   - Identify data classification types, hosting location and targeted user community.
   - Gather business requirements.
   - Determine data classification and regulation requirements and planned security controls.
   - Define security resource requirements.
   - Submit Accreditation Document to IT Security with following:
     - Business objectives
     - Business and project team members
     - Hosting and service level
     - Data classification Type
   - IT Security Engineering team to provide security control requirements and suggestions.

2. **Design:** Develop technology solution by leveraging tools, technology processes, and best practices to design the solution.

   - Complete high-level system design and application flow.
   - Define system requirements and service levels.
   - Submit Accreditation Document with the following:
     - High level design (Logical and Flow diagrams)
     - System Requirement and Hosting information
     - Security Controls (AAA information)
     - Review changes to adjust from the previous version.
     - Data View (Further information about data classification).
   - IT Security will review system design to ensure it meets security requirements.

3. **Development:** Code, build hardware, and deploy the application to QA environment.

   - Ensure all integration points meet security requirements.
   - Make sure application and systems are built according to design.
   - Inform IT Security team of any design or requirement changes.
   - Update Accreditation document with any requirement or design changes.
   - Perform Development environment App Scan and fix code as necessary.

4. **Testing:** Perform unit, system, and user acceptance test cases against the QA environment.

- Perform/request AppScan and MVM (McAfee Vulnerability Management) scan after the production code is deployed.
  - Submit AppScan request form to IT Security Engineering group. See AppScan Process for detail.
- Correct any findings (***all Medium and High vulnerabilities must be addressed***) from scans and rescan as needed.
- Provide scan detailed reports on scan findings.
- Update Accreditation Document with business and/or application risks identified.
- Finalize the Accreditation Document and make sure no changes to previous version.
- IT Security will review scan reports and provide guidance on addressing findings.
- Review Accreditation document to ensure all risks are addressed and the system is ready for final accreditation review.

5. **Implementation:** Deploy to production environment.
   - MVM scan to be completed by infrastructure team (after the production code is deployed).
   - Address all High and Medium findings.
   - Submit infrastructure vulnerability scan reports with all findings rated Medium and High resolved.
   - SOC team can provide guidance on addressing vulnerabilities found.
   - Provide a written communication from business owner stating the acceptance of any risks not addressed prior to implementation.
   - IT Security Engineering does final review of Accreditation Document for completeness.
   - Accreditation sign-off provided by Citywide CISO.

Accreditation High Level Criteria

Confirm the following requirements have been met. Please note that this is a high level check list. Detailed checklist is available on the first page of the Security Accreditation Document Template.

1) Data has been classified.
2) Data security controls match data classification levels.
3) Security Accreditation Document has been completed clearly and entirely.
4) System complies with ALL Information Citywide Security Policies, Standards and Guidelines (as they exist at project initiation), as well as generally accepted best practices as recommended by OWASP, ISO27001/2 and NIST.
5) Security Architecture complies with CityNet Security Reference Architecture.
6) System is in compliance with applicable regulatory and industry standards and applicable

laws (such as HIPAA, PCI).
7) System authentication credentials are stored in the Enterprise directory.
8) All user and application access to the system and its internal components (including web services) is properly authenticated and authorized.
9) System names comply with enterprise naming standards.
10) System utilizes proper enterprise DNS and SMTP services.
11) IBM Watchfire Application Scan (AppScan) scans are complete (All web and web service components scanned). and all medium and high severity issues have been addressed.
12) Infrastructure Vulnerability scans (McAfee MVM) of all new system components are complete and all medium and high severity issues have been addressed.
13) Results from any third Party assessments be reviewed and their remediation verified (if applicable).

Re-Accreditation

Application is subject to re-accreditation when any code, design, or data requirement is changed. Under normal conditions, an update to the existing accreditation document to reflect the changes would suffice, along with App Scan infrastructure vulnerability scan (if additional hardware is added to the design). This is also the case with Agile Development methodology. Every iteration requires necessary updates to the accreditation document and an appscan.

If an application is subject to major release, substantial functionality or architecture change, it will be subject to a new accreditation process. Review the changes with IT Security Engineering team to determine the requirements.

Exceptions

When consensus cannot be reached between the Business Owner and the Citywide CISO over the risks associated with an accreditation process finding, an exception can be requested. In recognition of the risk management approach in which policy exceptions are applied, an exception from a policy provision may be requested and granted due to unusual and/or exceptional circumstances. The approval process for exception requests shall be as follows:

1) The requestor or business owner desiring an exception to a policy provision shall complete a thorough analysis to determine if the unusual and/or exceptional circumstances will have any potential impact on the security of Citynet, any other City of New York agency, or any customer or partner.

2) Exceptions will only be granted based upon lack of a suitable technological control or on a time limited basis with the suitable compensating controls and defined resolution date.

3) The agency desiring an exception to a policy provision will also complete an analysis to determine if approval of an exception for the extraordinary circumstances would adversely affect compliance with any legal or regulatory requirements.

4) If the Agency determines that there will be no adverse impact or if there is a minimal adverse impact on another party, that agency's commissioner sends their request to the DoITT Commissioner.

5) The exception request will be reviewed by the Citywide CISO to confirm the impact is acceptable.

6) Risks must be accepted by the executive level business owner.

7) If there is non-concurrence, the final decision to approve the exception rests with the DoITT Commissioner and the Citywide CISO.

8) If an exception request is disapproved, it is the responsibility of the requesting City agency to remediate the circumstances that required the exception request.

Appendix A – Determining the Need For A Third Party Security Assessment

The goal of a third party security assessment is the preemptive discovery of application security vulnerabilities. When determining the need for an assessment, the most important considerations must be the volume and classification of the data and the transactional complexity of the application. The more complex the application, the more potential opportunities exist for a determined adversary to circumvent the application security controls. The value of the data should also be considered. Using this information for context, the Business Owner should consult his agency security lead as well as the DoITT CISO to determine if a third party security assessment is right for their application. The Open Web Application Security Project (http://www.owasp.org) can provide more background information on application security assessments.

Appendix B

Security Accreditation Process Service Level Objectives(SLO):

Stage	Initial Review – Days By complexity	Follow-up Review – Days By complexity	Ave # of iterations
Planning / Analysis	Low 1 Medium 2 High 2	Low 1 Medium 1 High 2	2
Design	Low 2 Medium 5 High 8	Low 1 Medium 2 High 4	5
Build	Low 1 Medium 3 High 5	Low 1 Medium 1 High 3	3
Test	Low 1 Medium 2 High 3	Low 1 Medium 2 High 3	3
Deploy	Low 1 Medium 2 High 3	Low 1 Medium 2 High 3	2

* This SLO only applies when accreditation starts before the planning and analysis phase. Unaddressed issues will lengthen the process. Also note that these SLO only apply to Waterfall model.

Document Revision History

Date	Version	Description
January 3, 2012	Version 2.0	Major update of entire document
March 26, 2012	Version 2.01	Fixed several minor typographical errors.