Chapter 8

Deployment Processes

The deployment process includes many of the configuration management (CM) tasks and programs. Deployment is a process that is repeated over and over as new software and hardware is introduced to the infrastructure to address business needs. The deployment process is very straightforward, but the details and how an organization actually implements them are complex. Many organizations neglect to follow the process and have issues with deployment because of the omission of critical steps. But dismissing certain steps as too costly or ineffective will later prove to be a poor decision. The steps exist to ensure that there is accountability and supportability in the deployment process. The deployment process is shown in Figure 8.1.

Selection Process

The selection process is the first step in the deployment process. The selection process is critical. The one thing an information technology (IT) department cannot afford to do is spend time and resources on projects that are not required or are ill-conceived. The selection process is about choosing partners and products to deliver a specific solution. Careful attention to budget is critical. IT departments have been carefully monitored from a budget standpoint for the past 7 years. In the current operating environment it is critical to ensure that the best value is delivered in solution deployment. The selection process is shown in Figure 8.2.

Needs Assessment

Needs assessment is an assessment of the needs of the business and its various business units. This review of technical deliverables must include the business owners.

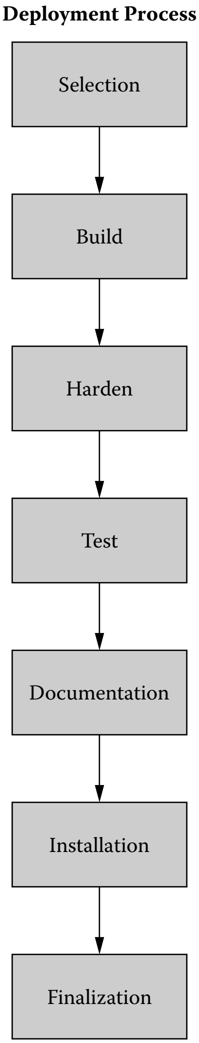

Figure 8.1 The deployment process.

The requirements start with the business owners making requests to the IT management for various services. The requests should not be specific, but should be focused on how an IT service will improve operational efficiency or quality. The IT staff will worry about the technical and product details. A needs review can occur near the end of the year before the following year's budget is solidified. This will give the IT department time to prioritize new projects and the budgets required for

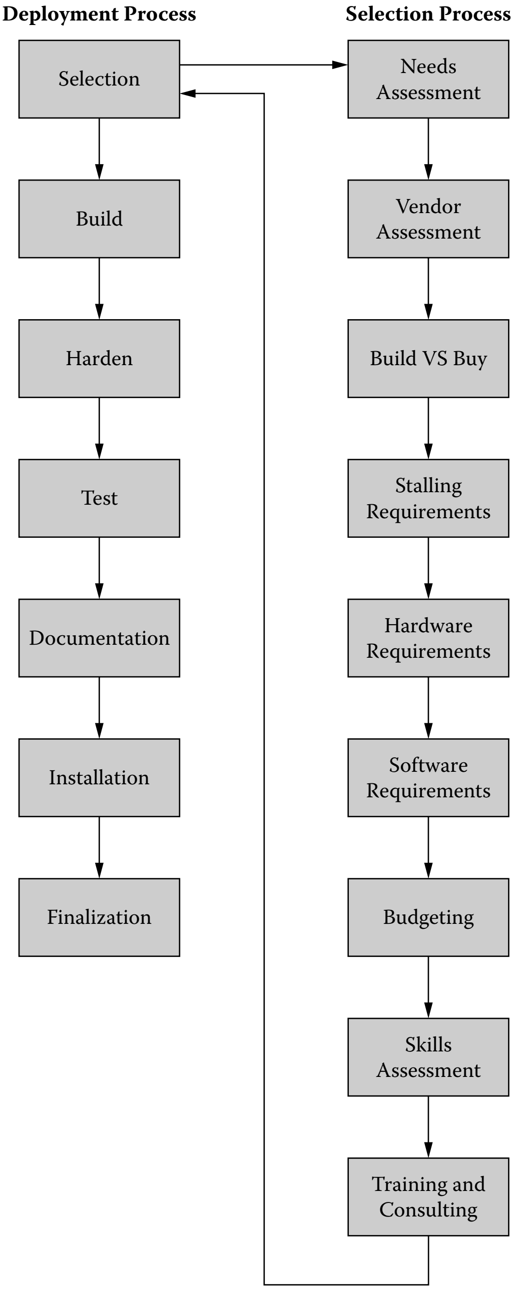

Figure 8.2 The selection process.

each project. The IT department should try to discover what initiated the request. Many times end users will hear of new services from friends or colleagues. The IT department should be aware of the latest IT developments in their industry segment. They need to understand both the positive and negative aspects of industry segment systems so they can articulate the complexities of any changes introduced into their current environment.

