Server Hardening Example Checklists

Initial Platform Hardening at a minimum includes:

- Install the operating system from an trusted source
- Apply operating application patches and updates
- Remove or disable unnecessary system services and/or drivers
- Uninstall unnecessary software
- Set security parameters, file protections and enable audit logging
- Disable or change the passwords of default accounts
- Install institutionally approved anti-virus software when appropriate
- Configure password expiration and complexity settings
- Enable password history
- Log password changes to the specific IP with time/date stamp
- Ensure credentials are hashed and not viewable in plain text when stored on server
- Implement time activated logon ID lock
- Ensure logging enabled to record when last successful login took place
- Enable session timeouts
- Configure logging parameters as appropriate to the classification of data stored on the system
- Provision firewall rules relevant to the application of the system
- Perform initial scanning for vulnerabilities
- In template / VM environment, application of these principles to the template, and subsequent logging of the testing of the template, is sufficient to assume the resultant guests are hardened.

Ongoing System Hardening

At a minimum ongoing system, hardening must include:

- Internal and external vulnerability scanning using industry standard tools, such as Tenable Nessus, should(?) be conducted at least quarterly to insure a system is maintained at a standard level of compliance.
- Monitoring of access and system logs for suspicious traffic or activity
- Risk Assessment done yearly as to examine the extent of risks to organization.
- Maintaining a schedule to include and OS and or Application specific updates for Systems to be done as needed, minimally once a quarter.
- Installation of virus detection software of software if applicable.
- Information Owners/custodians should review of access rights of individuals to system to ensure they are still valid based on role definition.

Portable Device System Hardening

- Passwords and PIN are required
- Portable devices should be encrypted if they have access to confidential data.