Server System Hardening Steps (Current & Future Forward)

1. Install OS.
2. Configure to Domain.
3. Assign to Appropriate OU with assigned group policies.
4. Assign any further specific group policies in accordance with build requirements.
5. Remove any un-necessary roles and features that may have been installed.
6. Perform all OS updates.
7. Install and configure role-specific software or modules.
8. Verify state of firewall configuration and placement in network.
9. Verify LAPS enrollment.
10. Perform a vulnerability scan to determine any risk factors.
11. Quality control review to confirm prior steps.
12. Submit for approval, approve deployment.

Workstation System Hardening Steps (Current & Future Forward)

1. Deploy via Central Image.
2. Assign to Appropriate OU with assigned group policies.
3. Assign any further specific group policies in accordance with build requirements.
4. Perform all OS updates.
5. Install and configure role-specific software or modules.
6. Verify state of firewall configuration and placement in network.
7. Verify LAPS enrollment.
8. QC and Deploy.

Achieving an Optimized Standard Build Process (Future Forward)

1. Determine business needs of each business unit.
    a. Build out minimum requirements document as required.

2. Determine data restrictions for each business unit, if applicable.
    a. Make appropriate notations to the business unit's custom build document.

3. Determine User Rings for Workstations
    a. *Insider Ring* – Intended for IT and InfoSec. Highly technical users identified in a business unit can be invited, but a backup image should be available to them should an update inhibit their job obligations. These users would fall in the "Fast Insider Ring" for Windows Updates.
    b. *Power User Ring* – Intended for users identified in each business unit that can operate as a test user and provide guidance to coworkers with new releases when they are rolled out. These users would fall in the "Slow Insider Ring" for Windows Updates.
    c. *General User Ring* – Intended for general users and aligns with the regular Microsoft release cycle.

4. Develop Builds
    a. Each system should be built out and kept turned off in a virtualized environment unless being worked in to update and delta a new image for deployment. Their ring configuration to be defined via Group Policy and Security Groups.

5. Assign builds and deployments based on the optimized process.