Vendor Assessment

Once there has been a review of the new projects the IT department will be adopting, a review of current vendor technology needs to be conducted. In mature businesses there will be line of business applications that are already in use that will need to be considered by any new project. The adoption of commercial off-the-shelf technology will greatly reduce the costs associated with installing and maintaining a set of software-based services. The other option is to build your own software, which in almost all cases is more expensive than using off-the-shelf software. Many times there are multiple vendors that provide a specific type of software functionality. The details may be different from vendor to vendor, but usually the basic services provided are similar and are grouped together into a specific category of software service. When assessing a vendor's software, the IT department must allow ample time, usually many months, if possible, to review features and make a well-researched decision. With many months for review, an IT department can set up lab environments and see which solution best meets their needs in both functionality and cost. In larger organizations there may even be a requirement to open up a project to a bid process, including a request for proposal (RFP) process. This is one way for an IT organization to review specific offerings and weigh their merit based on various factors. Some of the factors a company may use to assess a vendor's offering include:

- Cost
- Vendor's reputation
- Vendor's record on delivering solutions
- Organizational familiarity with a specific vendor's technology
- End user requests
- Usability
- Performance in a proof of concept lab
- Supportability
- Changes needed to existing infrastructure
- Help desk needs

Every system introduction needs to be reviewed individually against the selection factors. The weight of each selection factor will be different depending on the organization doing the review. Each IT department needs to determine what selection factors are most critical to their organization.

Build versus Buy

When reviewing solutions, there may be a lack of vendor products to do the job. In that case, if there is enough demand an IT organization may need to create the solution from scratch. When building your own solution you accept an additional set of issues. Building your own software solution is in almost all cases more expensive then using off-the-shelf software. An organization should only build their own software when a suitable solution does not exist or the current offerings do not meet their specialized needs. This will need to be assessed individually for each scenario. In most cases an IT organization will save money if they can purchase a solution. Even when some of the components are purchased and a subset of the solution is developed in house, there are still savings to be had.

Anything that is built must be supported. The support costs of internally built software are often poorly accounted for. In addition to the support costs, many times "homegrown" software is reliant on a few or even one individual in an organization; we have seen solutions fall apart because the "smart guy" decides to leave the company. The same can also apply to complicated packaged applications when there are only a few employees that understand how to operate a specific piece of software.

Even with all of the pitfalls of internally created applications, sometimes it is necessary to create homegrown solutions to meet a need. When an organization decides to create their own applications, proper processes need to be followed for sound development practices. Once the software is built, training and support must be a part of the process. Essentially any internally developed application should be treated as if it is a packaged product, with the delivering party (IT) being obligated to provide all of the services that are available for packaged software.

That brings us to an area that is somewhere between purchased software and homegrown software: open source software. If an organization has a highly skilled staff, open source software may be the way to go because you can obtain many pieces of software that can be modified per the open source agreement that the writers have placed on the package. The downside to using open source software is that IT staff will need to support it or someone IT pays will have to when anything goes wrong. This is where an IT organization will need to be honest with itself about the skill of its personnel with software development and its ability to support software and possibly make changes to the software so it works for the organization.

Staffing Requirements

When reviewing an IT solution, the staffing requirements need to be considered. A constant review of the IT staff skill set must be performed so that IT management can make changes and shift staff based on operational needs. When bringing on new services, there may be the need to bring in new staff or repurpose staff based on need. Wherever the staff comes from, when the system is new there will be some ramp-up time involved. When the staffing operational function is outsourced there may even be a need for additional time to bring the service online. The additional time and resources must be considered to ensure that a new service is initiated correctly.

Hardware Requirements

With new services being brought online, there will be the need for new hardware to drive the services. The resource requirements will be clearly listed in any vendor documentation. Based on the calculations provided in vendor documentation, an IT department can plan and budget for the needed hardware to support a specific service in their infrastructure. In the hardware estimate, IT managers need to plan for growth in both the service and the organization. This way there will be no shortcomings that will degrade the service. Slow service will always hinder a service's popularity with end users. Unpopular services are killed outright or through diminished funding. It is up to the IT staff to make sure that new services meet the end users' expectations, and one of the easiest ways to ensure a quality service is to make sure new applications run quickly.

Software Requirements

Software requirements can be very easy or complicated, depending on the organization and how it works, and what policies they have in place. All software must meet request for comments (RFC) requirements and be compliant with current organizational and security policies. Organizational policies can be very complicated, depending on the organization and what specifically is required for the software to be installed. Some of the things that may need to be considered when selecting software are:

- Hardware requirements
- Database needs
- Application servers
- Web servers
- Development environments
- Development languages
- Communication protocols
- Authentication methods
- Authorization methods
- Changes to the existing environment
- Directory needs

- Network requirements
- Additional software requirements

Budgeting

It is very important to get the budgeting correct. Sure there are times when projects go over, but making a habit of going over budget will shorten one's career in IT management. The best way to get the budget correct is to make sure that all of the aspects of a project are considered. Missing project components and then having to pull together funds later from some other source will ensure that the project as a whole is less effective. One way to ensure an adequate budget is to pad the budget, but overpadding will expose the fact that the scope of the project is not understood. The best way to get a budget correct is to meticulously cover all aspects of the deployment process and fund all of the steps in the process, including an exception for a margin of error.

