System's Assessment Methodology and Process

Prepared by: George Farah, GSEC Gold
Information Systems Security Manager
Queen's University, ITServices
February 20, 2007

Document Control

Authorities

Author	Role
George Farah	Information Systems Security Manager

Approved by	Role & Approval Responsibility	Approval Form Signed and Dated on:
George Farah	Information Systems Security Manager	
Sean Reynolds	Chief Information Officer	

Distribution list

Name	Organization/Role
All ITS Managers	

Revision History

Version	Reason for Issue	Date
V 1.0	Initial document	20th Feb. 2007

Table of Content

- **System's Assessment Methodology and Process**

What

1. System's Assessment is the holistic risk-based analysis of a computer system, network and application's technical and non technical components to seek out vulnerabilities that constitute risk to Queen's infrastructure and data.

2. The assessment process involves an exploration of the all security features of the system in question, including its environmental, and operational needs, followed by an attempt to explore possibility to breech security and compromise the system.

- **System's Assessment Methodology and Process**

Why

1. The threat Model today that IT systems face is growing and changing
2. University requirements to protect personal and confidential information
3. Privacy legislation requirements pertaining to the protection of personal information (FIPPA)
4. Identified as an audit requirement
5. It enables a risk based assessment and integration of risk assessment in deploying systems across ITServices and Queen's university.
6. Provides the ability to apply consistent IT controls across systems at the university

- **Today's Growing and Changing Threat Model**
    1. Exponential growth of attacks
    2. Today's Growing and Changing Threat Model
    3. Changing nature of attacks

- **System's Assessment Methodology and Process**

When

System Assessment is done in one of two situations:

1. New project initiatives: where the assessment will be done on all system components (Operating Systems, Databases, Applications and Network) that need to be promoted to production.
2. Systems in production: when major changes are done to the system in production which changes the security status of system or device(Server OS, Database, Application behaviour). Example: Major code implementation to add functionality, upgrading the operating system platform, or database, etc.

- **System's Assessment Methodology and Process**

How

- ***Two phases***
    - First Phase**: Environmental and Operational includes**
        - Defining the statement of sensitivity of system and data by asking:
            - What if the information is lost/destroyed/stolen/modified?
            - How much will it cost to replace?
            - Or ends up on the front page of the Globe and Mail?
            - Will it affect the credibility of Queen' University?
            - Will it compromise our competitive position in the marketplace?

- What will happen if personal privacy of users is compromised?
- How would the system/data owner classify the data housed by the system?

Defining Operational and Environmental requirements:

- Does the system require a system admin for support?
- Does it require backup and recovery?
- Does it require a disaster recovery plan?
- Does it need protection controls related to antivirus, spy ware, file system protection?
- Requirements for documentation, secure code reviews?
- Providing assistance with secure design decisions?
- Where does the system need to be housed? Data Center requirements?

- Second phase**: Conducting a penetration test**

1. Penetration testing is an integral part of System Assessment
2. Penetration testing is the security-oriented probing of a computer system, network and application to seek out vulnerabilities that an attacker could exploit. The testing process involves an exploration of the all security features of the system in question, followed by an attempt to explore possibility to breech security and penetrate the system.

- The penetration testing process can be sub-divided into distinct phases:
  - Information gathering
  - Preliminary scans
  - Application scans
  - Vulnerability and risk assessment
  - Report generation with mitigating/action items
  - Meetings with all involved
  - Follow up as required

Conclusion

- The system's assessment methodology and process is critical to our ability to integrate risk assessments in deployment of system components within ITS and across campus.
- It will help us to add value by enabling educated and well informed decision making regarding IT related risks.
- It will help us start to address some of the weaknesses we keep encountering by adding protection controls and enhancing IT security practice in ITServices and on campus IT shops.