The very first thing is more assumptions are going to have to be made due to partial vagueness of the question. For instance did we build there server? Or similar to the environment that I am currently in, did someone else build the system and now it goes to the hardening team? What type of environment is this server in? What information does this system process? What is the value of the data to the system owner? How long can the system be down? Logically is this server a single application? Or part of an existing system? Etc... These question will have an impact on the security standards and controls that we have to implement on the system in order for it to be harden correctly before production deployment.

To further clarify the question we will make the following assumptions:

* We did not build the system. The System was built by a team of Integrators and then handed over to the Security Engineers to perform the hardening.
* This IS (Information System) is a single self-efficient independent system, not logically supporting a larger IS.
* We will assume this system is being integrated into a datacenter environment.
* We will assume this is a federal datacenter.
* This system does not contain any Medical, PII, or classified information.
* This system does not process or store payment information.
* This system non-mission essential therefore system down time does not impact business goals
* The data this IS contains is non-essential and is therefore a low value asset
* The IS is hosted in a Virtual Environment
* A continuous monitoring solution has been implemented.

Now that we have enough of the unknown variables defined for this exorcise will begin hardening said IS:

* The first step is to insure I had all the build documentation that should have been generated during the build phase of this IS. In the event that build documents where not generated a thorough investigation will be conducted of the system to insure all parts of the IS and how it was built is documented so that proper hardening can occur.
* I will also retrieve the latest copy of the SSP (System Security Plan) and any other SOP (Standard Operating Procedures) style documents that are relevant for the hardening process (This includes what Firewall, Antivirus, HIPS application is used, etc.…).
* I would then research the best security practices for the software that is hosted/part of the IS.
* If the application is non GOTS/COTS then documentation from the developers may be required as well as a code review.
* With this system being federal the NIST framework will be used in this situation so a thorough review of the system level controls will be researched and applied to the final security implementation plan.
* I would then scan the system with the continuous monitoring system and document the vulnerabilities so that they can be added to the hardening plan
* Once I have all the necessary documentation together I would then formulate a plan to implement the security changes to the system in a pragmatic way, organizing the changes I plan on making from least likely to break the application to most likely to break the application.
* I would then perform a full system backup along with taking a snapshot of the system.
* I would then check to insure the IS is fully updated. In the event that it is not I would check vendor documentation as well as the system builders and system owners to see if there is known conflicts that cause the application to break. If there is, those updates will be documented, and mitigations developed/researched to be put in place until the issue has been remediated and the updates are able to be installed. I would then install all/remaining updates to insure the system is fully updated before I begin hardening.
* Assuming the updates did not cause anything to break I would create another snapshot (in the event an update did break the application, A rollback of the updates one at a time, testing the application each time would occur until the offending update was identified. It would then be documented and a mitigation strategy would be developed as necessary).
* I would then begin applying the changes as outline in the plan I created one at a time, insuring the system is still functioning, taking snapshots and documenting the changes (Success and Failures) each step of the way.
* Once the initial Harding process has been completed, I would scan the system again with our continuous monitoring solution to insure that It can still talk to the system and to identify any security related issues that may have been missed/added since the first scan. Assuming more has been identified the change process again would be followed to mitigate the remaining vulnerabilities.
* I would then scan the system a final time insuring there are no outstanding vulnerabilities that have not already been documented as requiring mitigation strategies due to breaking the application.
* I would then baseline the system, formalizing the documentation of the changes that occurred, the vulnerabilities that could not be fixed due to breaking the application, the open/listening ports operating on the system as well the application behind those ports. This step could include taking a hash of the system that could be used to compare in the future to identify changes. This depends on the sites baselining policies.
* At this point the snapshots can/should be deleted. The Initial backup that was taken will abide by the sites retention policies and will be deleted as those policies dictate.
* The system at this point can continue to the next team for integration into production.

Those are the step I would take to harden the system. The fact that IIS is installed does not change the hardening process. If the technician performing the Harding is thorough then IIS best security practices are researched and the proper Security Framework controls are added to the security plan during the research phase of hardening.