Skills Assessment

All IT departments should have regular skills assessments to understand the abilities of their personnel. This assessment can then be used to ensure the correct skill sets exist in the organization when new projects are brought on. If there is a lack of a specific skill, the group can either have someone trained in the skill or the department can hire a new employee with the needed skills to cover the new project.

Training, Consulting, or Both

There are many ways to bring new skills into an organization. Employees can be trained in new skills. Consultants can be brought in to take care of the job. Or consultants can be brought in to run a specific program until the staff is adequately trained to run the service. Tasks can also be outsourced. Each decision has consequences. Larger companies with a focus on permanence must focus on training or hiring new staff. This way the skills will propagate throughout the organization and remain in the corporate culture. A combined approach of using training and consultants can be effective, whereby full-time staff learn by observing the consultants who are familiar with a new system.

Solution Architecture Build Process

The solution build process is where the technical gurus of the company get to show their stuff. Building a solution requires various groups within the IT organization—operational staff, networking staff, development staff, and IT management—to

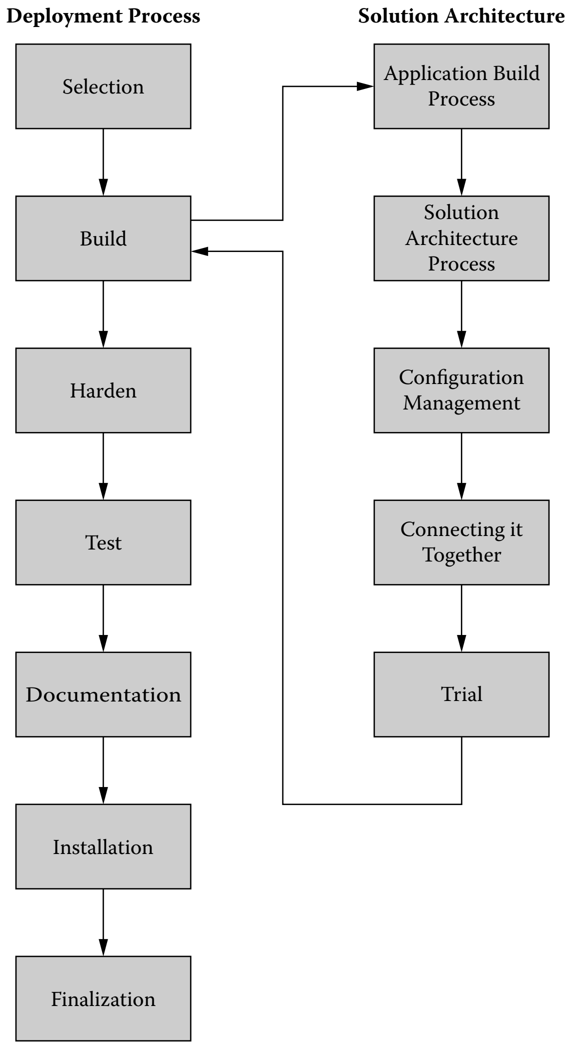

Figure 8.3 Solution architecture.

work together to put together a complete solution. Some of the steps in the process may be omitted depending on the solution that needs to be built. Certain solutions may require no software coding and rely on existing software solutions. The solution build process is shown in Figure 8.3.

Application Build Process

If there is coding required for a specific solution, this must begin first because it will probably be the task that requires the most time. Other pieces of the process can start in parallel to speed the overall solution build process in addition to supporting the development process. There are many books about the software development process. In this text we will not go into any detail about the build process because this book is more focused on broader IT management. The development required to bring a solution live can vary greatly depending on how much new code the solution requires. There are many off-the-shelf products that require little development. The only issue with off-the-shelf software is that many times it is not specific enough to meet the needs of an organization. Line of business (LOB) applications are very customizable. When using various LOB applications, organizations may need to develop various components of the application with either known programming languages or in some cases proprietary programming or scripting languages. In some instances there will need to be some “glue” code to connect various applications together.

Solution Architecture

The solution architecture is when all the pieces of the solution process are put together. This can include applications and glue code built in house as well as purchased software. The overall solution build includes cross IT organization collaboration to make sure that all of the correct groups are involved in the solution build process.

Configuration Management

When the solution is completely built, the configurations must be added to the configuration management database (CMDB). Previous chapters have discussed this process in depth.

Connecting It Together

When building a solution, there are times when the various components are built and configured by different groups within the IT department. There is a point when the various groups need to put all of the pieces together. This must take place in a test lab or trial area within the live production environment.

Trial

During the service deployment, a subset of trusted end users will need to be entered into a trial group. This group must include the IT staff that will support the new application. A trial should happen once the system is up and running in the production environment. It can even be open to limited trial while the new service is in the lab environment. The trial can be used to gather information on the end user experience. This way IT can improve the process and meet minimum user expectations before going live. The worst thing an IT group can do is go with a big line of business application release only to find that end users will not use the application.

Hardening Process

The hardening process must always happen before an application is released into the production environment. Hardening a system does not mean that it will then be "hack" proof, but it will ensure at least a minimum level of security is reached. By hardening a system, an IT security department does its due diligence in protecting corporate systems. The steps in the hardening process are shown in Figure 8.4.

Threat Modeling

Threat modeling is a method for discovering possible threats a piece of software or system may encounter. By going through the process of threat modeling a service manager can then put in place the countermeasures and controls to stop known threats. The threat model identifies threats to the system; it is not focused on mitigating risks. That comes later in the hardening process. There are entire books dedicated to threat modeling, so we will not go into great detail here.

Access Points

Threat modeling is a way of looking at your system through the eyes of the attacker. The first thing an attacker will look for is a way to get into your system. A networked entry point is always most desirable. The threat model must note all possible entry points. The entry points list should include every possible way an attacker can access a system, including:

- Login screens
- Communication ports
- Physical ports (USB, serial, etc.)
- Network application access
- Remote access protocols

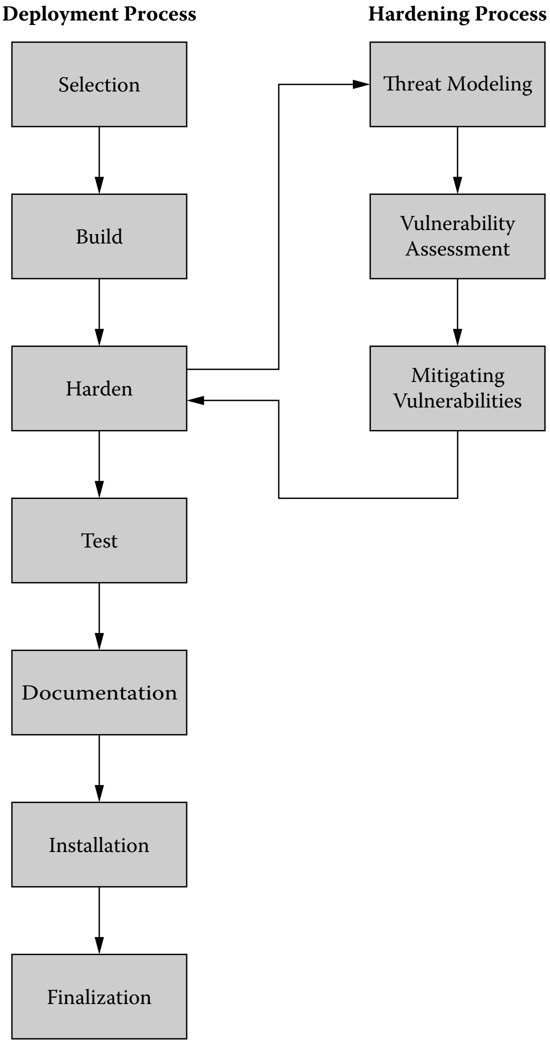

Figure 8.4 The hardening process.

Asset Targets

Understanding one's information assets is very important and a review performed yearly as a separate task from normal threat modeling will increase visibility. The value of various assets varies greatly from organization to organization. The determined value of informational assets will set the tone and budget for the information security group. The value of information will be different within various industries. Once the valuable information assets are identified an organization can use that information to decide how an attacker would go about accessing that information.

High-value information and key systems are targets for malicious attacks. An interesting exercise for an organization to try is to determine which systems would affect the company most if they were offline for 1 day. Some organizations are not so reliant on computer systems, and those companies may not have to worry about their information assets being the target of a malicious user. But for most organizations, their computer systems are critical to their ongoing operations. The determined value will help an organization understand the level of resources it needs to protect its information.

Access and Authorization Levels

The access people and applications have to other applications must be managed and limited. Access to various computing objects must be carefully monitored. Monitoring access can help catch intruders, and any access from unknown locations or excessive access should raise concern with the IT security group. There are applications that watch for these exact scenarios. Organizations that are vulnerable to network-based attacks will benefit from putting in place an application that monitors network activity and acts on spikes in certain activities.

Application Model

Each application that goes through the threat modeling process must be reviewed separately. All systems will have specific scenarios that can manifest vulnerabilities. When reviewing an application, various scenarios need to be created that will mirror what the threat modeling team thinks will be ways in which intruders could possibly attack the application. The various scenarios need to be listed and ranked by severity and probability. Dependencies on other applications must be noted and the communication channels must be understood in the application model. A list of all of the possible threat points needs to be noted in the threat model for use throughout the process.

Threat Understanding

Once all of the threat scenarios have been identified, the threats need to be listed and analyzed for severity and probability. A review of threats needs to take into consideration the environment the threat will occur in and how the organizational environment works. In all environments there is the possibility of human error, which raises the possibility of threats. These scenarios need to be considered with the probability of them happening. An employee may be coerced into giving up a password, but the probability of an attacker doing so at a bank is probably higher than at an auto parts reseller. All aspects of the threat need to be understood to make sure that after the threat is identified it can be properly addressed with mitigating measures.

Vulnerability Assessment

The vulnerability assessment is much different than threat modeling. Threat modeling is where possible threats are identified, while a vulnerability assessment is where attempts are made to breach a system with known attack techniques. There are two ways that one can conduct vulnerability assessments: automated vulnerability assessments and penetration test teams (human teams that attack systems). Automated systems are nice for periodic vulnerability checks, but for a more in-depth review of system vulnerability it is best to use a penetration test team.

Automated Assessments

There are many variations of automated vulnerability detection systems, including intrusion detection systems (IDS), network intrusion detection systems (NIDS), intrusion prevention systems (IPS), and host-based intrusion detection systems (HIDS). There are many vendors that sell systems that will search for system vulnerabilities. Larger organizations will have one or more types of assessment technology. These technologies are run against any new system that will be introduced into the production environment. This makes the person who runs the system scans aware of new systems and allows the new service managers to detect any large security vulnerabilities.

Penetration Test

Once the automated tests are done, the next step is to have professionals try to hack into your system. Large organizations usually have an internal team that does penetration testing. There are also consultants that specialize in penetration testing. If the system is critical, it is advisable to have both internal and external penetration test teams attack a system before it goes live. There are even groups that are teaching individuals to be certified ethical hackers. The EC-Council has a set of courses and exams. This is a good program, but as with any certification program, you need to look at the individual beyond the certification and make sure they have the skills to do the job you require. When hiring an external entity to do a penetration test, make sure you have a written contract in place. The contract must note all of the attack vectors that are in bounds and what things are off limits to the contractor.

Mitigating Vulnerabilities

Finally, vulnerabilities that have been identified need to be addressed. The vulnerabilities from both the vulnerability assessment and threat modeling are listed and ranked according to probability and severity. Risks can be dealt with in several ways: mitigate the risk, insure the risk, or accept the risk.

For new applications, many times mitigating the risk is as easy as a configuration change. These types of changes must be made immediately and added to the CM system so they become a part of the normal configuration environment. The next level of changes may include changes to a subsystem or may require add-ons to the original software. This level of change may require additional budget. The next type of vulnerability mitigation is to add additional systems to your current solution to perform specific security or hardening measures. These types of systems include firewalls, security protocols, access control systems, and encryption hardware and software.

If you cannot resolve a vulnerability, there are two other things that can happen. Insurance can be purchased to reduce or remove the risk from an organization and place the risk on the insurer. Or an organization can accept the risk and bear the burden itself. When an organization accepts a risk there must be a signoff process so that upper management is aware of and accepts the vulnerabilities.

Testing

For any IT organization, a test lab is an important part of the overall toolbox. The test lab is a place where they can try out things in an environment that is similar to the production environment. The test lab is a tool that can be used for verification of new initiatives and ideas.

Test Lab

The test lab needs to be a part of many different processes. A test lab needs to have a very strict protocol for usage and projects. Many organizations have a test lab in some form. Test labs need to have the same equipment that is used in the production environment. That is the only way the IT staff can prepare to take things live in the production environment. An IT department without a test lab is like a basketball team without a ball. There is no way for the team to prepare for a real game. They may be able to make an educated guess on how things work, but they will not know the specific mechanics. A test lab must have as much of the production environment as possible.

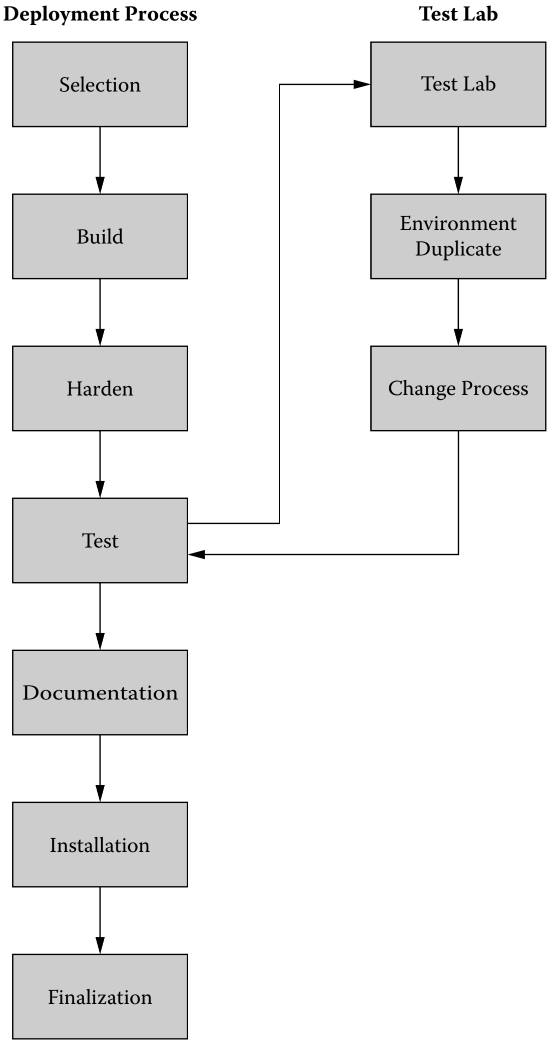

Figure 8.5 The test lab.

Duplicate Environment

A test lab must be able to duplicate the environments that need to be tested. In some duplication efforts even exact wire types may be critical in troubleshooting complicated environments. Every component must be duplicated. In some instances there may be a budgetary need to reduce costs. One way to reduce costs in a test lab is the virtualization of system hardware. This is acceptable for software solutions, but when testing a networking environment, the lab must include networking hardware such as switches and routers, and as much of the live environment as possible. When changes need to be made to hardware-specific operating systems, the lab must provide the ability to make changes to those pieces of equipment.

Change Process

The test lab is an integral part of the change process. Any changes to the production environment must go through the test process in a duplicate environment. The test lab must duplicate the change and the environment the change is going to be placed in. Application compatibility issues can be caught by running all other applications on the platform being tested. Putting changes through this type of lab process allows the IT department to make the change with a level of confidence. The acceptance process must include a signoff by lab personnel that tested the change in the environment.

Documentation

The documentation for commercial applications is provided with the applications. The company will need to do some documentation work when there is a company-specific use for an application (Figure 8.6). Line of business applications are the most typical applications that will require an IT department to rework the application's documentation so it makes sense for the organization. Also, if an organization creates custom applications or add-ons, those will need documentation as well.

Software and Hardware Documentation

Documentation comes with the software and hardware that an organization purchases. Most end users do not even want to look at the hardware documentation. Some like to have a copy of the software application documentation. But most will look to the IT department to provide training on new applications.

Organization-Specific Documentation

More important is the documentation work that needs to be done on custom applications. The documentation needs to be specific so that an end user can follow step by step and perform the new tasks required of them.

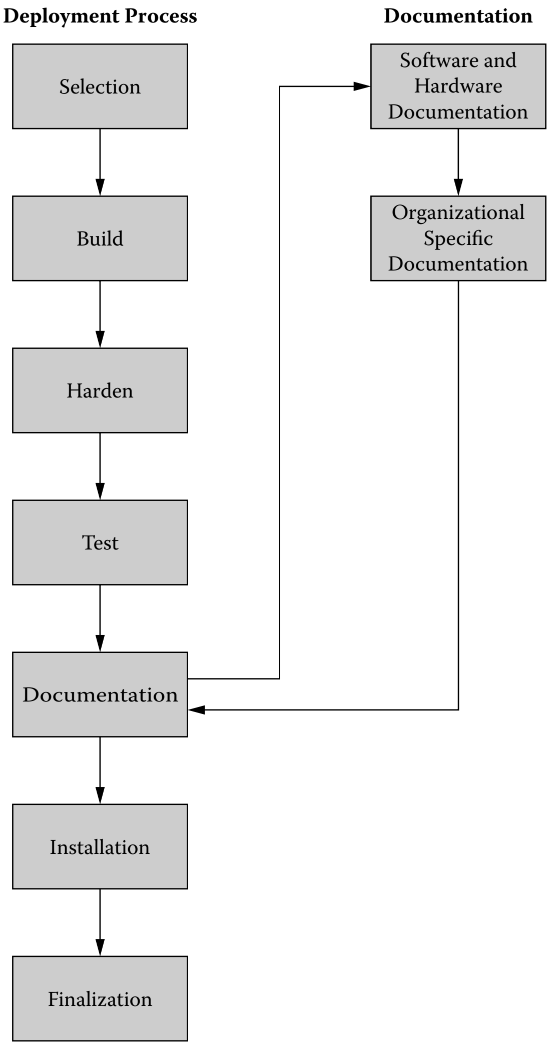

Figure 8.6 The documentation process.

Installation

Now that all of the preparation work has been done it is time to take the plans live and install the new service in the production environment (Figure 8.7). A few questions need to be answered: Where will the service be installed? How will it be installed? Who will do what tasks?

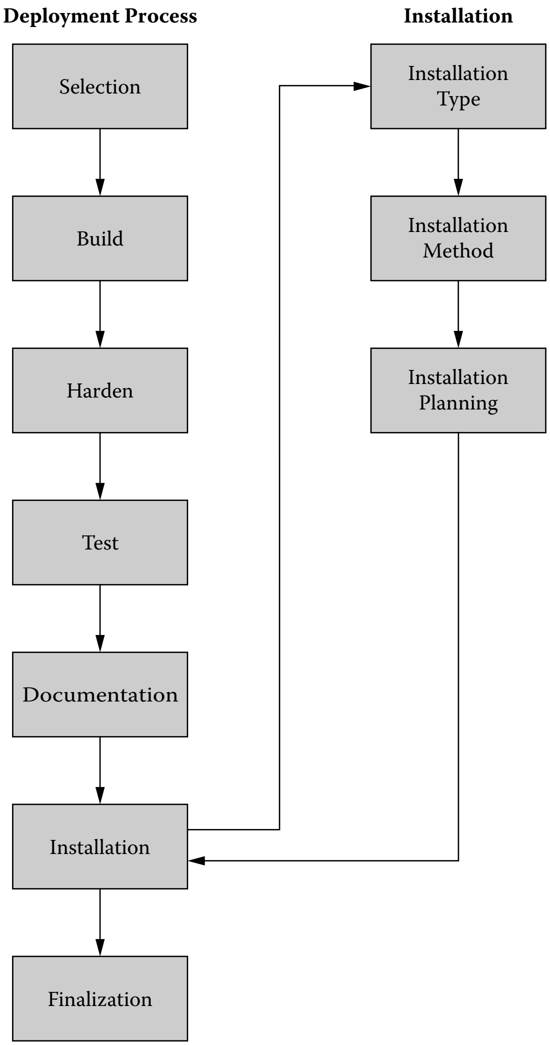

Figure 8.7 The installation process.

Installation Type

When deploying a system into the production environment, the target systems need to be identified. Server systems are easier than having to push systems out to the end users. In some cases software may need to be put on both servers and clients. Each type of install is very different, so planning needs to take place for the various types of installations. Hardware needs to be identified as targets for the software.

Installation Method

Software can be installed in several different automated ways— systems management software, OS-based software push, PXE boot-based software install—and if required software can be installed manually. There are multiple vendors that support each of these methods and it is up to the IT department to select the preferred solution. In the worst-case scenario, IT can install software manually.

Installation Planning

Planning for the installation will ensure that it goes smoothly and is finished in the scheduled time. Planning can identify the required staff for the various tasks. It can assign a timeline to all of the tasks so that project planners can be aware of any issues with the installation process.

Finalization

The finalization of a deployment is about making sure the installation is ready to be taken live in the production environment (Figure 8.8). There are a several tasks that must be completed to make sure the offering is ready to be supported by the IT department.

Installation and Operational Verification Process

With the installation complete, there will be a signoff process where someone other than the installer checks the configuration against what is logged in the CMDB. This is a secondary check to make sure there is nothing that was missed during the installation. After the system is handed over to a service management team, a check must be performed on the operational components to make sure that the operations team is capable of handling the day-to-day management of the system.

Check Installation

The installation must be verified by someone that was not a part of the installation group. All of the configurations that have been entered into the CMDB must be verified as accurate. This verification will catch any misconfigurations. Once the installation is verified as accurate it can then be considered production ready, and from that point any changes to the configuration must go through the change management process. This way the level of accountability will be raised on the offering and it can be considered a trusted service.

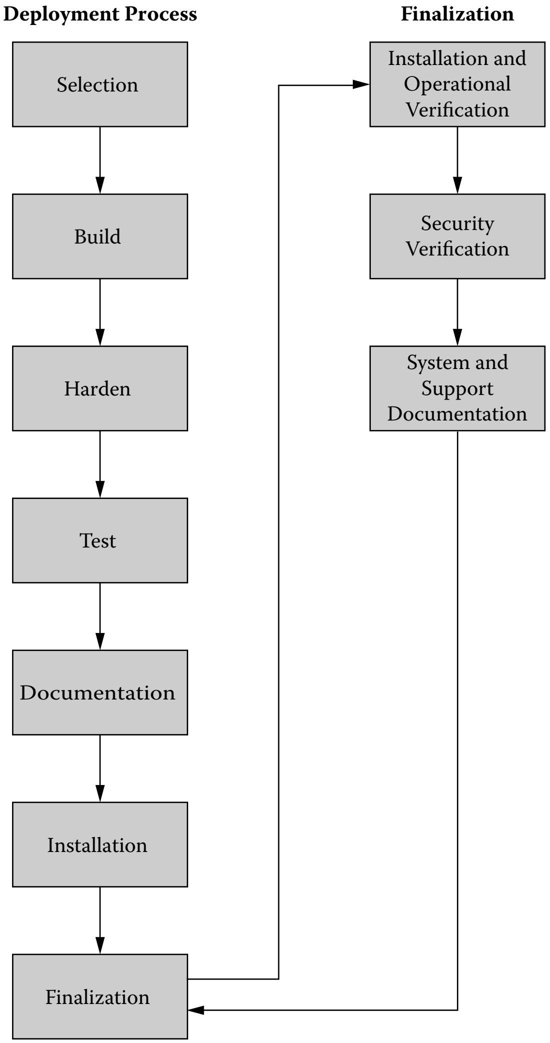

Figure 8.8 The finalization process.

Check Operations

The service is handed over to an operations group once the installation is verified. The operational components of a service must also be verified. This may require that some changes be made to the service operations team. Things to check for in an operational review are:

- Staff training
- Staff numbers

- Knowledge of service
- Understanding of documented procedures
- Incident response
- Business continuity

This is a short list of the things to verify. There are many others that are business and application specific.

Security Verification Process: Vulnerability Assessment

Security checks were performed during the system hardening process. This is a great way to find flaws in the architecture. The production system must be checked again once it is in place. Inevitably there will be some changes between the architecture phase and the systems that are placed in production; these differences may not even be noted anywhere. Because there is a human element to software deployment there is always the chance that there will be some missed system vulnerabilities.

Run Scans

The software-based scans must be run again against the system. In addition to a one-time scan that is heavily scrutinized, scans of all systems should be a regular occurrence in enterprise-level production IT environments. The first scan is used to identify a baseline of health. From this baseline it will be easier for the scans to identify changes in the system.

Internal Penetration Test

These tests were run once before, but it is important to perform penetration tests in the final phase as well. Internal penetration tests are performed by larger enterprise organizations that have the resources to have their own penetration test teams. These tests are also a great way to create a baseline of system health. The internal penetration test accentuates the intricacies of the system and is a great resource in case there is need for incident response.

External Penetration Test

External penetration tests are something that should be performed by all organizations, regardless of size, deploying a new large software service. This second set of penetration tests is critical to ensure things are ready to go. External testers have a different skill set than internal penetration testers and can discover new vulnerabilities. External testers are a great second check for people that may be too close to the project to see all of the flaws. One thing to make sure is that the organization's IT department must consider external testers a positive. All external consultants should be used as tools for organizational improvement. A hostile internal environment will only diminish the work of the external consultants by making it less effective. Consultants rely on correct input from the IT staff to make their conclusions. Any deception only hurts an IT organization by giving it a false sense of security.

Initial System and Support Documentation

System and support documentation is very important in the handover process of software deployment from the install/build team to the operations team. Even if the operations team is involved in the build, the two functions are very different. Even when a software deployment is successful, it does not mean the project overall is successful until the operational goals have been realized. This may happen over many years. Quality documentation is key to this success. Within IT organizations, change is normal. IT organizations seem to change faster than other departments; this is indicative of the way technology is changing. Good documentation can allow these changes to occur without causing a degradation in the quality of service.

Check the Support Process

A support process needs to be created and in place before a service is available to the end users. The support process, if correctly managed, will improve over time. It takes some time to work out all of the issues in new products and services. With time, issues appear and are eventually resolved. The process must support both change and improvement so that the support required over time is reduced.

Check the Documentation

The documentation must be checked for technical and operational accuracy. Problems will eventually come to light via the support process. A review of the documentation reduces the number of errors in the initial version. Revisions need to be made to the documentation so that at a certain point the service can be considered mature and only needs to change based on the broader environment the service is deployed in. The documentation should be targeted to specific users and must be simple and provide step-by-step solutions to various scenarios an end user may encounter. Administrator documentation can be more technically specific.

Gather End User Feedback

Many IT organizations work without soliciting end user feedback. The end user is your customer. End user feedback should be gathered frequently to make sure there is an acceptable level of confidence in the IT organization and their services. The end users should understand the issues the IT organization faces so that IT can be seen as an asset to the organization instead of a necessary evil. Training can go a long way in improving IT's organizational perception. When an IT organization is seen as doing a poor job it will become increasingly difficult to provide quality service.

Conclusion

The deployment process is a linear process that must be followed in specific order. This order is shown in Figure 8.9. The deployment process is risky for IT organizations to execute because failures will waste large amounts of the IT budget. The

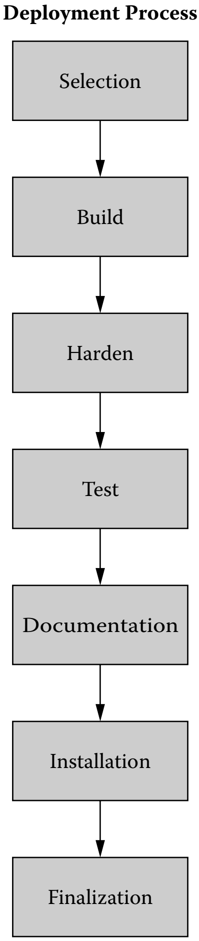

Figure 8.9 The configuration management deployment process.

positive aspect of deployment is it provides a valued service to the organization to improve the business. The more successful an organization is at deploying new technology, the more successful the IT organization as a whole will be viewed. Careful adherence to a well-defined deployment process will help IT be successful in their overall goals.